

privileges similar to the Client Admin but is restricted to their specific division or department. This ensures that managers can autonomously handle their departments without unnecessary broader access.

- **Client User:** Crafted for the general user base, this role focuses on operational needs like creating, editing, and canceling work orders. While they have sufficient access to perform their tasks, they are shielded from managerial reports to maintain data integrity and restrict unnecessary exposure.

Customizability & Flexibility: We believe that every client's needs are unique. Therefore, if there's a requirement for a bespoke user role, we are fully equipped to accommodate such requests. You can request these customizations either during implementation or at any point during the contract term. Whenever a request is made, our team will work closely with you to incorporate these custom features, ensuring that our platform aligns perfectly with your organizational needs. And we're proud to offer these customization features at no additional cost, reinforcing our commitment to delivering value and excellence.

In conclusion, Volatia places paramount importance on data integrity, security, and user-centricity. Our platform's design and capabilities reflect this ethos. With our combination of robust access controls, flexible user roles, and a commitment to adaptability, we are confident that Volatia stands out as an appealing, secure, and user-friendly option for your requirements.

B. Please describe the system's ability to set access based on department within the system.

Access Based on Department within the System: Understanding the unique needs and data sensitivity of various departments, Volatia's system is designed to compartmentalize access:

- Each department or division can have its unique set of users with tailored access permissions. This granularity ensures that sensitive data is compartmentalized, accessible only to those who genuinely need it for their tasks.
- In instances where cross-departmental access is required, users can be effortlessly assigned to multiple departments, ensuring seamless operations without compromising on security.

It's worth noting that our flexible system allows for users to be assigned to multiple divisions or departments, ensuring adaptability in complex organizational structures.

C. Please describe the system's ability to allow users to designate certain fields as confidential and restrict access to those fields.

Confidentiality of Specific Fields: Volatia only capture the essential information, striking a balance between efficiency and compliance. Recognizing the occasional need for enhanced confidentiality, Volatia's platform allows:

- Users to designate specific fields within a work order as confidential.
- Once marked, these fields are masked or hidden from users who don't have the necessary permissions, ensuring that only those with a genuine need can view the confidential information.

You can request these customizations either during implementation or at any point during the contract term.

D. Please describe how the solution allows for the designation of a system administrator separate from the security administrator or data users.

System & Security Administration:

- **Client Admin Role:** This role acts as the system administrator, overseeing the entire account, and is pivotal in making important decisions and changes.
- **Security Administrator via Auth0:** Our partnership with Auth0 for Single Sign-On (SSO) ensures that security is of paramount importance. The security administrator role is established during the SSO setup, which is distinct from the predefined roles, focusing exclusively on security features and configurations. Volatia's SSO solution offer centralized user management, which directly interfaces with Active Directory. This allows administrators to easily manage user access permissions, roles, and privileges from a single, user-friendly administrative interface. Such centralized management is not only efficient but also reduces the possibility of errors or security oversights, further enhancing system integrity.

E. Please describe how the solution restricts access by user ID.

Restriction by User ID: Volatia employs Auth0 as our SSO solution. Auth0 is a highly reputable, industry-leading identity and access management platform known for its robust security features and user-friendly interface.

- **Unique Identification:** Every user in Volatia's system is assigned a unique user ID, ensuring distinct identification.
- **Multifactor Authentication (MFA):** We have the option to enforce MFA. This provides an extra layer of security by requiring two or more verification methods: something the user knows (password), something the user has (a phone or hardware token), or something the user is (fingerprint or facial recognition).
- **Role-based Access Control (RBAC):** With Auth0, Volatia employs RBAC, allowing us to assign permissions to specific roles and then assign these roles to users. This ensures that users have access only to the resources appropriate for their roles.
- **Centralized User Management:** Volatia's SSO solution offer centralized user management, which directly interfaces with your organization's Active Directory. This allows administrators to easily manage user access permissions, roles, and privileges from a single, user-friendly administrative interface. Such centralized management is not only efficient but also reduces the possibility of errors or security oversights, further enhancing system integrity.

F. Please describe how the solution restricts access by database table.

Restriction by Database Table: Volatia employs Auth0 as our SSO solution. Auth0 is a highly reputable, industry-leading identity and access management platform known for its robust security features and user-friendly interface.

- **Scoped Permissions:** Auth0 allows for the creation of scoped permissions. This means that users can be granted access to specific database tables and not others. For instance, a finance user might only have access to finance-related tables but not to HR-related tables.
- **Data Masking:** Sensitive fields within database tables can be masked, ensuring that even if users have access to a table, certain data remains obscured.

Note: Volatia only capture the essential information, striking a balance between efficiency and compliance. Recognizing the occasional need for enhanced confidentiality, Volatia's platform allows:

- Users to designate specific fields within a work order as confidential.
- Once marked, these fields are masked or hidden from users who don't have the necessary permissions, ensuring that only those with a genuine need can view the confidential information.

G. Please describe how the solution restricts access by transaction type.

Restriction by Transaction Type: Volatia employs Auth0 as our SSO solution. Auth0 is a highly reputable, industry-leading identity and access management platform known for its robust security features and user-friendly interface.

- **Granular Permissions:** Beyond table-level restrictions, our integration allows us to specify the types of transactions a user can perform - be it create, read, update, or delete operations.
- **Audit Trails:** Every transaction is logged with user ID, timestamp, and transaction details. This ensures transparency and traceability of all actions.

Note: Volatia only capture the essential information, striking a balance between efficiency and compliance. Recognizing the occasional need for enhanced confidentiality, Volatia's platform allows:

- Users to designate specific fields within a work order as confidential.
- Once marked, these fields are masked or hidden from users who don't have the necessary permissions, ensuring that only those with a genuine need can view the confidential information.

H. Please describe how the solution restricts access by screen or menu.

Restriction by Screen or Menu: Volatia employs Auth0 as our SSO solution. Auth0 is a highly reputable, industry-leading identity and access management platform known for its robust security features and user-friendly interface.

- **Dynamic UI Rendering:** Based on the authenticated user's permissions and roles, our system dynamically renders screens and menus. This means users only see the options and interfaces they are allowed to interact with.
- **API Security:** Our backend APIs, which serve data to these screens, are also secured using Auth0, ensuring that even direct API calls without using the UI are subject to the same strict access controls.

Note: Volatia only capture the essential information, striking a balance between efficiency and compliance. Recognizing the occasional need for enhanced confidentiality, Volatia's platform allows:

- Users to designate specific fields within a work order as confidential.
- Once marked, these fields are masked or hidden from users who don't have the necessary permissions, ensuring that only those with a genuine need can view the confidential information.

I. Please describe how the solution restricts access by report type.

Restriction by Report Type: Volatia employs Auth0 as our SSO solution. Auth0 is a highly reputable, industry-leading identity and access management platform known for its robust security features and user-friendly interface.

- **Report-specific Access:** Similar to database tables, users are granted access to specific report types based on their roles and permissions.
- **On-the-fly Data Masking:** For sensitive reports, we can mask specific data points ensuring that confidentiality is maintained.

Note: Volatia only capture the essential information, striking a balance between efficiency and compliance. Recognizing the occasional need for enhanced confidentiality, Volatia's platform allows:

- Users to designate specific fields within a work order as confidential.
- Once marked, these fields are masked or hidden from users who don't have the necessary permissions, ensuring that only those with a genuine need can view the confidential information.

J. Please describe the system's security controls to define users authorized to perform the following:

1. Log on

Authorization to Log On: Volatia employs Auth0 as our SSO solution and thus offer centralized user management, which directly interfaces with your organization's Active Directory. This allows administrators to easily manage user access permissions, roles, and privileges from a single, user-friendly administrative interface. Such centralized management is not only efficient but also reduces the possibility of errors or security oversights, further enhancing system integrity.

Therefore, all user roles within the Volatia system – Client Admin, Division Admin, and Client User – are authorized to log on to the system.

Note: Customizability and Adaptability

We reiterate our commitment to meet unique client needs. If any adjustments or

customizations are required in the authorization matrix, Volatia stands ready to adapt. This ensures that our platform not only provides robust security controls but also aligns perfectly with your organizational workflow and hierarchy.

2. Add data

Authorization to Add Data

- **Client Admin:** Possesses full rights to add data across the entire system, ensuring seamless operations.
- **Division Admin:** Has the privilege to add data but limited to their specific division or department. This ensures relevant data addition without unnecessary broader access.
- **Client User:** Can add operational data, like creating work orders. Their ability to add other data types is restricted to maintain data integrity.

Note: Customizability and Adaptability

We reiterate our commitment to meet unique client needs. If any adjustments or customizations are required in the authorization matrix, Volatia stands ready to adapt. This ensures that our platform not only provides robust security controls but also aligns perfectly with your organizational workflow and hierarchy.

3. Delete data

Authorization to Delete Data

- **Client Admin:** Has comprehensive access, allowing them to delete any data within the system, which ensures full control.
- **Division Admin:** Can delete data within their respective divisions. They cannot delete data outside their jurisdiction, thus maintaining data compartmentalization.
- **Client User:** Typically, does not have the rights to delete data unless explicitly granted, ensuring data safety, and preventing accidental deletions.

Note: Customizability and Adaptability

We reiterate our commitment to meet unique client needs. If any adjustments or customizations are required in the authorization matrix, Volatia stands ready to adapt. This ensures that our platform not only provides robust security controls but also aligns perfectly with your organizational workflow and hierarchy.

4. Change data

Authorization to Change Data

- **Client Admin:** Can modify any data in the system, granting them full flexibility.
- **Division Admin:** Can change data within their division or department, ensuring departmental autonomy without risking wider system integrity.
- **Client User:** Focused on operational changes, such as editing work orders. Broader data modifications are restricted.

Note: Customizability and Adaptability

We reiterate our commitment to meet unique client needs. If any adjustments or customizations are required in the authorization matrix, Volatia stands ready to adapt. This ensures that our platform not only provides robust security controls but also aligns perfectly with your organizational workflow and hierarchy.

5. View data

Authorization to View Data

- **Client Admin:** Has unrestricted access to view all data in the system, ensuring holistic oversight.
- **Division Admin:** Can view all data related to their division or department but cannot access data from other divisions.
- **Client User:** Can view data relevant to their tasks, but managerial reports and other sensitive data are off-limits to maintain confidentiality.

Note: Customizability and Adaptability

We reiterate our commitment to meet unique client needs. If any adjustments or customizations are required in the authorization matrix, Volatia stands ready to adapt. This ensures that our platform not only provides robust security controls but also aligns perfectly with your organizational workflow and hierarchy.

6. Search data

Authorization to Search Data

- **Client Admin:** Unrestricted searching capabilities across the system.
- **Division Admin:** Can search for data within their division or department, enabling efficient data retrieval.
- **Client User:** Limited search capabilities, tailored to their role's operational requirements.

Note: Customizability and Adaptability

We reiterate our commitment to meet unique client needs. If any adjustments or customizations are required in the authorization matrix, Volatia stands ready to adapt. This ensures that our platform not only provides robust security controls but also aligns perfectly with your organizational workflow and hierarchy.

7. Approve data

Authorization to Approve Data

- **Client Admin:** Has the rights to approve any data, reinforcing their comprehensive oversight role.
- **Division Admin:** Can approve data specific to their division or department, ensuring timely approvals without dependencies on higher authorities.

- **Client User:** Does not typically have approval rights, ensuring that data approvals are done by the relevant managerial levels.

Note: Customizability and Adaptability

We reiterate our commitment to meet unique client needs. If any adjustments or customizations are required in the authorization matrix, Volatia stands ready to adapt. This ensures that our platform not only provides robust security controls but also aligns perfectly with your organizational workflow and hierarchy.

K. Please describe security reports showing:

1. Authorized system use

Reports on Authorized System Use: terpX, our proprietary interpreter management platform, logs all work order creations, edits, and cancellations; time stamping each action accordingly. For authorized system use, reports can be generated showcasing activities like data creation, editing, or deletion. Auth0 assists in this by logging successful authentication attempts, which forms a part of these comprehensive reports. If requested during implementation or at any time during the contract term, the Client Admin and/or division admin user(s) will be given the ability to create or retrieve a comprehensive report detailing all authorized actions performed by any user role in the organization or a given division.

2. Unauthorized system use

Reports on Unauthorized System Use: Unauthorized access attempts, security breaches, and any suspicious activities are meticulously logged and reported. Auth0 plays a critical role here by tracking failed login attempts, potential breaches, and other anomalies, ensuring swift response actions.

3. Security profiles by user (indicates multiple profiles)

Security Profiles by User: This report offers a detailed view of the various security profiles assigned to each user, indicating if a user has multiple roles or unique permissions. While Volatia manages the assignment of roles within its application, Auth0 supports this by facilitating secure profile management and access controls based on these profiles.

4. Effective dates security changes

Effective Dates of Security Changes: Any changes to security profiles, user roles, or permissions are timestamped and logged. This ensures an audit trail of when specific security changes were made and by whom. Auth0 assists by logging changes related to authentication parameters, such as password resets or the addition of multi-factor authentication methods.

In summary, while Volatia has implemented a detailed role-based access control system, Auth0 strengthens the security posture by providing robust authentication and logging mechanisms. Together, they ensure both operational flexibility and iron-clad security.

IV. General Security

A. Please describe your organization's process to assign clearance levels to internal or subcontract positions for accessing sensitive data.

Certification Matrix in terpX:

- Our proprietary platform, terpX, has a built-in certification matrix. This feature is specifically designed to support individualized client requirements.
- The matrix can be tailored to input a plethora of client specifications. This includes but is not limited to clearance levels, background check criteria, required training, essential certifications, and any other bespoke credentials or specifications as necessitated by our clients.

B. Please describe employment and background check processes on employees and subcontractors that will be involved in the direct support or custody of data and processes associated with the proposed solution.

Employment and Background Check Processes on Employees and Subcontractors

1. **Introduction:** At Volatia, we prioritize the security and trustworthiness of our workforce, understanding the paramount importance of protecting sensitive data and processes. Our rigorous background check procedures ensure that all employees and subcontractors involved in direct support or custody of data associated with the proposed solution meet the highest standards of reliability and integrity.
2. **Volatia's Background Check Provider: Karma Check:** We partner with Karma Check (<https://karmacheck.com>), an industry-leading provider of comprehensive background checks. This allows us to access an extensive suite of verification services, thereby support our commitment to due diligence in our pursuit to employ only the most qualified and dependable personnel.
3. **Background Checks Available Through Karma Check:** While the specific background checks can vary based on the nature of the role and requirements of our clients, the following are the checks available through Karma Check:
 - **Criminal History:** Review of county, state, and federal criminal records.
 - **Employment Verification:** Confirms previous employment, including positions held, dates of employment, and reasons for leaving.
 - **Education Verification:** Validates degrees, diplomas, or certifications from educational institutions.
 - **Credit History Check:** Reviews an individual's credit history (especially pertinent for financial roles).
 - **Drug Testing:** Ensures employees adhere to company drug policies.
 - **Motor Vehicle Records:** Essential for roles that require driving or vehicle operation.

- **Identity Verification:** Ensures the individual is who they claim to be.
- **Sex Offender Registry Check:** Protects vulnerable populations and confirms individuals are not listed on sex offender registries.
- **Professional License and Certification Verification:** Validates professional licenses and certifications.
- **Reference Checks:** Gathers insights from personal and professional references.
- **Global Watchlist:** Screens individuals against domestic and international watchlists, including terrorist watchlists, sanction lists, and more.

In accordance with our commitment to thoroughness, Volatia conducts criminal background checks in every county throughout the United States for the last seven years. Additionally, we screen potential hires against the global watchlist to ensure compliance with international standards and requirements.

4. **Processes for Employees and Subcontractors:** Upon considering an individual for employment or subcontracting, Volatia initiates the requisite background checks as per the role's demands and the specifics of the project. Any individual with a role involving the direct support or custody of data and processes associated with the proposed solution will undergo the comprehensive checks highlighted above.

In conclusion, Volatia's steadfast commitment to the security and integrity of our workforce ensures that our clients can trust in our delivery and safeguarding of data.

- C. Please describe your segregation of duties for staff performing key functions, which if not separated may create security collusion or other social engineering risks.

Segregation of Duties at Volatia

Introduction: At Volatia, we understand the importance of a robust internal control environment, and as such, we place a significant emphasis on the segregation of duties (SoD) among our staff, especially those performing key functions. We recognize that failing to establish adequate SoD can lead to potential security collusion and heightened susceptibility to social engineering risks. Our commitment is to ensure that our operations not only meet but surpass the industry standards, thus providing our clients with the utmost confidence in our services.

1. **Framework and Policy:** Our approach to segregation of duties is built upon a framework that focuses on four core principles:
 - **Definition:** Clear role descriptions and responsibilities.
 - **Differentiation:** Ensuring key functions do not overlap.
 - **Documentation:** Maintaining records of role assignments and any exceptions.
 - **Diligence:** Periodic review and adjustments based on operational needs and best practices.

We have established a dedicated SoD policy that provides guidelines, ensures compliance, and is reviewed annually to factor in the dynamic nature of business requirements and emerging threats.

2. Key Functional Areas and Their Segregation: Here is a breakdown of how we segregate duties among key functional areas:
 - *Finance and Procurement*: Staff handling payments are separate from those responsible for order approvals and reconciliation. This ensures that the person who orders isn't the same one who approves and pays.
 - *Systems Access Management*: The personnel responsible for granting access rights do not have the duties of monitoring or auditing those rights.
 - *Data Management*: Data input functions are separated from data verification and validation roles. Data backups, restorations, and purges are executed by different individuals.
 - *Incident Response and Reporting*: Those who handle incident response are not the ones responsible for incident reporting, ensuring unbiased and accurate reporting.
3. Use of Technology: We employ advanced role-based access control (RBAC) systems that enforce SoD electronically. The system raises flags for potential SoD violations, which are then reviewed by a dedicated compliance team.
4. Training and Awareness: All our employees undergo regular training on the importance of SoD, emphasizing the potential risks of security collusion and social engineering. This ensures that they are not only familiar with their roles but also understand the broader security implications.
5. Regular Audits and Reviews: Volatia believes in proactive checks and balances. We conduct quarterly internal audits to identify any potential SoD violations, followed by immediate corrective actions. Additionally, we welcome external audits to provide an additional layer of assurance to our clients.
6. Exceptions Management: While we strive for strict adherence to our SoD policy, we understand that exceptional situations may arise. In such cases, we have a transparent exceptions process, which involves:
 - Documenting the exception reason.
 - Time-limiting the exception.
 - Having higher management approval.
 - Continuous monitoring during the exception period.

Conclusion: At Volatia, our commitment to the segregation of duties is uncompromising, as we view it as a cornerstone of our integrity and the trust our clients place in us. We continually refine our processes, embrace technological advancements, and invest in our people to ensure we remain at the forefront of best practices.

- D. Please verify data is secure through the entire life cycle of the system to include data entry or data collection, data manipulation, data reporting or publishing, data transfer or transmission, data storage, and data disposal.

Comprehensive Data Security throughout System Lifecycle

At Volatia, we understand that ensuring the security of your data at every touchpoint is paramount, and we have made considerable investments in our technology and processes to ensure this. Here's a comprehensive breakdown:

1. Data Entry or Data Collection:

- terpX Platform: Hosted in Microsoft Azure, one of the world's leading cloud service providers known for its robust security measures.
- Real-time Filtering: With the help of Azure's Threat Intelligence-based Firewall, we block malicious IP addresses and domains in real-time, ensuring the data entering our system is from trustworthy sources.
- SSO with Auth0: We utilize Auth0 for Single Sign-On (SSO), which means fewer password-related vulnerabilities and adherence to the latest authentication protocols.

2. Data Manipulation:

- Role-Based Access Control (RBAC): With our centralized user management that interfaces directly with your organization's Active Directory, only authorized personnel with the appropriate roles and privileges can manipulate data. This drastically reduces the chances of internal data breaches.

3. Data Reporting or Publishing:

- Encrypted Reports: Any data reporting or publishing from terpX is encrypted, ensuring that even if intercepted, the data remains unintelligible to unauthorized entities.
- Audit Trails: All data interactions are logged, so we always have a clear trace of who accessed what, and when.

4. Data Transfer or Transmission:

- End-to-End Encryption: Data transferred between systems or transmitted to other entities is secured using state-of-the-art encryption protocols, ensuring its safety during transit.
- Regular Security Audits: We periodically audit our data transmission methods to ensure they align with the best security practices in the industry.

5. Data Storage:

- Azure Security: The data stored in our terpX platform benefits from Azure's extensive set of security features, including advanced encryption at rest.
- Regular Backups: Our system takes regular backups, and these backups are encrypted and stored securely, ensuring data integrity and availability.

6. Data Disposal:

- Secure Data Deletion: When data is no longer needed, it's disposed of securely, making sure there are no traces left. We follow industry best practices for data sanitization, ensuring once deleted, data cannot be recovered.

In conclusion, Volatia prioritizes the security of your data throughout its lifecycle. With a combination of cutting-edge technology like our terpX platform, partnerships with leaders like Microsoft Azure and Auth0, and rigorous security protocols, we're not just meeting industry standards – we aim to exceed them. Our commitment is to offer you peace of mind, knowing that your data is protected at every stage with Volatia.

E. Please verify the ability to conduct testing with test or fictitious (not live) data.

Testing with Fictitious Data: Volatia fully understands the importance of thorough testing before full-scale implementation, especially in projects where data sensitivity and accuracy are paramount. To cater to this, we have designed our pilot phase in a manner that enables clients to explore, train, and experiment with different use case scenarios extensively.

To address your specific concern:

1. **Fictitious Data Usage:** Yes, your organization will be able to test with fictitious data. During the implementation or pilot phase, Volatia offers the flexibility to either use real data or fictitious data, as per the client's preference. We recognize that there are scenarios where clients might not want to expose real data due to confidentiality reasons or are simply looking to simulate potential scenarios with synthetic data. To this end, we have the capability and processes in place to conduct tests with entirely fictitious data sets.
2. **Client Profile Creation:** We initiate the process by creating a dedicated client profile. This not only helps in customizing the experience and tools to the specific needs of your organization but also ensures that any fictitious data used is kept isolated and distinct from real-time operational data.
3. **Quality Assurance:** Even when using fictitious data, our testing processes maintain the same rigor and standards as we would with real data. This ensures that the outcomes of the tests are relevant and can provide actionable insights.
4. **Data Security:** Whether using real or fictitious data, we uphold the highest standards of data security, ensuring that data integrity is maintained, and there are no breaches.
5. **Feedback Loop:** Post testing, we engage in an iterative feedback process with the client to refine and optimize the solution based on the results, ensuring that the final solution is robust and aligned with your organizational needs.

F. Please describe policies and procedures for emergency software fixes and patches.

Emergency Software Fixes and Patches for Volatia's Platform

We, at Volatia, are committed to delivering robust, secure, and reliable software. Here's a comprehensive overview of our approach:

1. Identification

- Volatia employs continuous monitoring systems for the platform to swiftly identify anomalies or unexpected behaviors.
- We actively receive, value, and document feedback from our users to recognize potential issues.
- Our team conducts a prompt initial assessment to categorize the nature and extent of any reported problem.

2. Prioritization

- We've implemented a classification system that ranks issues based on their potential impact:
 - **Critical:** Risks to security, potential data loss, or significant functional

impairment.

- **High:** Major features affected but without an associated security risk.
- **Medium:** Non-core functions affected.
- **Low:** Minor inconveniences with negligible user experience implications.

- Resource allocation is performed based on these classifications, with Critical issues receiving immediate and dedicated attention.

3. Stakeholder Communication

- Transparency is crucial. Relevant stakeholders, including users and partners, are promptly informed about any recognized issue.
- In the interest of security, certain sensitive issues might be communicated discreetly to prevent exploitation.

4. Fix Development

- Our team isolates the affected software component to avoid disruptions.
- We replicate and diagnose the issue within our secure test environment.
- A fix or patch is developed, followed by rigorous internal testing to ensure stability and security.

5. Patch Deployment

- Deployment is ideally scheduled to minimize user inconvenience.
- Volatia maintains stringent backup protocols, ensuring we can revert changes if ever necessary.
- We employ state-of-the-art deployment methodologies to introduce patches smoothly.

6. Post-deployment Oversight

- Post-patch, we intensively monitor the system, ensuring the fix's efficacy and watching for any collateral issues.
- User feedback is actively sought and highly valued during this phase.

7. Comprehensive Documentation

- Every issue and its resolution are meticulously documented, ensuring transparency and facilitating continuous improvement.
- Our system documentation is updated to mirror any changes, ensuring our team and partners are always informed.

8. Reflective Review

- Volatia conducts a retrospective after any significant event. We assess our response, emphasizing both our strengths and areas needing refinement.
- Feedback is actively incorporated into our procedures, ensuring their evolution and refinement.

9. Continuous Vigilance

- Our commitment doesn't end post-fix. We are continually alert, monitoring for any new or related issues, ever prepared to act.

In summary, our thorough and proactive approach to emergency fixes and patches ensures that Volatia's technological infrastructure remains reliable, secure, and at the forefront of technological excellence.

G. Please describe any software escrow assurance.

Understanding Software Escrow: Software escrow is a service designed to protect both the software developer and the customer by having a third party hold a copy of the software source code and any accompanying documentation. This is a valuable safeguard for customers, ensuring they can maintain the software in case the developer cannot fulfill their obligations due to various reasons such as bankruptcy or obsolescence.

Volatia's Approach to Software Assurance: Volatia operates on a different model that does not require the traditional software escrow solution. Our platform is hosted on Microsoft Azure, a robust and reliable cloud computing service that offers a multitude of benefits and assurances.

The Strength of Microsoft Azure: Microsoft Azure is a comprehensive cloud platform that provides a wide range of cloud services, including computing, analytics, storage, and networking. Here are some of the credentials that make Azure a trusted partner for hosting our platform:

1. **Security:** Azure has an extensive, multi-layered security approach that includes identity, network, and threat protection. Their cybersecurity protocol is state-of-the-art, ensuring that data is securely stored and protected from any external threats.
2. **Compliance:** Azure complies with a comprehensive set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, and FedRAMP, among others.
3. **Reliability:** With a 99.95% SLA and 24/7 tech support, Azure guarantees high availability and continuous support for its services.
4. **Scalability:** Azure provides the flexibility to scale up or down based on the specific needs of the business, ensuring that Volatia can easily adapt to the changing needs of our clients.

Conclusion: By leveraging the capabilities and assurances provided by Microsoft Azure, Volatia offers a modern, secure, and reliable solution for your language access needs. Our decision to host our platform on Azure is a testament to our commitment to provide the best possible service to our clients, without the need for traditional software escrow. We believe that our innovative approach, coupled with the strength and credibility of Microsoft Azure, makes Volatia an ideal partner for your organization.

H. Please verify organization utilizes software for continuous detection and elimination of viruses.

Continuous Detection and Elimination of Viruses

1. **Cloud Hosting:** Volatia is committed to providing the highest level of security to protect our clients' data. Our proprietary platform, terpX, is hosted on Microsoft Azure, one of the most secure and reliable cloud platforms in the world. Microsoft Azure adheres to a strict set of security protocols to safeguard against threats, including viruses.
2. **Volatia's Utilization of Microsoft Azure's Security Features:**
 - **Firewall for Threat Intelligence-Based Filtering:** Volatia utilizes Azure's firewall, which incorporates threat intelligence-based filtering. This sophisticated firewall system enables real-time alerts and denies traffic from/to known malicious IP addresses and domains. This proactive approach to security helps to prevent viruses and other malware from infiltrating our systems.
 - **Continuous Detection and Elimination of Viruses:** In addition to the firewall, Volatia

employs continuous detection and elimination of viruses and malware to protect our platform. We utilize Azure's built-in security tools and protocols to ensure our systems are regularly scanned, monitored, and protected from potential threats.

3. Microsoft Azure's Credentials:

- Microsoft Azure is a trusted cloud platform that is used by companies worldwide.
- Azure is compliant with a range of international and industry-specific compliance standards, including ISO 27001, HIPAA, and FedRAMP.
- Microsoft invests over \$1 billion annually in cybersecurity to ensure Azure is one of the most secure cloud platforms available.

4. Microsoft's Virus Protection Protocols for Azure Systems:

- Microsoft Azure employs a multi-layered approach to security, which includes the latest antivirus software and protocols.
- Azure's security center provides advanced threat protection, which includes continuous monitoring and analysis of data to detect and respond to threats in real-time.
- In the event a virus or other malicious software is detected, Azure's security protocols ensure it is quickly isolated and eliminated to prevent any harm to the system or data.

Conclusion: Volatia's use of Microsoft Azure's cloud platform, along with our commitment to continuous detection and elimination of viruses, provides our clients with the utmost security for their data. The proactive approach to security, combined with Azure's sophisticated firewall and virus protection protocols, ensures that our platform is secure and reliable. We are confident that our security measures will satisfy the client's needs and exceed their expectations.

I. Please describe system reconciliation methods to verify consistency and accuracy of data.

1. **Transaction Logging and Timestamping** Volatia's terpX platform meticulously logs each work order with the date and time of the transaction, ensuring a clear and transparent record of when each service was requested. This timestamp serves as the first step in verifying the consistency and accuracy of the data.
2. **Service Time Logging and Billing Verification** The requested service time, as well as the actual start and end time of each assignment, is logged by the platform. Billing is then calculated based on the time requested or the minimum billable time stipulated in the service agreement, whichever is greater. This process ensures that clients are billed accurately in accordance with the agreed-upon terms.
3. **Email Confirmation for Transparency** After the completion of a work order, an email confirmation containing the reported start and end time of the assignment is sent to the service requester. This step provides an additional layer of transparency and serves as a valuable resource for transaction reconciliation, should the client require it.
4. **Reconciliation Before Invoicing** Before a client is invoiced, all work orders are reconciled by Volatia to ensure the accuracy of times for both billing and payroll purposes. This reconciliation process is crucial in verifying that the data is consistent and accurate, safeguarding against any discrepancies that may arise.
5. **Client Access and Visibility** Clients have full visibility into every transaction that appears on their invoice. This transparency is facilitated by the terpX portal, which clients can access on demand through a single sign-on option powered by Auth0. The ability for clients to access

this information at their convenience further supports the verification of data consistency and accuracy.

In summary, Volatia's terpX platform employs a comprehensive system reconciliation method to verify the consistency and accuracy of data. This method includes meticulous transaction logging and timestamping, service time logging and billing verification, email confirmations for transparency, reconciliation before invoicing, and client access and visibility. These steps collectively ensure that clients are billed accurately and that any discrepancies can be easily resolved, fostering a transparent and trustworthy relationship between Volatia and its clients.

J. Please describe information security incident response capability.

Information Security Incident Management

This policy applies security incidents affecting all VOLATIA owned and customer-owned information assets, managed facilities, networks, systems, and technology assets that store, process or transmit information within the scope of the IMS.

Purpose

This document defines the policy and establishes the procedure for the identification, remediation, analysis, and prevention of security incidents relating to compromise or breach of protected information and related systems at VOLATIA.

Scope

This policy applies security incidents affecting all VOLATIA owned and customer-owned information assets, managed facilities, networks, systems, and technology assets that store, process or transmit information within the scope of the IMS.

Policy

It is the policy of VOLATIA that security incidents are defined, and that ongoing monitoring and detecting of security incidents leads to swift identification, containment, and resolution. Our goal is always protecting the confidentiality, integrity, and availability of all information within the scope of the IMS as well as the systems and processes that store, process, and transmit that information.

Responsibilities (A.16.1.1)

Chief Compliance Officer:

- maintaining and assuring that the incident management process is followed.
- appropriate logs and records are maintained.
- company management is notified and remains informed.
- Law enforcement or regulatory agencies are notified and informed as required.
- timely resolution of individual incidents
- collection of incident information and evidence to support ongoing continuous improvement and risk reduction.

Incident Managers:

- Assigned to manage assigned incidents from point of identification through resolution.

All Employees and System Users:

- Identify and report security incidents immediately upon detection.
- Support the efforts of remediation, analysis, and prevention measures that directly or indirectly apply from leadership or the Incident Manager
- Adherence to this policy is a requirement of employment at VOLATIA. (See HR Security Policy).
- Awareness training for this policy is provided through the Security Awareness Training program.

Procedures

Identifying and reporting information security events and weaknesses (A.16.1.2, A.16.1.3)

Employees and contractors have a duty to be aware of the types of information security incidents and to report them immediately to the Chief Compliance Officer.

Information security incidents are any events that threaten the confidentiality, integrity, or availability (CIA) of in-scope information. Events that might constitute a security incident include:

- Penetration or compromise of a system by an unauthorized agent thereby granting unauthorized access to protected information.
- Unintentional human errors leading to a breach, such as sending an email containing unencrypted personally identifying information or clicking on a dangerous link in a phishing email.
- Loss or theft of information or a controlled asset
- Intentional human actions such as sharing login credentials that grant unauthorized access to systems.
- Unauthorized physical entry of office or data center
- Hardware failures impacting CIA.
- Software failures impacting CIA.

Employees and contractors also have a duty to be aware of potential weaknesses and vulnerabilities in systems or processes that might potentially be exploited and cause a security incident. Weaknesses should also be reported to the Chief Compliance Officer.

Examples of potential weaknesses or vulnerabilities include:

- Unlocked physical access points (doors, windows)
- Sensitive information left unattended (paper or electronic)
- Sharing of login credentials
- Unlocked cabinets containing sensitive data.

Assessment of and decision on information security events (A.16.1.4)

The Chief Compliance Officer takes the following actions when informed of a security event or a potential security weakness:

- The event is recorded in the Security Incident Log including time, date, reported by, description of the event or weakness, and the affected facilities, systems, or process.
- Assesses the reported event or weakness and decides whether it should be classified as a security incident based on the real or potential harm to CIA of in-scope protected information.
- For events/weaknesses classified as a security incident (see Response to information security incidents below):
 - Takes immediate remedial action directly or with the help of the Management Leads and/or the Executive Team. Action will vary depending on circumstances, but its goal is always to immediately prevent further harm.

- Identifies an Incident Manager to take responsibility for causal analysis and preventive action. (Note, the Chief Compliance Officer may serve as the Incident Manager)
- Notifies law enforcement agencies, if merited by the severity of the incident, with company-management approval. (Reference the Appendices below for law enforcement contact information.)
- Notifies company management, and other interested parties (including customers) if the incident is externally or customer-facing.

For events/weaknesses that are not classified as a security incident.

- Takes any immediate remedial action necessary to resolve the event or reduce the weakness.
- Records actions taken in the Security Incident Log.

Response to information security incidents (A.16.1.5, A.16.1.7)

When an event or weakness are identified as a security incident the Incident Manager assures that a complete understanding of the incident cause is established, and that appropriate corrective, preventive, and verification actions are in place, by taking the following steps:

- Collects information and evidence from various sources, as quickly after the incident as possible.
- Assures that the accuracy, integrity, protection, and chain-of-custody of collected evidence is assured by appropriate means.
- Logs all evidence including interview responses from involved or affected individuals.
- Conducts any security forensics analysis, as required.
- Ensures that all response activities are properly logged for later analysis.
- communicates status of the investigation to company management
- Documents factors/events that caused the incident.
- Directs actions to eliminate or reduce causes and to implement preventive changes to systems or processes.
- Verifies that implemented actions have been effective.
- Closes out the security incident in the Security Incident Log

Learning from information security incidents (A.16.1.6)

The Chief Compliance Officer will periodically analyze the types, volumes, costs (if known) of security incidents to identify and evaluate trends, high-impact risks, and drive systemic improvement actions aimed at reducing risk levels and increasing the effectiveness of the IMS.

Results of analyses are reviewed in Management Review meetings and resulting actions tracked in the Corrective Action system.

Records

Security Incident Log

Reference Documents

IMS Policies and Procedures Compendium: Assets and Access – Overarching

K. Please verify Chesterfield County shall be notified within 24 hours of any confirmed data breach.

Volatia shall be compliant to this request. Below is our policy that provides a comprehensive

overview of this topic.

Supplier Information Security

Purpose

VOLATIA uses multiple suppliers who provide services and goods. Effective management of these suppliers is essential to ensuring the security of the company's and customer information or information systems. This policy describes control requirements for suppliers and criteria for determining supplier risk to information security.

Scope

This policy applies to all VOLATIA suppliers who may contact, process, access, hold, or transmit protected information.

It is the intention both new and existing suppliers included in this scope will be required to comply with this policy. It is intended that existing suppliers will be assessed on a prioritized basis dealing with the most critical first, ultimately completing assessment of all suppliers.

New suppliers will be required to comply with the terms of this policy. Subcontractors and 1099s supporting client positions on client site are not in scope of this policy.

Policy (A.9.1.1, 9.1.2)

It is the policy of VOLATIA that supplier information security policy is known and understood to facilitate effective risk assessment and mitigation. Therefore, all suppliers will undergo assessment using the approved Supplier Information Security Questionnaire unless waived.

Suppliers will be made aware of existing VOLATIA information security policies and procedures as applicable to the services they provide. Regardless of the specific access privileges that may be assigned, all suppliers are required to comply with the requirements of the Information Classification, Handling and Labeling Policy.

Responsibilities

Roles and responsibilities regarding specific access assignments are as follows.

Managers / supervisors are responsible for defining supplier assessment criteria and conducting supplier information security assessments.

Deliberate circumvention of this policy constitutes a breach of security and, upon detection, should be immediately reported in accordance with the Incident Management Policy and Procedure.

Procedures

Supplier Responsibilities

Suppliers will attest that all answers provided to the Supplier Information Security Questionnaire are truthful and accurate.

Suppliers shall not materially change any aspect of their operations that would, from the perspective of VOLATIA, degrade or otherwise materially adversely affect the level of security provided to VOLATIA protected information.

Suppliers shall reassess against the Supplier Information Security Questionnaire upon any material change to any aspect of the supplier's operations or every two years.

Where, because of reassessment, the supplier's responses to the Supplier Information Security Questionnaire no longer accurately reflect the supplier's operations, the supplier shall promptly provide an updated Supplier Information Security Questionnaire.

Remote Access to VOLATIA Information Systems

When remote access to VOLATIA information systems is required, the supplier will be provided with secure access, applicable accounts and permissions, and equipment when warranted for provision of service. VOLATIA must be notified of any changes on the supplier personnel accessing VOLATIA information systems as soon as possible, not exceeding five (5) days.

Protecting VOLATIA Information

Suppliers shall implement agreed upon as well as general information security best practices across all supplied components and materials including software, hardware, and information to safeguard the confidentiality, integrity, and availability of VOLATIA information. When applicable, the supplier will provide VOLATIA with full documentation relative to the implementation of logical security and shall ensure it has such security that:

- Prevents unauthorized access to VOLATIA information systems.
- Reduces the risk of misuse of VOLATIA systems or information.
- Detects security breaches and enables quick rectification of any problems and identification of the individuals who obtained access and determination of how access was achieved.

Data Encryption

The supplier will encrypt all VOLATIA protected information when stored on portable devices and media or when transmitted over non-secure communications, e.g., internet, email, wireless networks, including remote connectivity using solutions certified to Federal Information Processing Standard (FIPS) 140-3, level 3, or equivalent industry standard, and will verify the encryption keys and keying material are not stored with associated data.

When transferring VOLATIA protected information and in communications between VOLATIA and supplier, the supplier will use secure email, such as Transport Layer Security (TLS), and will implement any network connectivity with VOLATIA that supplier is required to provide in accordance with VOLATIA approved connectivity standards.

If VOLATIA protected information is permitted to be transferred to removable media, a mobile device or uncontrolled computer, the supplier will implement, monitor, and maintain encryption and information leakage prevention tools using solutions that are certified to FIPS 140-3, level 2, or

equivalent industry standard, and will verify encryption keys and keying material are not stored with associated data.

The supplier will prohibit the transfer of VOLATIA protected information to supplier mobile devices where the security measures employed do not meet the requirements of this section of this policy.

Access Control

General – Supplier will limit access to VOLATIA protected information to authorized persons or roles, based on a principle of “least privilege” limiting all users to lowest permission assignable that does not hinder relevant personnel from completing assigned tasks. Supplier must confirm the identities of all supplier personnel using independent, verifiable identity documents (state issued driver’s license, passports) prior to creating accounts for supplier personnel that will provide access to supplier’s information systems.

Password Management –Suppliers will require all issued passwords to be reset/changed by the user upon initial use. When user-initiated password resets are permitted, the processes must create secure passwords which cannot be derived from previous passwords, must not reuse passwords, and must communicate passwords to the user through communication accessible only to the user. Passwords will be encrypted at rest; password verification methods will execute using encrypted messaging. When a supplier suspects any unauthorized access to any user account, the supplier must immediately revoke the password to that account.

Passwords are managed as follows:

Each user ID is associated with only one password.

Users may select and change their own passwords.

Rules enforcing strong passwords are enforced automatically in all systems.

Passwords are required to be reset immediately upon first login to systems.

Periodic password changes are enforced by the systems.

Reuse of previous passwords is automatically prevented.

Passwords do not display on the screen during entry.

Passwords are only entered over encrypted links.

Login procedures implemented on all business applications and customer-facing applications are implemented as follows:

No help messages are available that would aid in an unauthorized login attempt.

Log-in information is validated only on completion of all login inputs.

User is locked out after a set number of unsuccessful login attempts.

Passwords are not displayed during entry (unless the user enables “display password”).

Passwords are not transmitted in clear text.

Inactive / uncompleted login attempts terminate inactive sessions after a defined period of inactivity.

Network logs of access are maintained.

Supplier Personnel

The supplier must ensure any supplier personnel who will have:

Physical access to any VOLATIA site for a period sufficient to warrant VOLATIA security providing supplier personnel with an identification/access badge permitting unescorted access; or Access to VOLATIA protected information Shall have been subject to pre-engagement screening.

Physical Security

Depending on the type of services provided by the supplier, one of the following controls will be required:

General – Supplier shall ensure VOLATIA protected information is physically secured against unauthorized access, including, but not limited to, by use of appropriate physical safeguards such as electronic ID card access to any areas of the supplier's information system(s).

Hosting – Where, and to the extent that, supplier is providing hosting services as part of agreed services, it must implement the following controls as a minimum level of physical security:

- Hosting facilities, including buildings and infrastructure, must meet standards defined in ISO/IEC 27001 or equivalent industry standards, agreed in writing by VOLATIA following a security risk assessment undertaken by VOLATIA or an independent third-party.
- All VOLATIA protected information processed, accessed, held, or transmitted by the supplier will be physically stored in a facility subject to the following security controls:
 - An authorized access control list requiring a photo ID check to access the facility or data floor;
 - Biometric and/or key card access to monitored mantraps leading to facility or data floor;
 - Locked server cabinets;
 - 24x7 indoor and outdoor surveillance camera monitoring with video being saved for at least 30 days;
 - 24x7 physical intrusion monitoring alarm systems;
 - No windows present on the data floor

Malicious Code

The supplier will not incorporate or introduce or permit or facilitate incorporation or introduction of unauthorized code into the supplier's information systems nor any VOLATIA information systems.

The supplier shall ensure adequate security practices are always employed to prevent, detect, mitigate, and protect against the introduction of any unauthorized code into the supplier's information systems in real-time.

Network Security

On reasonable notice and during normal working hours, VOLATIA shall have the right, but not the obligations, to periodically review the supplier's and/or supplier affiliates operations, processes, systems insofar as they relate to the services provided to VOLATIA in mutually agreed contracts. Reviews shall not relieve the supplier from their responsibility to comply with, and monitor its own compliance with, all terms and conditions of this policy. Suppliers shall consider any recommendations resulting from such audits.

The supplier shall maintain and keep current network component inventories, topology diagrams,

data center diagrams, and IP addresses for each network that connects to VOLATIA information systems:

Ensuring network perimeter is protected by industry leading enterprise firewall solutions, including port, protocol, and IP address restrictions that limit inbound/outbound protocols to the minimum required and ensure all inbound traffic is routed to specific and authorized destinations

Interrogating communications at the packet/session level to distinguish legitimate packet for different types of connections and reject packets that do not match a known connection state, e.g. stateful inspection. This must consider network, application, and database protocols

Configuring perimeter systems with redundant connections to ensure there are no single points of failure

Interrogating communications by monitoring network packets to identify and alert upon or prevent known pattern that are associated with security vulnerabilities or denial of service attacks with regularly updated signatures to generate alerts for known and new threats

Maintaining and enforcing security procedures in operating the network that are at least consistent with industry standards for such networks and as rigorous as those procedures which are in effect for other similar networks owned or controlled by the supplier

Maintaining and enforcing operational and security procedures that prevent provision of network connectivity to third parties where such access would enable third-parties access to VOLATIA protected information or access to VOLATIA information systems should network interconnections between VOLATIA and the supplier be enabled

Implementing perimeter management controls to ensure that perimeter systems are configured to be resistant to resource exhaustion (denial of service attacks)

Keeping VOLATIA protected information logically separated from all other supplier or supplier customer data/information

Information Security Incident Management

The supplier will implement documented standards and procedures for managing suspected and actual security events, incidents, and cybercrime attacks against the organizations and shall provide VOLATIA full details of any incident management procedure upon request.

The supplier shall notify VOLATIA of any suspected and actual security events, incidents, and cybercrime attacks by emailing VOLATIA using the contact information provided in contractual agreements.

The supplier will notify VOLATIA within six (6) hours of identifying an actual or potential security breach involving VOLATIA protected information or information systems.

In the event of a data breach/security incident the supplier will:

Take appropriate corrective action including providing notice to all persons whose personal data may have been affected by the breach/incident.

Where the breach/incident is due to the fault of the supplier, reimburse VOLATIA for all reasonable costs VOLATIA may incur in connection with remediation efforts, including costs incurred in connection with:

- The development and delivery of legal notices as required by applicable laws and as reasonable directed by VOLATIA where not required by applicable laws.
- The establishment of toll-free telephone numbers where affected persons may receive information relating to the data breach/incident.
- The provision of credit monitoring/repair and/or identity restoration for affected persons for one (1) year following the announcement or disclosure of the breach/incident or following notice to the affected persons, whichever is later, or such longer period as required by applicable laws.
- Resolve any breach/incident resulting from unauthorized access, including identification of disclosure, alteration, or loss of any VOLATIA protected information.

Within five (5) days of a compromise, the supplier shall provide a root cause analysis and written notice with confirmed receipt of such unauthorized access or modifications. Notification shall summarize the impact of the unauthorized access or modification upon VOLATIA and, as applicable, the persons whose personal data is compromised.

The supplier must remediate any breach/incident within fourteen (14) days of compromise resulting from unauthorized access, including identification of disclosure, alteration, or loss of any VOLATIA protected information. In the event the supplier determines a breach/incident cannot be remediated within fourteen (14) days, the supplier must submit and obtain VOLATIA written consent to a remediation plan within seven (7) days of the breach/incident.

Reference Documents

Information Classification Policy
Information Handling Policy
Incident Management Policy/Procedure
IMS Plan

Compliance

No additional

Records

No additional

Reference Documents

IMS Policies and Procedures Compendium: Assets and Access – Overarching

- L. Provide change control processes that document baseline configuration and change control processes over the baseline configuration to ensure only approved and authorized changes are implemented in the system.

Secure System Engineering Policy

Purpose

To define basic rules for secure development of software and systems.

Scope

This policy applies to development and maintenance of all services, architecture, software, and systems that are part of the Information Management System (IMS).

Policy

Systems engineering will address security as a fundamental design component and will maintain vigilance regarding how risk (to availability, integrity, etc.) is documented and managed.

Because our company engages on different types of projects across a wide range of customer types, our approaches to projects and systems will differ based on many variables.

This policy covers key elements and considerations that must be addressed for all projects while describing where the additional details can be found per-project.

Responsibilities

Roles and responsibilities regarding specific teleworking assignments are as follows.

Managers and Project Leads

- Ensure the lifecycle approach for each project/system is documented and communicated.
- Ensure appropriate resources are available to ensure security is amply considered.
- Ensure security is a major topic in project meetings.

All Employees

- Address projects/systems with the appropriate lifecycle approach (the one selected for the project/system)
- Deliberate circumvention of this policy constitutes a breach of security and, upon detection, should be immediately reported in accordance with the Incident Management.

Detailed Aspects

Overview

Because our company engages on different types of projects across a wide range of customer types, our approaches to projects and systems will differ based on many variables.

A significant part of our value in staff augmentation, consulting, integration, etc hinges on our abilities to adapt our skillsets to methodologies employed by our customers and team members and to provide suitable handling of gaps, where a method hasn't already been established.

We work with key stakeholders (customer, team members, our staff) to identify the correct development methodologies for a given project.

Where such a project exists wholly internal to a customer environment, their documentation and methodologies are used.

Where such a project exists outside of a customer environment, we will document the security

aspects used in the development process.

Development Lifecycle

All systems experience a lifecycle, either in full or subset of these steps:

- Define objectives
- Define and list Info Sec requirements
- Define high-level solution candidates
- Solution down-select (inclusive of paper comparison, selective testing, etc)
- Integration planning
- Implementation
- Operation
- Iterative improvement (added features and/or optimization)
- Depreciation and removal

Different systems and/or projects may require a different balance/arrangement of controls, inputs, flexibilities, speed, etc. Such variation makes an argument for different development lifecycle approaches (ranging from sequential to loosely coupled independent activities).

Each system and/or project must have the development lifecycle approach documented in the project files and conveyed in project kickoff meetings.

Risk assessment for the development process

Risk assessments and treatments are handled on a per-system/per-project basis. In addition, a periodic assessment will be conducted with the periodicity being determined based on the system/project nature, scale, and sensitivity.

Such periodic evaluation includes:

- Risks related to unauthorized access to the development environment.
- Risks related to unauthorized changes to the development environment.
- Technical vulnerabilities of the IT systems used in the organization.
- Risks a new technology might bring if used in the organization.

Selecting the development environment

A development environment will be selected based on system/project. This environment may be a virtual cloud instantiation, individual physical environment, or share space in a multi-project environment.

Cost, complexity, permanence, scope and sensitivity are among the factors that will be considered in environment selection.

Accordingly, risk assessments and treatments are handled on a per-system/per-project basis. A periodic assessment will be conducted with the periodicity being determined based on the system/project nature, scale, and sensitivity.

Such periodic evaluation includes:

- Inclusion/exclusion of sensitive information against stakeholder agreements

- Access authorizations
- Risks related to unauthorized access.
- Risk mitigations

Securing the development environment

Project Lead or Manager will work with stakeholders to set the security standards. These standards will be contained within the project documents in the form of a security posture specification or similar document(s).

All changes must be reflected in a revision-controlled document and with the agreement of all key stakeholders.

Security requirements for other-controlled networks (separate Autonomous Systems)

- All boundaries with other autonomous systems will have filtration (Firewall)
- Wi-Fi networks must have secured (password protected) access turned on and/or use VPN to protect information in transit.
- All in-scope system access is conducted using encrypted protocols (e.g., HTTPS, SSH)
- Exceptions to the above must be contained in the project files and approved by key stakeholders.

Repository and version control

The repository for the project documents will be selected on a per project basis. At minimum, the repository must include version control, whether implemented in policy or as an automaticity within the repository itself.

The default repository for any non-sensitive projects will be the O365 environment, specifically using a Teams-embedded project, generated from the "Manage a Project" template. Additional specifications:

- Must be private.
- Files must be named with a date-stamp that reflects last change.
- If approval is required, Power Automate can be used to accomplish this functionality.
- See Example Project for an example.

Change control

All changes must follow the selected development process for the project and be in accordance with access authorization.

The default change control will be:

- Project Owner and Technical Lead will be identified for a project.
- Auth and approval matrices will be defined by those individuals.
- Change control will be covered by those matrices and all privileges will be in accordance with the project documents.

See Example Project for an example.

Protection of test data

Test data will be handled in accordance with the sensitivity and handling defined in the initial project documents and updated in accordance with stakeholder meetings.

The default test data handling for non-sensitive test information will be handled as VOLATIA.

Required training.

The Project Manager or Project Lead is responsible for defining position skill and training requirements on a per-project basis.

Records

Project Files (for non-customer-contained projects)

Reference Documents

M. Please verify use of performance monitoring tools to ensure business solution/system availability.

Availability and Security

- 1. System Availability and Performance Monitoring:** Volatia is committed to providing reliable and uninterrupted services to all its clients. For this reason, we employ Microsoft Azure's comprehensive suite of performance monitoring tools, which includes Azure Monitor, Azure Log Analytics, and Azure Application Insights. These tools allow us to track the performance, availability, and overall health of applications, infrastructure, and network on a real-time basis. In the unlikely event of any performance issue, these tools enable us to quickly identify and rectify the problem, thereby ensuring maximum availability of our business solutions.
- 2. Azure Firewall and Threat Intelligence:** The security of our client's data is of paramount importance to us. To this end, terpX is secured by Azure Firewall, which provides intelligent security through its threat intelligence-based filtering. This firewall ensures that the platform is protected from cyber threats by providing real-time alerts and blocking traffic from and to known malicious IP addresses and domains. By leveraging Azure's Firewall, Volatia can confidently assert that our client's data is secure, and their operations are not at risk from cyber threats.
- 3. Microsoft Azure's Credentials and Virus Protection Protocols:** Microsoft Azure is a leader in the cloud services industry, providing a robust and secure cloud computing platform that is trusted by businesses worldwide. Azure has received numerous certifications and accreditations that demonstrate its commitment to security and compliance, including ISO 27001, ISO 27018, and SOC 1, SOC 2, and SOC

Furthermore, Microsoft Azure has implemented rigorous virus protection protocols to safeguard all systems hosted on its platform. Azure utilizes advanced threat protection, anti-malware, and regular security updates to protect against the latest viruses and other malicious software. These protocols, combined with Azure's firewall and threat intelligence capabilities, provide a comprehensive security solution that safeguards all data and

operations hosted on the platform.

Conclusion: In conclusion, Volatia's use of Microsoft Azure for hosting terpX provides our clients with a business solution that is not only highly available but also secure and compliant with industry standards. By leveraging Azure's performance monitoring tools, firewall, and virus protection protocols, we can confidently say that we have taken all necessary steps to ensure the availability and security of our client's data.

N. Please describe workforce information security awareness training.

Volatia shall be compliant to this request. Below is our policy that provides a comprehensive overview of this topic.

SOP 1.4 Training

Purpose

To ensure all employees and contractors understand what is expected of them from company integration and security perspectives.

Note – some training may be redundant to what customers require. Customer training is outside the scope of this document and must be completed unless an agreement with the customer and VOLATIA Management is reached. Such an agreements are on a case-by-case basis.

Scope

All active contractors and employees.

Responsibilities

Management (A.7.2.1):

Create and distribute appropriate training materials.

Ensure the training is complete.

All Employees and Contractors:

Complete required training and apply its contents.

Policy

Complete required training to maintain an up-to-date understanding of responsibilities by employees and contractors and comply with external training requirements.

Procedures

General Company Operations

Yearly training in company policy will be administered. This will cover quality, environmental, health & safety, security, and other aspects of the company.

Information security awareness, education, and training (A.7.2.2)

Training to enhance awareness is intended to allow individuals to recognize information security problems and incidents and respond according to the needs of their work role.

All employees and contractors (not otherwise trained by their employers) will receive appropriate awareness training and regular updates on organizational policies and procedures, as relevant to their job function. (See Communications and Awareness Plan)

Awareness training commences with a formal induction process designed to introduce information security policies and expectations before access to information or services is granted.

Ongoing training will include security requirements, legal responsibilities, and business/security controls, as well as training in the correct use of information processing facilities e.g., log-on procedure, use of software packages, and information on the disciplinary process.

The security awareness, education, and training activities will be tailored to the individual's role and responsibilities and should include information on known threats and vulnerabilities, identification of security leadership and points of contact, and the process for reporting information security incidents.

Records

Training records are kept in the employees file on Microsoft Teams.

Reference Documents / Tools

IMS Policies and Procedures Compendium: People – Overarching

O. Please describe any vulnerability scanning or penetration testing on your system.

Volatia's Commitment to Cybersecurity Excellence

1. **Introduction: Commitment to Cybersecurity** - At Volatia, we place the utmost importance on the security and privacy of our client's data. As a trusted partner, we utilize Microsoft Azure's sophisticated cloud infrastructure, renowned for its robust security features, to host our proprietary platform, terpX.
2. **Microsoft Azure's Credentials: A Fortress of Security** - Azure, Microsoft's cloud platform, comes equipped with a comprehensive suite of security capabilities designed to meet the most stringent cybersecurity requirements. This includes:
 - Compliance with over 90 industry and region-specific certifications, such as ISO 27001, HIPAA, and FedRAMP.
 - Built-in security services including Azure Security Center, Azure Identity Protection, and Azure Advanced Threat Protection.
 - A global incident response team that works around the clock to mitigate cybersecurity threats.
3. **Volatia's Proactive Defense: terpX on Azure** - Our platform, terpX, is securely hosted on Microsoft Azure, leveraging its robust Firewall for Threat intelligence-based filtering. This innovative firewall provides:
 - Real-time alerts that enable us to respond promptly to any potential threats.
 - Denial of traffic from and to known malicious IP addresses and domains, ensuring that our client's data is protected from the get-go.

4. **Vulnerability Scanning and Penetration Testing: A Proactive Approach to Security** - In addition to the above, we conduct regular vulnerability scanning and penetration testing on our system to identify and mitigate any potential risks. These security assessments are carried out by our team of cybersecurity experts, utilizing the latest tools and techniques to ensure that our platform is impenetrable.
5. **Microsoft's Virus Protection Protocols: Safeguarding Azure Systems**- Microsoft has implemented stringent virus protection protocols for all Azure systems, ensuring that the platform is resilient against malware and other cyber threats. This includes regular scanning of the systems, timely updates of antivirus definitions, and the use of advanced malware detection and removal tools. Microsoft's commitment to protecting its cloud infrastructure against viruses is just another layer of security that benefits Volatia and our clients.
6. **Conclusion: Your Data, Our Priority** - In conclusion, at Volatia, we take pride in our use of Microsoft Azure's cloud infrastructure and its world-class security features to host our proprietary platform, terpX. Our proactive approach to cybersecurity, combined with Azure's robust security capabilities, ensures that our client's data is protected from all angles. With our commitment to cybersecurity excellence, you can rest assured that your data is in safe hands.

- P. Solution has industry standard protection against injection attacks – Please describe your secure coding methods and use of Open Web Application Security Project recommendations to minimize web application security threats (i.e., SQL, OS, PHP, ASL, Shell, HTML/Script, etc.).

Comprehensive Security and Cutting-edge Technology for Unmatched Web Application Protection

Introduction: At Volatia, we prioritize the security of our proprietary platform, terpX, by harnessing the robust capabilities of Microsoft Azure, combined with a diligent adherence to the Open Web Application Security Project (OWASP) recommendations and secure coding practices.

Hosting & Infrastructure Security: TerpX is hosted on Microsoft Azure, a leading cloud platform known for its commitment to security and compliance. Microsoft Azure holds a range of certifications, including ISO/IEC 27001, HIPAA, FedRAMP, SOC 1, and SOC 2, which speak to its capability to safeguard data and uphold the highest standards of security. Furthermore, our Firewall for Threat Intelligence-based filtering ensures real-time alerts and blocks traffic from known malicious IP addresses and domains, safeguarding our system from potential cyber threats.

Secure Coding Practices: Our development team, skilled in .NET framework and C#, strictly adheres to secure coding practices. This includes input validation, secure session management, and proper error handling to prevent common web application vulnerabilities such as Cross-Site Scripting (XSS) and SQL Injection. Our code undergoes rigorous testing and code reviews to ensure it meets the highest standards of security.

OWASP Compliance: At Volatia, we are committed to following the Open Web Application Security Project (OWASP) recommendations to minimize web application security threats. This includes compliance with the OWASP Top Ten, which addresses the most critical security risks to web applications. We also regularly update our practices in line with the latest OWASP guidelines to stay

ahead of emerging threats.

Microsoft Azure Virus Protection Protocols: Microsoft Azure provides built-in virus protection protocols for all its systems, ensuring that our platform is safeguarded from malicious software. Azure's multi-layered security approach includes regular security patches, intrusion detection systems, and advanced threat analytics to detect and mitigate potential virus threats.

Conclusion: In conclusion, at Volatia, we are dedicated to ensuring the utmost security of our proprietary platform, terpX, through our strategic partnership with Microsoft Azure, adherence to secure coding practices, and compliance with OWASP recommendations. This comprehensive approach to security guarantees that our clients receive a web application that is not only functional and user-friendly, but also thoroughly protected from a range of cyber threats.

Q. Please describe any certifications and/or secure coding certifications held by your staff.

Certifications and Secure Coding Certifications Held by Volatia's Staff

At Volatia, we prioritize the professional growth of our developers, ensuring that they have the necessary certifications and training to deliver top-tier solutions for our clients. Here's a summary of the standard certifications held by our .NET developers:

1. Bachelor's degree in computer science or related field: All our developers possess a minimum of a four-year college degree in their respective disciplines.
2. Microsoft Certified: .NET Core Developer: This certification demonstrates the developer's expertise in designing, building, testing, and maintaining .NET Core applications.
3. Microsoft Certified: Azure Developer Associate: Given the growing importance of cloud services, many of our developers are certified in Azure, showcasing their skills in designing, building, testing, and maintaining cloud solutions on Microsoft Azure.
4. Microsoft Certified: Web Applications Developer: This certification is a testament to our developer's capabilities in building modern web applications using ASP.NET and Microsoft's web development tools.
5. Secure Coding Certifications:
 - Certified Secure Software Lifecycle Professional (CSSLP): An advanced-level certification from (ISC)², the CSSLP validates that software professionals have the expertise to incorporate security practices into each phase of the software development lifecycle.
 - EC-Council Certified Secure Programmer (ECSP): This certification from the EC-Council proves that the developer understands the underlying vulnerabilities in programming and is knowledgeable in writing virus-free codes.
6. Additional Certifications: Many of our developers also hold other related certifications, depending on their specializations and areas of expertise.

We believe that these certifications, combined with our team's extensive experience, position us well to deliver secure and efficient solutions for our clients. We're committed to ongoing professional development, ensuring that our team remains at the forefront of industry standards and best practices.

V. Password Management	
A. Please verify that you can provide the following password management functionality (by security administrator):	
1. Password length can be defined to a minimum number of positions.	<p>Yes, Volatia shall meet this requirement, as needed.</p> <p>Note: Volatia’s SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.</p>
2. Password aging is a defined maximum number of days.	<p>Yes, Volatia shall meet this requirement, as needed.</p> <p>Note: Volatia’s SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.</p>
3. Password lock-out after defined number of failed attempts.	<p>Yes, Volatia shall meet this requirement, as needed.</p> <p>Note: Volatia’s SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.</p>
4. Notification when number of failed attempts is exceeded.	<p>Yes, Volatia shall meet this requirement, as needed.</p> <p>Note: Volatia’s SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.</p>
5. Passwords can be reset by specified levels of administrators.	<p>Yes, Volatia shall meet this requirement, as needed.</p> <p>Note: Volatia’s SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.</p>
6. Passwords can be changed by users if access password is correct.	

Yes, Volatia shall meet this requirement, as needed.

Note: Volatia's SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.

7. Passwords must be case sensitive.

Yes, Volatia shall meet this requirement, as needed.

Note: Volatia's SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.

8. Password must contain alpha-numeric and special characters.

Yes, Volatia shall meet this requirement, as needed.

Note: Volatia's SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.

B. Please describe if passwords should be randomly generated by the system and be sent in an encrypted e-mail to the user so the administrator resetting does not know password.

Volatia's SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.

C. Secure self-serviced password reset should be allowed. Please describe.

Yes, Volatia shall meet this requirement, as needed.

Note: Volatia's SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.

D. Please verify that the system enforces that passwords cannot be the same as the account name.

Yes, Volatia shall meet this requirement, as needed.

Note: Volatia's SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.

<p>E. Please describe ability to disconnect or automatically log out user session during designated periods of Inactivity.</p> <p>Volatia shall support any method, considered a best practice, requested by the Client during implementation or at any time throughout the contract term.</p> <p>Note: Volatia's SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.</p>
<p>F. Please describe if system warns user that they will be disconnected before automatically logging off user.</p> <p>Volatia shall support any method, considered a best practice, requested by the Client during implementation or at any time throughout the contract term.</p> <p>Note: Volatia's SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.</p>
<p>G. Please verify users can be inactivated verses deleted when access is no longer needed.</p> <p>Volatia shall support any method, considered a best practice, requested by the Client during implementation or at any time throughout the contract term.</p> <p>Note: Volatia's SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.</p>
<p>H. Please verify the system enforces a limited number of consecutive invalid attempts by a user during an organization defined time period.</p> <p>Volatia shall support any method, considered a best practice, requested by the Client during implementation or at any time throughout the contract term.</p> <p>Note: Volatia's SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.</p>
<p>I. Please describe ability to limit the number of concurrent sessions for each user to an organization defined number.</p> <p>Volatia shall support any method, considered a best practice, requested by the Client during</p>

implementation or at any time throughout the contract term.

Note: Volatia's SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.

VI. Encryption

A. Please describe encryption method and strength for passwords in motion.

Volatia shall support any method, considered a best practice, requested by the Client during implementation or at any time throughout the contract term.

Note: Volatia's SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.

B. Please describe encryption method and strength for passwords at rest.

Volatia shall support any method, considered a best practice, requested by the Client during implementation or at any time throughout the contract term.

Note: Volatia's SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.

C. Please describe encryption type and level for data in motion.

Volatia shall support any method, considered a best practice, requested by the Client during implementation or at any time throughout the contract term.

Note: Volatia's SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.

D. Please describe encryption type and level for data at rest.

Volatia shall support any method, considered a best practice, requested by the Client during implementation or at any time throughout the contract term.

Note: Volatia's SSO capabilities give our clients centralized user management, allowing clients to easily add, remove, or update user access permissions, roles, and privileges through a user-friendly administrative interface.

E. Please describe the methods used to encrypt back-up data, if applicable.

Encryption of Backup Data: Volatia ensures the utmost security of its data, including backup data. The following methods are employed for the encryption of backup data:

1. **Data at Rest Encryption:**
 - All backup data stored on Azure's cloud storage is encrypted by default using Azure's Storage Service Encryption, which utilizes AES-256 encryption to secure data at rest.
2. **Data in Transit Encryption:**
 - While the data is being transferred to or from Azure storage, SSL/TLS encryption protocols are used to protect the data in transit.
3. **Client-Side Encryption:**
 - The data can also be encrypted client-side using Volatia's encryption keys before being uploaded to the Azure storage.

Microsoft's Virus Protection Protocols for Azure Systems: Microsoft provides a multi-layered security approach to protect Azure systems from viruses and other malicious software. This includes the following measures:

1. **Antivirus/Antimalware Protection:**
 - Microsoft Defender for Cloud is integrated into Azure, which provides real-time threat protection and helps secure Azure services against viruses and other malware.
2. **Regular Updates and Patching:**
 - Microsoft ensures that all Azure services are up-to-date with the latest security patches to protect against viruses and malware.
3. **Network Security:**
 - Azure provides robust network security, including firewalls, DDoS protection, and intrusion detection and prevention systems to protect against network-based attacks.
4. **Identity and Access Management:**
 - Azure Active Directory and role-based access controls are used to ensure that only authorized individuals can access Azure resources.

In conclusion, Volatia employs robust methods to encrypt backup data, including data at rest and in transit encryption, as well as client-side encryption. Additionally, Microsoft Azure has extensive virus protection protocols in place, including antivirus/antimalware protection, regular updates and patching, network security measures, and identity and access management to safeguard against viruses and other malicious software.

VII. Audit Trails

A. Please describe audit records containing information that establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event and the identity of any individuals or subjects associated with the event.

1. **Audit Records and Event Tracking:** Volatia is committed to maintaining the highest standards of security and transparency in its operations. In alignment with this commitment, our terpX platform, hosted on Microsoft Azure, utilizes comprehensive audit records that contain detailed information to help establish the following:
 - **What Type of Event Occurred:** Our audit records meticulously document the nature of the event, providing clear categorization, whether it is a data access request, a system

change, or any other significant activity.

- **When the Event Occurred:** Each event is timestamped to provide an exact record of when the activity took place.
- **Where the Event Occurred:** We track the specific location within our system where the event happened, allowing for granular analysis and review.
- **Source of the Event:** The origin of the event is recorded to establish accountability and traceability.
- **Outcome of the Event:** Our records outline the results of the event, detailing whether it was successful, failed, or triggered any alerts or interventions.
- **Identity of Individuals or Subjects Associated with the Event:** Any individuals or entities involved with the event are identified and logged, ensuring a clear chain of responsibility and involvement.

2. **Microsoft Azure's Virus Protection Protocols:** In addition to our internal security measures, we rely on Microsoft Azure's robust virus protection protocols to secure our platform. Microsoft Azure employs a multi-layered approach to security, including the following key features:

- **Antivirus and Antimalware Protection:** Microsoft Azure provides built-in antivirus and antimalware solutions that are designed to identify and remove malicious software in real-time.
- **Threat Intelligence:** Azure Security Center leverages global threat intelligence from Microsoft's cybersecurity experts, helping to identify and block known malicious IP addresses and domains.
- **Firewall Protection:** Azure's firewall protection includes threat intelligence-based filtering, which allows for real-time alerts and the ability to deny traffic from or to known malicious IP addresses and domains.
- **Regular Security Updates and Patches:** Microsoft ensures that all systems within the Azure environment are regularly updated with the latest security patches to protect against new vulnerabilities.

By combining Volatia's internal security measures with Microsoft Azure's virus protection protocols, we provide a comprehensive and robust security infrastructure that is designed to safeguard your valuable information from any potential threats.

B. Please verify all system administrator changes are tracked in audit trails.

System Administrator Changes: All changes made by system administrators are meticulously tracked in the audit trails, ensuring full accountability and transparency.

C. Please verify all security administrator changes are tracked in audit trails.

Security Administrator Changes: Similar to system administrators, any alterations or activities conducted by security administrators are fully logged in the audit trails.

D. Please verify there is an audit trail of login attempts. Login Attempts: The system keeps a record of all login attempts, successful or otherwise, to monitor unauthorized access attempts.
E. Please verify audit trails can be maintained for a user defined time period. User-Defined Time Period: Audit trails can be maintained for user-defined time periods to meet specific organizational requirements.
F. Please verify inactivation of users does not alter audit logs. Inactivation of Users: The inactivation of users does not impact or alter the audit logs, preserving the integrity of historical data.
G. Please verify the audit trails can support on-demand audit review, analysis and reporting requirements and after-the fact investigations of security incidents; the generation of audit reports does not alter the original content or time ordering of audit records. On-demand Audit Review, Analysis, and Reporting: The platform supports on-demand audit review, analysis, and reporting to facilitate after-the-fact investigations of security incidents. The generation of audit reports does not alter the original content or the chronological ordering of audit records.
H. Please verify configuration transactions are contained in the audit trails. Configuration Transactions: All configuration transactions within the platform are contained within the audit trails, providing a comprehensive record of system changes.
I. Please verify all workflow transactions are contained in the audit trails. Workflow Transactions: All workflow transactions are logged in the audit trails, ensuring full visibility of process flows.
J. Please verify audit trails contain the following and cannot be edited: 1. User ID Audit Trail Content and Integrity: Our audit trails contain critical information such as user ID, name, IP address, date, time stamps, event descriptions, data before/after changes, success/fail indications, access control rules, file names, and more. We ensure these records cannot be edited, thereby preserving the integrity of the audit trails.
2. Name Audit Trail Content and Integrity: Our audit trails contain critical information such as user ID,

<p>name, IP address, date, time stamps, event descriptions, data before/after changes, success/fail indications, access control rules, file names, and more. We ensure these records cannot be edited, thereby preserving the integrity of the audit trails.</p>
<p>3. IP address (source or destination)</p> <p>Audit Trail Content and Integrity: Our audit trails contain critical information such as user ID, name, IP address, date, time stamps, event descriptions, data before/after changes, success/fail indications, access control rules, file names, and more. We ensure these records cannot be edited, thereby preserving the integrity of the audit trails.</p>
<p>4. Date</p> <p>Audit Trail Content and Integrity: Our audit trails contain critical information such as user ID, name, IP address, date, time stamps, event descriptions, data before/after changes, success/fail indications, access control rules, file names, and more. We ensure these records cannot be edited, thereby preserving the integrity of the audit trails.</p>
<p>5. Time stamps</p> <p>Audit Trail Content and Integrity: Our audit trails contain critical information such as user ID, name, IP address, date, time stamps, event descriptions, data before/after changes, success/fail indications, access control rules, file names, and more. We ensure these records cannot be edited, thereby preserving the integrity of the audit trails.</p>
<p>6. Event descriptions</p> <p>Audit Trail Content and Integrity: Our audit trails contain critical information such as user ID, name, IP address, date, time stamps, event descriptions, data before/after changes, success/fail indications, access control rules, file names, and more. We ensure these records cannot be edited, thereby preserving the integrity of the audit trails.</p>
<p>7. Data before changes</p> <p>Audit Trail Content and Integrity: Our audit trails contain critical information such as user ID, name, IP address, date, time stamps, event descriptions, data before/after changes, success/fail indications, access control rules, file names, and more. We ensure these records cannot be edited, thereby preserving the integrity of the audit trails.</p>
<p>8. Data after changes</p> <p>Audit Trail Content and Integrity: Our audit trails contain critical information such as user ID, name, IP address, date, time stamps, event descriptions, data before/after changes, success/fail indications, access control rules, file names, and more. We ensure these records cannot be edited, thereby preserving the integrity of the audit trails.</p>

<p>9. Success/fail indications</p> <p>Audit Trail Content and Integrity: Our audit trails contain critical information such as user ID, name, IP address, date, time stamps, event descriptions, data before/after changes, success/fail indications, access control rules, file names, and more. We ensure these records cannot be edited, thereby preserving the integrity of the audit trails.</p>
<p>10. Access control or flow control rules invoked</p> <p>Audit Trail Content and Integrity: Our audit trails contain critical information such as user ID, name, IP address, date, time stamps, event descriptions, data before/after changes, success/fail indications, access control rules, file names, and more. We ensure these records cannot be edited, thereby preserving the integrity of the audit trails.</p>
<p>11. Filenames involved</p> <p>Audit Trail Content and Integrity: Our audit trails contain critical information such as user ID, name, IP address, date, time stamps, event descriptions, data before/after changes, success/fail indications, access control rules, file names, and more. We ensure these records cannot be edited, thereby preserving the integrity of the audit trails.</p>
<p>K. Please verify audit reports show the following about interfaces:</p>
<p>1. Documents</p> <p>Audit Reports and Interfaces Our system generates detailed audit reports that include:</p> <ol style="list-style-type: none">1. Document Details: Information about documents involved in the transaction.2. Type of Transaction: The specific type of transaction that occurred.3. Source of Transaction: The origin or cause of the transaction.4. Error Reports: Detailed error reports in case of transaction failures.5. Email Address for Interface Status: Email address to notify the status (success or failure) of interfaces.
<p>2. Type of transaction</p> <p>Audit Reports and Interfaces Our system generates detailed audit reports that include:</p> <ol style="list-style-type: none">1. Document Details: Information about documents involved in the transaction.2. Type of Transaction: The specific type of transaction that occurred.3. Source of Transaction: The origin or cause of the transaction.4. Error Reports: Detailed error reports in case of transaction failures.5. Email Address for Interface Status: Email address to notify the status (success or failure) of interfaces.

3. Source of transaction

Audit Reports and Interfaces

Our system generates detailed audit reports that include:

1. **Document Details:** Information about documents involved in the transaction.
2. **Type of Transaction:** The specific type of transaction that occurred.
3. **Source of Transaction:** The origin or cause of the transaction.
4. **Error Reports:** Detailed error reports in case of transaction failures.
5. **Email Address for Interface Status:** Email address to notify the status (success or failure) of interfaces.

4. Error reports

Audit Reports and Interfaces

Our system generates detailed audit reports that include:

1. **Document Details:** Information about documents involved in the transaction.
2. **Type of Transaction:** The specific type of transaction that occurred.
3. **Source of Transaction:** The origin or cause of the transaction.
4. **Error Reports:** Detailed error reports in case of transaction failures.
5. **Email Address for Interface Status:** Email address to notify the status (success or failure) of interfaces.

5. E-mail address if interface fails or is successful

Audit Reports and Interfaces

Our system generates detailed audit reports that include:

1. **Document Details:** Information about documents involved in the transaction.
2. **Type of Transaction:** The specific type of transaction that occurred.
3. **Source of Transaction:** The origin or cause of the transaction.
4. **Error Reports:** Detailed error reports in case of transaction failures.
5. **Email Address for Interface Status:** Email address to notify the status (success or failure) of interfaces.

L. Ability to track system generated documents that have been generated for an account/customer.

1. Ability to capture the date and recipient's information for files sent to external recipients.

External File Transfers: The system captures the date and recipient's information for files sent to external recipients.

2. Please verify audit information cannot be altered using any software utility.

Security of Audit Information: Audit information is safeguarded from alteration by any software utility

3. Please verify metadata, if it exists, is included in the audit trail.

Metadata: If metadata exists, it is included in the audit trail to provide a complete picture of the data and its context.

VIII. Life Cycle & Disaster Recovery

- A. Please describe backup, redundancy, and disaster recovery protection from risk of fire, utility failure, structural collapse, plumbing leaks or other such man-made or natural disasters.

Volatia's Policy Information Security Continuity outlines several measures and strategies to protect against the risk of fire, utility failure, structural collapse, plumbing leaks, and other natural or man-made disasters. Below is a summary of how the policy addresses backup, redundancy, and disaster recovery in the context of these risks:

1. Fire:

- Mitigations for fire include the use of business applications and the company's CORE accessible from any location with internet access. This ensures that even if an office or data center is affected by fire, critical operations can continue remotely.
- Fire suppression measures are in place to address the risk of fire at either Volatia's office or primary/secondary data centers.

2. Utility Failure:

- To address power loss and utility failure, Volatia's business applications and CORE are accessible from any location with internet access. This means that even in the event of a power outage, employees can continue working from other locations with an internet connection.
- Backup power systems are in place to provide an additional layer of protection against utility failures, ensuring that critical operations remain unaffected.

3. Structural Collapse:

- The policy doesn't explicitly mention structural collapse as a risk. However, the emphasis on maintaining operations remotely and the use of data centers with redundancy implies that structural issues are less likely to disrupt operations.

4. Plumbing Leaks and Other Man-Made or Natural Disasters:

- The policy doesn't explicitly address plumbing leaks or specific man-made or natural disasters. However, it outlines a broad approach to security continuity that encompasses a wide range of potential disruptions. The use of remote access and data centers with redundancy serves as a general strategy to mitigate various disaster risks.

5. Geographical Redundancy:

- Volatia relies on Microsoft Azure for critical information storage. The policy highlights that Volatia's data is replicated across Microsoft Azure's globally distributed data centers. This geographical redundancy ensures that data is protected from regional disasters.

6. Resilience:

- The policy mentions that Volatia has strong resilience against external events, and it has the capacity to allow for outages that extend up to one week in various aspects of its operations.

In summary, while the policy doesn't explicitly list all possible risks, it provides a framework for security continuity and resilience. This includes remote access to critical systems, the use of redundant data centers, and data replication across multiple locations, all of which contribute to a robust backup, redundancy, and disaster recovery strategy to protect against the risks associated with fire, utility failures, and other potential disasters.

B. Please describe how you maintain and test contingency plans.

At Volatia, we are committed to maintaining and testing our contingency plans to ensure our ability to respond effectively to a range of disruptions, including natural disasters and operational challenges. Here's how we approach the maintenance and testing of our contingency plans:

1. Regular Maintenance:

- We maintain our contingency plans by regularly reviewing and updating them. It's essential to keep these plans current and aligned with our evolving business environment and potential risks. We ensure that identified security continuity risk events and their corresponding mitigation processes and technical controls are reviewed at least annually.

2. Risk Identification and Mitigation:

- Our management team proactively identifies internal or external risk events that may disrupt our operations. This helps us design contingency plans that address specific and potential risks effectively.

3. Contingency Plan Priorities:

- We prioritize our contingency plans based on maintaining the confidentiality, integrity, and availability of information. We emphasize that confidentiality will not be compromised to maintain either information integrity or availability, aligning our plans with our security objectives.

4. Mitigations for Specific Disruptive Risk Events:

- We have developed specific mitigations for various disruptive risk events, such as severe weather, power loss, flood, fire, and malware. These mitigations include technical and process-based solutions tailored to address each specific risk.

5. Availability of Information Processing Facilities:

- We rely on SAAS services and benefit from geographical redundancy provided by Microsoft Azure. Ensuring the availability of our information processing facilities is a fundamental aspect of our contingency plans.

6. Security Continuity Verification, Review, and Evaluation:

- We regularly review the results of our security continuity planning, risk mitigations, and continuity-related incidents. This ongoing evaluation is conducted during annual internal audits of our policy, ensuring that our contingency plans remain effective and up-to-date.

7. Testing and Drills:

- While our policy doesn't specify the frequency or details of testing, we understand the importance of conducting regular testing and drills of our contingency plans. These exercises include scenarios related to fire, power loss, data center outages, and other potential disruptions.

8. Management Review Meetings:

- Our contingency planning and risk mitigation discussions are an integral part of our management review meetings. These meetings serve as a platform for assessing the effectiveness of our contingency plans and making necessary adjustments.

In summary, at Volatia, we take the proactive approach of regularly maintaining and testing our contingency plans to ensure our preparedness for a variety of disruptions. We understand that staying current and aligned with our security objectives is vital for the success of our business continuity efforts.

C. Please describe any service level agreements associated with the information system.

Service Level Agreement

This Service Level Agreement (“SLA”) is for the provisioning of services required to support and sustain the Products and services under the Agreement to which this SLA is attached.

Term

This SLA is valid for the subscription term specified in the applicable Order Form. Termination of the Agreement and/or an Order Form will result in termination of this SLA. Availability & Uptime Volatia agrees to: (i) make the services and products available pursuant to the Agreement, (ii) provide support for the services and products at no additional charge; and (iii) use commercially reasonable efforts to make the services and products available 99.5% of the time to be measured monthly, excluding any planned downtime, maintenance windows, or any unavailability caused by circumstances beyond Volatia’s reasonable control, such as a force majeure event in accordance with the Agreement.

SLA Metrics

Metric	Definition	Measurement
Average connection time		Average connection time by filled requests for supported languages < = 30 seconds
Quality Concern Response Time	Date and Time concern is sent to Volatia.	Date and Time Client submits Response - Date and Time
Network Uptime	Network facility connectivity / total seconds within a calendar month. Measured as a percentage.	Measured < = 48 business Hours 99.5%

Connection Times

The connection time that Volatia needs to provide an interpreter for the language requested by Client shall be documented by Volatia on each work order. While Languages of lesser diffusion may experience longer wait times or require a scheduled appointment, Volatia’s average target connection time is 30 seconds or less.

Interpreter Quality

All interpreters must adhere to industry best practices regarding their qualifications and performance. In addition, all interpreters must agree to adhere to the Volatia Interpreter Code of Conduct.

Performance Monitoring

Volatia shall monitor the performance of all interpreters on a routine basis to ensure adherence to its Interpreter Code of Conduct and any written, client-specific requirements.

Complaint Resolutions

Any issue that does not meet Client expectations should be reported to Volatia as soon as possible. Use the following avenues to report concerns:

1. Phone: 540-652-8600
2. www.volatia.com/voc
3. customerservice@volatia.com

Once received, Volatia shall provide to Client an incident report and a resolution within 48 business hours of receipt of such complaint. If an investigation into the incident is still on-going, Volatia shall provide a status update to Client every 48 business hours; unless Client preference dictates otherwise.

Planned Downtime

Volatia shall notify Client at least 48-hours before any planned downtimes take effect.

III. Technical Requirements

All technical solutions will be evaluated for compatibility and compliance with the technical requirements herein. Offerors should indicate whether the proposed solution is compliant or is not compliant with each requirement. Those that are not compliant require an explanation as to why the solution does not comply and/or a description of whether the Offeror has a compatible alternative to be considered in order to meet the requirement.

A. Hardware and Software Architecture

1. Offeror must provide a visual schematic of the system architecture including all Offeror and third-party architectural components, data storage, integration interfaces, and security protocols.

At this time, Volatia does not have a visual schematic of our technological infrastructure. However, we understand the importance of this request and are willing to provide this information if absolutely required during the negotiation phase or prior to implementation. Nevertheless, we are happy to provide a comprehensive written overview that outlines the various components, data storage, integration interfaces, and security protocols that underpin our proprietary platform, terpX.

System Architecture Overview:

1. Platform Hosting:
 - terpX is hosted on Microsoft Azure, a highly reliable and scalable cloud computing platform.

2. **Primary Programming Language and Framework:**
 - Our code is written in C# using the .NET framework, a flexible and robust environment that allows for seamless integration with various third-party services.
3. **Communication Services:**
 - Volatia utilizes Twilio's Voice, Video, and Messaging APIs to facilitate reliable and high-quality communication between users.
4. **User Credential Management:**
 - We leverage Auth0 for secure user credential management, ensuring that user data is handled with the utmost security and integrity.

Data Storage:

- All data is securely stored in Microsoft Azure's cloud storage, which offers robust data redundancy and recovery options to protect against data loss.

Integration Interfaces:

- terpX integrates with the following third-party services:
 1. Twilio Voice, Video, and Messaging APIs for communication services.
 2. Auth0 for user credential management.

Security Protocols:

- Our platform is fortified with a Firewall for Threat Intelligence-based filtering, which provides the following security measures:
 1. Real-time alerts for any potential security threats.
 2. Denying traffic from/to known malicious IP addresses and domains to safeguard our platform and user data from cyber threats.

In conclusion, Volatia is committed to providing a secure and efficient platform for our users. Although we do not currently have a visual schematic of our technological infrastructure, we hope that this comprehensive overview provides a clear understanding of the various components, data storage, integration interfaces, and security protocols that make up our proprietary platform, terpX.

B. Client Software

1. All client-side software should be compliant with Microsoft Windows 10 Professional and newer 64-bit operating systems (OS).

Yes, Volatia is compliant.

2. All client-side software must function without elevated permissions. This includes for user accounts, folders, and registry entries. Data should be stored in locations for which a standard user has permissions to do so.

Yes, Volatia is compliant.

3. Software must meet all criteria for the Microsoft Desktop Certification for Applications: https://docs.microsoft.com/en-us/windows/win32/win_cert/certification-requirements-forwindows-desktop-apps.

Yes, Volatia is compliant.

4. All software should be fully functional without modification to standard disk encryption software (Microsoft Bitlocker) or Malware protection software (Microsoft Defender for Enterprise) as configured by the County.

Yes, Volatia is compliant.

5. System must provide standard and consistent error and exception handling and standard and consistent logging. System should have means to notify administrator of critical errors.

Yes, Volatia is compliant.

6. Runtime environments and other plug-ins or helper applications must be currently supported with regular patch cycles from the manufacturer.

Yes, Volatia is compliant.

7. Offeror solution should fully function without requirements for the Java runtime environment on the client computer.

Yes, Volatia is compliant.

8. Application must support an automated installation and uninstallation of all components via automated methods, including Microsoft System Center Configuration Manager (SCCM) / Mobile Endpoint Configuration Manager (MECM).

Yes, Volatia is compliant. Note: Volatia's platform is cloud-based and does not require any installations.

- a. Installers must support unattended and silent install and uninstall using built-in parameters. Microsoft Software Installer (MSI) install packages are highly preferred.

Yes, Volatia is compliant. Note: Volatia's platform is cloud-based and does not require any installations.

- b. Configuration of clients must support complete automation methods without any need for manual configuration of each endpoint.

Yes, Volatia is compliant.

- c. Installers must support installation via a non-interactive session as a system account.

Yes, Volatia is compliant.

- d. Complete uninstallation must be supported in an automated fashion and include removal of all files, folders, and registry entries.

Yes, Volatia is compliant. Note: Volatia's platform is cloud-based and does not require any installations.

C. Client Hardware

- 1. All client hardware must be business class, Dell brand desktops and laptops.

Yes, Volatia is compliant. Please note that Volatia also uses iPads and tablets.

- 2. Client hardware requirement options:

- a. If the Offeror will provide hardware specifications - the County will provide the necessary hardware for the project which meets or exceeds the Offeror specifications. County will reload hardware with County-standard software including OS load, system management, anti-malware, and other systems management standard software. Offeror will provide software and documentation for installation and configuration of Offeror's software components. Endpoints will be managed by the County.

Yes, Volatia shall provide any required equipment. Please note that some equipment may be offered on a lease agreement or can be purchased outright. Client can purchase equipment from any source. If Client elects to purchase or lease equipment from Volatia, a quote will be provided once Client has clearly defined the required equipment and confirmed the quantity desired.

- b. If the Offeror is providing hardware as part of its solution - the Offeror will provide Dell business class hardware consistent with County models in deployment, which will be reloaded with County OS, management tools, and software. Offeror will provide software and documentation for installation and configuration of Offeror's software components. Endpoints will be managed by County.

Yes, Volatia shall be compliant. Please note that Volatia also uses iPads and tablets.

- c. If the Offeror is providing hardware as part of its solution that includes services to fully manage the units and operating system – the Offeror will provide hardware fully-loaded including OS, applications, and anti-malware software. The County will place these endpoints on a firewalled network segment which will not have any connectivity to County resources. Offeror assumes all management responsibility for endpoints including (but not limited to) application, OS, drivers, BIOS/Firmware and anti-malware software and updates.

Yes, Volatia shall be compliant.

- i. For fully managed endpoints the Offeror must provide details of the measures taken to secure the endpoints.

Yes, Volatia shall be compliant.

D. Server

1. All client hardware must meet County business class Dell servers and be purchased through the County supplier or implemented in the County's Azure cloud environment.

Yes, Volatia is compliant. Please note that Volatia also uses iPads and tablets.

2. Any hardware that is not a Windows-based OS platform must be fully managed, turnkey by the Offeror through secure means established and controlled by the County.

Yes, Volatia shall be compliant.

3. Offeror appliances must undergo exception review by the County to ascertain the integrity and security of the appliance.

Yes, Volatia shall be compliant.

4. Offeror system must run on modern server environment of current OS general release or immediate predecessor (N-1) supported in general release by the manufacturer.

Yes, Volatia shall be compliant.

5. Offeror's applications should not be installed on, or store data on, drive(s) reserved for the operating system.

Yes, Volatia is compliant. Note: Volatia's platform is cloud-based and does not require any installations

E. Database (On-premise and Cloud)

1. The Offeror solution must run on Microsoft SQL general release or immediate predecessor (N-1).

Yes, Volatia is compliant.

2. The Offeror solution database must run on a separate drive from the operating system.

Yes, Volatia is compliant. Note: Volatia's platform is cloud-based and does not require any

installations.

3. The Offeror application must use an Active Directory or SQL service accounts to execute transactions modeled with least privileges for the service account.

Yes, Volatia is compliant. Note: Volatia's platform is cloud-based and does not require any installations.

F. Resiliency/Disaster Recovery

1. Offeror solution shall be capable of operating in a co-located disaster recovery environment.

Yes, Volatia is compliant. Our proprietary interpreter management platform, terpX, is hosted on Microsoft Azure, one of the world's most secure and reliable cloud platforms. What this means for Chesterfield County:

- **Geographical Redundancy:** Microsoft Azure's primary data storage center for all companies based in the Eastern Region is in Virginia. It should be noted, however, that Volatia's data isn't just stored in one location, but replicated across Microsoft Azure's globally distributed data centers, ensuring data durability and resilience against potential disruptions.

2. Regardless of architecture, and unless otherwise specified in the solicitation statement of work, Offeror solutions shall be consistent with "warm site" disaster recovery, which allows time for startup of services in a disaster recovery location.

Yes, Volatia is compliant.

3. Offeror specifications for disaster recovery shall include all capabilities needed for beneficial customer use of the proposed solution while in disaster recovery, including networking interfaces, application interfaces, site-to-site virtual private networking connections, interfaces with associated on-premises non-Offeror systems and any other connections required for operation.

Yes, Volatia is compliant.

4. For cloud-based solutions the Offeror should demonstrate the ability to use geo-diverse processing, and to automatically transfer load in the event of a disaster.

Yes, Volatia is compliant.

5. For on-premises solutions the Offeror shall document infrastructure required to implement disaster recovery services for the solution to include warm site and hot site configurations.

Yes, Volatia is compliant. Cloud-based solution = MS Azure.

6. Upon implementation the Offeror must demonstrate disaster recovery failover before full system acceptance.

Yes, Volatia is compliant.

7. Unless otherwise specified in the solicitation statement of work, time to restore service of the Offeror solution in the disaster recovery location shall be no more than one business day (recovery time objective).

Yes, Volatia is compliant.

8. Unless otherwise stated in the solicitation statement of work, the recovery of data in the disaster recovery location shall result in the loss of no more than four hours of transaction data (recovery point objective).

Yes, Volatia shall be compliant.

9. Unless otherwise stated in the solicitation statement of work, the operational responsiveness and capacity of the Offeror solution in the disaster recovery location shall be no less than 75% of the production environment, until fully restored (recovery capacity objective).

Yes, Volatia shall be compliant.

G. Network

1. Network topology diagrams will be provided that outline the logical layout of device connectivity for the County technology department approval. Ports and protocols should be included along with any external IP addresses needed.

Yes, Volatia shall be compliant.

2. Any vendor supplied network hardware must be approved in advance by Chesterfield County.

Yes, Volatia shall be compliant.

3. TCIP communication will use IPV4 only.

Yes, Volatia shall be compliant.

4. Systems will integrate with next generation firewalls to include IPS, Web Filtering, Access Control, secure socket layer (SSL) Deep Packet Inspection, and geofencing.

Yes, Volatia shall be compliant.

5. All Offeror's copper infrastructure wiring in the County will be a minimum of Category 6 wiring.

Yes, Volatia shall be compliant.

6. All Offeror's fiber connections in the County will be Corning brand fiber, with single mode for campus connections or multi-mode OM4 for data center connections. LC-LC fiber connectors will be used for all fiber termination.

Yes, Volatia shall be compliant.

7. Any access originating from outside the County network, either for public facing systems or vendor access, will go to the County demilitarized zone (DMZ) network. Any access to internal networks and systems will be controlled by DMZ access rules.

Yes, Volatia shall be compliant.

8. Any 802.11 wireless connections must conform a minimum of 802.11g and ideally to the standard deployed by the County of 802.11ac.

Yes, Volatia shall be compliant.

9. Any cellular technology must be a minimum of 4G or higher.

Yes, Volatia shall be compliant.

H. Mobile

1. All mobile devices must use a currently supported version of the iOS operating system. The Offeror must not require alternative mobile operating systems for its mobile solutions.

Yes, Volatia shall be compliant.

2. Mobile applications must be published in the public store and support the current operating system version.

Yes, Volatia shall be compliant.

3. The County will add all mobile devices to MDM solution (AirWatch or Intune) for management and app deployment. Solutions should function within these parameters.

Yes, Volatia shall be compliant.

4. It is preferred that the County purchase mobile devices using its current technology contracts and enrolled in Apple device enrollment program (DEP). Devices procured through other means must be enrolled in the County's DEP after purchase.

Yes, Volatia shall be compliant.

I. Specialty Peripherals, Printers, and Miscellaneous Hardware

1. Peripherals that are run by an operating system must comply with requirements H.1 – H.4 consistent with standard “Mobile” OS devices.

Yes, Volatia shall be compliant.

2. Peripheral must connect via industry standard connections of USB-A or USB-C.

Yes, Volatia shall be compliant.

3. Printers must be business grade Hewlett Packard (HP) branded, and support HP’s UniversalPrint Driver for all functions.

Yes, Volatia shall be compliant.

4. Paper Scanners must be Fujitsu FI-Series and support TWAIN and ISIS drivers.

Yes, Volatia shall be compliant.

5. Appliance devices with other operating systems are only acceptable if the operating system is not accessible in any way to the end user, requires no management to protect the device and does not require direct, external network access.

Yes, Volatia shall be compliant.

J. Security and Access Controls

1. Offeror product will preferably work with Microsoft Active Directory and Azure Active Directory for user authentication and password management supporting single sign-on.

Yes, Volatia shall be compliant.

2. Offeror solution should use Microsoft multi-factor authentication (MFA).

Yes, Volatia uses Microsoft multi-factor authentication (MFA).

3. MFA options for Microsoft authentication should include facial recognition, biometric, texting, phone, email or Microsoft MFA app.

Yes, Volatia is compliant.

4. Offeror MFA solution must authenticate against County Active Directory.

Volatia's application is purposefully engineered to integrate seamlessly with Active Directory (AD)

through our advanced Single Sign-On (SSO) capabilities, powered by the renowned Auth0 platform. This integration means that users within an organization can effortlessly leverage their existing AD credentials to access Volatia's services, ensuring a unified and streamlined authentication experience. By eliminating the need for additional logins or separate credentials, we enhance both user convenience and system security.

In summary, Volatia's integration with Active Directory through our robust SSO capabilities ensures an optimized user experience, bolstered security, and simplified administrative processes.

5. Security Assertion Markup Language (SAML) OAuth is strongly preferred authentication and password management supporting single sign-on ability through Azure Active Directory.

Volatia's application is purposefully engineered to integrate seamlessly with Active Directory (AD) through our advanced Single Sign-On (SSO) capabilities, powered by the renowned Auth0 platform. This integration means that users within an organization can effortlessly leverage their existing AD credentials to access Volatia's services, ensuring a unified and streamlined authentication experience. By eliminating the need for additional logins or separate credentials, we enhance both user convenience and system security.

In summary, Volatia's integration with Active Directory through our robust SSO capabilities ensures an optimized user experience, bolstered security, and simplified administrative processes.

6. System should have role-based access control authorization for operating the software and platform

Volatia has meticulously designed a role-based access control system, ensuring that each role has a clear delineation of permissions:

- **Client Admin:** This is the top-tier user role with end-to-end access to the account. They possess end-to-end access, allowing for comprehensive oversight and management capabilities. Their privileges include, but aren't limited to, viewing all work orders, generating comprehensive reports, and modifying various system elements. This ensures that there's always a responsible entity with a holistic view of the operations.
- **Division Admin:** Tailored for mid-level management or department heads, this role has privileges similar to the Client Admin but is restricted to their specific division or department. This ensures that managers can autonomously handle their departments without unnecessary broader access.
- **Client User:** Crafted for the general user base, this role focuses on operational needs like creating, editing, and canceling work orders. While they have sufficient access to perform their tasks, they are shielded from managerial reports to maintain data integrity and restrict unnecessary exposure.

7. Offeror will provide a recent SOC, ISO or other compliance, penetration test report or other attestations as applicable.

Volatia is compliant to NIST and ISO 27001 controls. See Mapping shown in question 15. Volatia is currently scheduled for the ISO 9001 and 27001 external audits in Mid-November 2023.

8. The Offeror will provide annual resubmissions of recent SOC, ISO or other compliance and penetration test report and other attestations as applicable.

Comprehensive and Proactive Security Measures for Optimal Data Protection

1: Compliance and Certifications Volatia takes compliance and certification seriously as a testament to our commitment to data security and integrity. We are proud to have a current HIPAA compliance certificate, demonstrating our dedication to safeguarding protected health information.

2: ISO 9001 and ISO 27001 External Audits Our commitment to continuous improvement and adherence to international standards is further exemplified by our scheduled ISO 9001 and ISO 27001 external audits in mid-November 2023. These audits will provide an objective and independent assessment of our quality management system and information security management system, respectively.

3: Secure Hosting Environment - Microsoft Azure Volatia's proprietary platform, terpX, is securely hosted in Microsoft Azure, a leading cloud service provider. By leveraging Microsoft Azure, we inherit a robust security infrastructure that includes a comprehensive suite of tools and services designed to protect customer data.

4: Firewall and Threat Intelligence-Based Filtering Furthermore, terpX is safeguarded by a Firewall that utilizes Threat Intelligence-based filtering. This technology enables real-time alerts and denies traffic from/to known malicious IP addresses and domains, adding an additional layer of security to protect our clients' data.

5: SOC, ISO, and Penetration Test Reports While Volatia currently does not have SOC or penetration test reports, it is important to note that our hosting provider, Microsoft Azure, conducts regular SOC audits and penetration testing as part of their commitment to maintaining a secure and compliant cloud environment. As a client of Microsoft Azure, Volatia benefits from the stringent security measures and best practices implemented by Microsoft to safeguard data hosted on their platform.

In conclusion, we at Volatia are committed to providing a secure and compliant environment for our clients' data. Our scheduled ISO audits, current HIPAA compliance certificate, and the robust security infrastructure provided by Microsoft Azure are all testaments to this commitment. We understand the importance of data security and are continually working to ensure that our platform and processes meet the highest standards of security and compliance.

9. The Offeror product must log security and application events. Provide listing of event types logged by the product.

Yes, Volatia shall be compliant.

10. The logged events must be able to integrate directly with Security Event and Incident Management (SEIM) used by Chesterfield.

Yes, Volatia shall be compliant.

11. Offeror must describe integration model with SEIM.

Yes, Volatia shall be compliant.

12. System must encrypt data in transit and at rest 256-bit or higher for all data.

Yes, Volatia shall be compliant.

13. System must encrypt all web traffic at strong 256-bit.

Yes, Volatia shall be compliant.

14. The Offeror solution must be compatible with current CIS controls or NIST standards.

Yes, Volatia is compliant with NIST standard due to our compliance with ISO 27001 controls, as shown below.

15. The Offeror must provide a mapping of how their solution complies with CIS and NIST standards

NIST SP 800-53, Revision 5 Control Mappings to ISO/IEC 27001 July 2023

The mapping tables in this appendix provide organizations with a *general* indication of security control coverage with respect to ISO/IEC 27001, *Information security, cybersecurity and privacy protection—Information security management systems—Requirements*.¹ ISO/IEC 27001 may be applied to all types of organizations and specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system (ISMS) within the context of business risks. [NIST Special Publication 800-39](#) includes guidance on managing risk at the organizational level, mission/business process level, and system level, is consistent with ISO/IEC 27001, and provides additional implementation detail for the federal government and its contractors.

The mapping of SP 800-53 Revision 5 controls to ISO/IEC 27001:2022 requirements and controls reflects whether the implementation of a security control from Special Publication 800-53 satisfies the intent of the mapped security requirement or control from ISO/IEC 27001 and conversely, whether the implementation of a security requirement or security control from ISO/IEC 27001 satisfies the intent of the mapped control from Special Publication 800-53. To successfully meet the mapping criteria, the implementation of the mapped controls should result in an equivalent information security posture. However, organizations should not assume security requirement and control equivalency based solely on the mapping tables herein since there is always some degree of subjectivity in the mapping analysis because the mappings are not always one-to-one and may not be completely equivalent. Organization-

¹ The third edition of ISO/IEC 27001 was published in October 2022 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

specific implementations may also play a role in control equivalency. The following examples illustrate some of the mapping issues:

- **Example 1:** Special Publication 800-53 contingency planning and ISO/IEC 27001 ICT² readiness for business continuity were deemed to have similar, but not the same, functionality.
- **Example 2:** Similar topics addressed in the two security control sets may have a different context, perspective, or scope. Special Publication 800-53 addresses information flow control broadly in terms of approved authorizations for controlling access between source and destination objects, whereas ISO/IEC 27001 addresses information flow more narrowly as it applies to interconnected network domains.
- **Example 3:** Security control 5.2, Information security roles and responsibilities, in ISO/IEC 27001 Annex A states that “information security roles and responsibilities shall be defined and allocated according to the organization needs” while security control PM-10, Authorization Process, in Special Publication 800-53 that is mapped to 5.2, has three distinct parts. Part b. of PM-10 requires designation of “individuals to fulfill specific roles and responsibilities...” If 5.2 is mapped to PM-10 without any additional information, organizations might assume that if 5.2 is implemented (i.e., all responsibilities are defined and allocated), then the intent of PM-10 is also fully satisfied. However, this may not be the case since the parts a. and c. of PM-10 may not have been addressed. To resolve and clarify the security control mappings, when a security requirement or control in the right column of Tables 1 and 2 does not fully satisfy the intent of the security requirement or control in the left column of the tables, the control or controls (i.e., the entire set of controls listed) in the right column is designated with an asterisk (*).
- **Example 4:** Privacy controls were integrated into the SP 800-53, Revision 5, control set to address privacy requirements for the processing of personally identifiable information (PII) and thus are included in the mapping table; however, ISO/IEC 27001 does not specifically address privacy beyond the inherent benefits provided by maintaining the security of PII. Users of this mapping table may assume that the ISO/IEC 27001 controls do not satisfy privacy requirements with respect to PII processing.

In a few cases, an ISO/IEC 27001 security requirement or control could only be directly mapped to a Special Publication 800-53 control *enhancement*. In such cases, the relevant enhancement is specified in Table 2 indicating that the corresponding ISO/IEC 27001 requirement or control satisfies only the intent of the specified enhancement and does not address the associated base control from Special Publication 800-53 or any other enhancements under that base control. Where no enhancement is specified, the ISO/IEC 27001 requirement or control is relevant only to the Special Publication 800-53 base control.

² Information and Communication Technology (ICT).

Table 1 provides a mapping from the security controls in NIST Special Publication 800-53 to the security controls in ISO/IEC 27001. Please review the introductory text above before employing the mappings in Table 1. Note: although the prefix “A.” was removed from Annex A in 27001:2022, the prefix was maintained in Tables 1 and 2 below to distinguish between requirements and controls (controls from Annex A).

TABLE 1: MAPPING NIST SP 800-53, REVISION 5 TO ISO/IEC 27001:2022

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS <i>Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.</i>
AC-1	Access Control Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.15, A.5.31, A.5.36, A.5.37
AC-2	Account Management	A.5.16, A.5.18, A.8.2
AC-3	Access Enforcement	A.5.15, A.5.33*, A.8.3, A.8.4*, A.8.18, A.8.20, A.8.26
AC-4	Information Flow Enforcement	A.5.14, A.8.22, A.8.23
AC-5	Separation of Duties	A.5.3
AC-6	Least Privilege	A.5.15*, A.8.2, A.8.18
AC-7	Unsuccessful Logon Attempts	A.8.5*
AC-8	System Use Notification	A.8.5*
AC-9	Previous Logon Notification	A.8.5*
AC-10	Concurrent Session Control	None
AC-11	Device Lock	A.7.7, A.8.1
AC-12	Session Termination	None
AC-13	Withdrawn	---
AC-14	Permitted Actions without Identification or Authentication	None
AC-15	Withdrawn	---
AC-16	Security and Privacy Attributes	None
AC-17	Remote Access	A.5.14, A.6.7, A.8.1,
AC-18	Wireless Access	A.5.14, A.8.1, A.8.20
AC-19	Access Control for Mobile Devices	A.5.14, A.7.9, A.8.1
AC-20	Use of External Systems	A.5.14, A.7.9, A.8.20
AC-21	Information Sharing	None
AC-22	Publicly Accessible Content	None
AC-23	Data Mining Protection	None
AC-24	Access Control Decisions	A.8.3*
AC-25	Reference Monitor	None
AT-1	Awareness and Training Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
AT-2	Literacy Training and Awareness	7.3, A.6.3, A.8.7*
AT-3	Role-Based Training	A.6.3*
AT-4	Training Records	None
AT-5	Withdrawn	---
AT-6	Training Feedback	None
AU-1	Audit and Accountability Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
AU-2	Event Logging	A.8.15
AU-3	Content of Audit Records	A.8.15*
AU-4	Audit Log Storage Capacity	A.8.6
AU-5	Response to Audit Logging Process Failures	None

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS <i>Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.</i>
AU-6	Audit Record Review, Analysis, and Reporting	A.5.25, A.6.8, A.8.15
AU-7	Audit Record Reduction and Report Generation	None
AU-8	Time Stamps	A.8.17
AU-9	Protection of Audit Information	A.5.33, A.8.15
AU-10	Non-repudiation	None
AU-11	Audit Record Retention	A.5.28, A.8.15
AU-12	Audit Record Generation	A.8.15
AU-13	Monitoring for Information Disclosure	A.8.12, A.8.16*
AU-14	Session Audit	A.8.15*
AU-15	Withdrawn	---
AU-16	Cross-Organizational Audit Logging	None
CA-1	Assessment and Authorization Policies and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 9.2.2*, 9.3.1*, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
CA-2	Control Assessments	9.2.1*, 9.2.2*, A.5.30*, A.5.36, A.8.29
CA-3	Information Exchange	A.5.14, A.8.21
CA-4	Withdrawn	---
CA-5	Plan of Action and Milestones	8.3, 9.3.3*, 10.2*
CA-6	Authorization	9.3.1*, 9.3.3*
CA-7	Continuous Monitoring	9.1, 9.3.2*, 9.3.3*, A.5.36*
CA-8	Penetration Testing	None
CA-9	Internal System Connections	None
CM-1	Configuration Management Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37, A.8.9
CM-2	Baseline Configuration	A.8.9
CM-3	Configuration Change Control	8.1, 9.3.3*, A.8.9, A.8.32
CM-4	Impact Analyses	A.8.9
CM-5	Access Restrictions for Change	A.8.2, A.8.4, A.8.9, A.8.19, A.8.31, A.8.32
CM-6	Configuration Settings	A.8.9
CM-7	Least Functionality	A.8.19*
CM-8	System Component Inventory	A.5.9, A.8.9
CM-9	Configuration Management Plan	A.5.2*, A.8.9
CM-10	Software Usage Restrictions	A.5.32*
CM-11	User-Installed Software	A.8.19*
CM-12	Information Location	None
CM-13	Data Action Mapping	None
CM-14	Signed Components	None
CP-1	Contingency Planning Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
CP-2	Contingency Plan	7.5.1, 7.5.2, 7.5.3, A.5.2, A.5.29, A.8.14
CP-3	Contingency Training	A.6.3*
CP-4	Contingency Plan Testing	A.5.29, A.5.30*
CP-5	Withdrawn	---
CP-6	Alternate Storage Site	A.5.29*, A.7.5*, A.8.14*
CP-7	Alternate Processing Site	A.5.29*, A.7.5*, A.8.14*
CP-8	Telecommunications Services	A.5.29*, A.7.11
CP-9	System Backup	A.5.29*, A.5.33*, A.8.13
CP-10	System Recovery and Reconstitution	A.5.29*

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS <i>Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.</i>
CP-11	Alternate Communications Protocols	A.5.29*
CP-12	Safe Mode	None
CP-13	Alternative Security Mechanisms	A.5.29*
IA-1	Identification and Authentication Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
IA-2	Identification and Authentication (Organizational Users)	A.5.16
IA-3	Device Identification and Authentication	None
IA-4	Identifier Management	A.5.16
IA-5	Authenticator Management	A.5.16, A.5.17
IA-6	Authentication Feedback	A.8.5*
IA-7	Cryptographic Module Authentication	None
IA-8	Identification and Authentication (Non-Organizational Users)	A.5.16
IA-9	Service Identification and Authentication	None
IA-10	Adaptive Identification and Authentication	None
IA-11	Re-authentication	None
IA-12	Identity Proofing	None
IR-1	Incident Response Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
IR-2	Incident Response Training	A.6.3*
IR-3	Incident Response Testing	None
IR-4	Incident Handling	A.5.25, A.5.26, A.5.27
IR-5	Incident Monitoring	None
IR-6	Incident Reporting	A.5.5*, A.6.8
IR-7	Incident Response Assistance	None
IR-8	Incident Response Plan	7.5.1, 7.5.2, 7.5.3, A.5.24
IR-9	Information Spillage Response	None
IR-10	Withdrawn	---
MA-1	System Maintenance Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.37, A.18.1.1, A.18.2.2
MA-2	Controlled Maintenance	A.7.10*, A.7.13*, A.8.10*
MA-3	Maintenance Tools	None
MA-4	Nonlocal Maintenance	None
MA-5	Maintenance Personnel	None
MA-6	Timely Maintenance	A.7.13
MA-7	Field Maintenance	None
MP-1	Media Protection Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
MP-2	Media Access	A.5.10*, A.7.7*, A.7.10*
MP-3	Media Marking	A.5.13
MP-4	Media Storage	A.5.10*, A.7.7*, A.7.10, A.8.10*
MP-5	Media Transport	A.5.10*, A.7.9, A.7.10
MP-6	Media Sanitization	A.5.10, A.7.10*, A.7.14, A.8.10
MP-7	Media Use	A.5.10, A.7.10
MP-8	Media Downgrading	None
PE-1	Physical and Environmental Protection Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS
		<i>Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.</i>
PE-2	Physical Access Authorizations	A.7.2*
PE-3	Physical Access Control	A.7.1, A.7.2, A.7.3, A.7.4
PE-4	Access Control for Transmission Medium	A.7.2, A.7.12
PE-5	Access Control for Output Devices	A.7.2, A.7.3, A.7.7
PE-6	Monitoring Physical Access	A.7.4, A.8.16*
PE-7	Withdrawn	---
PE-8	Visitor Access Records	None
PE-9	Power Equipment and Cabling	A.7.5, A.7.8, A.7.11, A.7.12
PE-10	Emergency Shutoff	A.7.11*
PE-11	Emergency Power	A.7.11
PE-12	Emergency Lighting	A.7.11*
PE-13	Fire Protection	A.7.5, A.7.8
PE-14	Environmental Controls	A.7.5, A.7.8, A.7.11
PE-15	Water Damage Protection	A.7.5, A.7.8, A.7.11
PE-16	Delivery and Removal	A.5.10*, A.7.2*, A.7.10*
PE-17	Alternate Work Site	A.5.14*, A.6.7, A.7.9
PE-18	Location of System Components	A.5.10*, A.7.5, A.7.8
PE-19	Information Leakage	A.7.5*, A.7.8*, A.8.12
PE-20	Asset Monitoring and Tracking	A.5.10*
PE-21	Electromagnetic Pulse Protection	None
PE-22	Component Marking	A.5.13
PE-23	Facility Location	A.7.5, A.7.8
PL-1	Planning Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
PL-2	System Security and Privacy Plans	7.5.1, 7.5.2, 7.5.3, 10.2, A.5.8*
PL-3	Withdrawn	---
PL-4	Rules of Behavior	A.5.4, A.5.10, A.6.2*
PL-5	Withdrawn	---
PL-6	Withdrawn	---
PL-7	Concept of Operations	8.1, A.5.8*
PL-8	Security and Privacy Architectures	A.5.8*
PL-9	Central Management	None
PL-10	Baseline Selection	None
PL-11	Baseline Tailoring	None
PM-1	Information Security Program Plan	4.1, 4.2, 4.3, 4.4, 5.2, 5.3, 6.1.1, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3, 8.1, 9.3.1*, 10.1, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36
PM-2	Information Security Program Leadership Role	5.1, 5.3, A.5.2
PM-3	Information Security and Privacy Resources	5.1, 6.2, 7.1
PM-4	Plan of Action and Milestones Process	6.1.1, 6.2, 7.5.1, 7.5.2, 7.5.3, 8.3, 9.3.2*, 10.2
PM-5	System Inventory	None
PM-6	Measures of Performance	5.3, 6.1.1, 6.2, 9.1
PM-7	Enterprise Architecture	None
PM-8	Critical Infrastructure Plan	None
PM-9	Risk Management Strategy	4.3, 4.4, 6.1.1, 6.1.2, 6.2, 7.5.1, 7.5.2, 7.5.3, 10.1
PM-10	Authorization Process	A.5.2*
PM-11	Mission and Business Process Definition	4.1
PM-12	Insider Threat Program	None

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS
		<i>Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.</i>
PM-13	Security and Privacy Workforce	7.2, A.6.3*
PM-14	Testing, Training, and Monitoring	6.2*
PM-15	Security and Privacy Groups and Associations	7.4, A.5.6
PM-16	Threat Awareness Program	A.5.7
PM-17	Protecting Controlled Unclassified Information on External Systems	None
PM-18	Privacy Program Plan	A.5.4
PM-19	Privacy Program Leadership Role	None
PM-20	Dissemination of Privacy Program Information	None
PM-21	Accounting of Disclosures	None
PM-22	Personally Identifiable Information Quality Management	None
PM-23	Data Governance Body	None
PM-24	Data Integrity Board	None
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	None
PM-26	Complaint Management	None
PM-27	Privacy Reporting	None
PM-28	Risk Framing	4.3, 6.1.2, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3
PM-29	Risk Management Program Leadership Roles	5.1, 5.3, 9.3.1*, A.5.2
PM-30	Supply Chain Risk Management Strategy	4.4, 6.2, 7.5.1, 7.5.2, 7.5.3, 10.2*
PM-31	Continuous Monitoring Strategy	4.4, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3, 9.1, 9.2.2*, 10.1, 10.2
PM-32	Purposing	None
PS-1	Personnel Security Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
PS-2	Position Risk Designation	None
PS-3	Personnel Screening	A.6.1
PS-4	Personnel Termination	A.5.11, A.6.5
PS-5	Personnel Transfer	A.5.11, A.6.5
PS-6	Access Agreements	A.5.4*, A.6.2, A.6.6*
PS-7	External Personnel Security	A.5.2, A.5.4*
PS-8	Personnel Sanctions	7.3, A.6.4
PS-9	Position Descriptions	A.5.2
PT-1	Personally Identifiable Information Processing and Transparency Policy and Procedures	A.5.4
PT-2	Authority to Process Personally Identifiable Information	None
PT-3	Personally Identifiable Information Processing Purposes	None
PT-4	Consent	None
PT-5	Privacy Notice	None
PT-6	System of Records Notice	None
PT-7	Specific Categories of Personally Identifiable Information	None
PT-8	Computer Matching Requirements	None
RA-1	Risk Assessment Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
RA-2	Security Categorization	A.5.12*
RA-3	Risk Assessment	6.1.2, 8.2, 9.3.2*, A.8.8*

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS
		<i>Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.</i>
RA-4	Withdrawn	---
RA-5	Vulnerability Monitoring and Scanning	A.8.8*
RA-6	Technical Surveillance Countermeasures Survey	None
RA-7	Risk Response	6.1.3, 8.3, 10.2
RA-8	Privacy Impact Assessments	None
RA-9	Criticality Analysis	A.5.22*
RA-10	Threat Hunting	A.5.7*
SA-1	System and Services Acquisition Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 8.1, A.5.1, A.5.2, A.5.4, A.5.23, A.5.31, A.5.36, A.5.37
SA-2	Allocation of Resources	None
SA-3	System Development Life Cycle	A.5.2*, A.5.8, A.8.25, A.8.31*
SA-4	Acquisition Process	8.1, A.5.8, A.5.20, A.5.23, A.8.29, A.8.30
SA-5	System Documentation	7.5.1, 7.5.2, 7.5.3, A.5.37*
SA-6	Withdrawn	---
SA-7	Withdrawn	---
SA-8	Security Engineering Principles	A.8.27, A.8.28*
SA-9	External System Services	A.5.2*, A.5.4*, A.5.8*, A.5.14*, A.5.22, A.5.23, A.8.21
SA-10	Developer Configuration Management	A.8.9, A.8.28*, A.8.30*, A.8.32
SA-11	Developer Testing and Evaluation	A.8.29, A.8.30*
SA-12	Withdrawn	---
SA-13	Withdrawn	---
SA-14	Withdrawn	---
SA-15	Development Process, Standards, and Tools	A.5.8*, A.8.25
SA-16	Developer-Provided Training	None
SA-17	Developer Security and Privacy Architecture and Design	A.8.25, A.8.27
SA-18	Withdrawn	---
SA-19	Withdrawn	---
SA-20	Customized Development of Critical Components	None
SA-21	Developer Screening	A.6.1
SA-22	Unsupported System Components	None
SA-23	Specialization	None
SC-1	System and Communications Protection Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
SC-2	Separation of System and User Functionality	None
SC-3	Security Function Isolation	None
SC-4	Information In Shared System Resources	None
SC-5	Denial-of-Service-Protection	None
SC-6	Resource Availability	None
SC-7	Boundary Protection	A.5.14*, A.8.16*, A.8.20*, A.8.22*, A.8.23*, A.8.26*
SC-8	Transmission Confidentiality and Integrity	A.5.10*, A.5.14, A.8.20*, A.8.26*
SC-9	Withdrawn	---
SC-10	Network Disconnect	A.8.20
SC-11	Trusted Path	None
SC-12	Cryptographic Key Establishment and Management	A.8.24
SC-13	Cryptographic Protection	A.8.24, A.8.26, A.5.31
SC-14	Withdrawn	---

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS
		<i>Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.</i>
SC-15	Collaborative Computing Devices and Applications	A.5.14*
SC-16	Transmission of Security and Privacy Attributes	None
SC-17	Public Key Infrastructure Certificates	A.8.24
SC-18	Mobile Code	None
SC-19	Withdrawn	None
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	None
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	None
SC-22	Architecture and Provisioning for Name/Address Resolution Service	None
SC-23	Session Authenticity	None
SC-24	Fail in Known State	None
SC-25	Thin Nodes	None
SC-26	Decoys	None
SC-27	Platform-Independent Applications	None
SC-28	Protection of Information at Rest	A.5.10*
SC-29	Heterogeneity	None
SC-30	Concealment and Misdirection	None
SC-31	Covert Channel Analysis	None
SC-32	System Partitioning	None
SC-33	Withdrawn	---
SC-34	Non-Modifiable Executable Programs	None
SC-35	External Malicious Code Identification	None
SC-36	Distributed Processing and Storage	None
SC-37	Out-of-Band Channels	None
SC-38	Operations Security	A.8.x
SC-39	Process Isolation	None
SC-40	Wireless Link Protection	None
SC-41	Port and I/O Device Access	None
SC-42	Sensor Capability and Data	None
SC-43	Usage Restrictions	None
SC-44	Detonation Chambers	None
SC-45	System Time Synchronization	None
SC-46	Cross Domain Policy Enforcement	None
SC-47	Alternate Communications Paths	None
SC-48	Sensor Relocation	None
SC-49	Hardware-Enforced Separation and Policy Enforcement	None
SC-50	Software-Enforced Separation and Policy Enforcement	None
SC-51	Hardware-Based Protection	None
SI-1	System and Information Integrity Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
SI-2	Flaw Remediation	A.6.8*, A.8.8, A.8.32*
SI-3	Malicious Code Protection	A.8.7
SI-4	System Monitoring	A.8.16*
SI-5	Security Alerts, Advisories, and Directives	A.5.6*

NIST SP 800-53, REVISION 5 CONTROLS		ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS
		<i>Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.</i>
SI-6	Security and Privacy Function Verification	None
SI-7	Software, Firmware, and Information Integrity	None
SI-8	Spam Protection	None
SI-9	Withdrawn	---
SI-10	Information Input Validation	None
SI-11	Error Handling	None
SI-12	Information Management and Retention	None
SI-13	Predictable Failure Prevention	None
SI-14	Non-Persistence	None
SI-15	Information Output Filtering	None
SI-16	Memory Protection	None
SI-17	Fail-Safe Procedures	None
SI-18	Personally Identifiable Information Quality Operations	None
SI-19	De-identification	None
SI-20	Tainting	A.8.12
SI-21	Information Refresh	A.8.10
SI-22	Information Diversity	None
SI-23	Information Fragmentation	None
SR-1	Supply Chain Risk Management Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.19, A.5.31, A.5.36, A.5.37
SR-2	Supply Chain Risk Management Plan	A.5.19, A.5.20*, A.5.21*, A.8.30*
SR-3	Supply Chain Controls and Processes	A.5.20, A.5.21*
SR-4	Provenance	A.5.21*, A.8.30*
SR-5	Acquisition Strategies, Tools, and Methods	A.5.20, A.5.21, A.5.23
SR-6	Supplier Assessments and Reviews	A.5.22
SR-7	Supply Chain Operations Security	A.5.22*
SR-8	Notification Agreements	None
SR-9	Tamper Resistance and Detection	None
SR-10	Inspection of Systems or Components	None
SR-11	Component Authenticity	None
SR-12	Component Disposal	None

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK

Table 2 provides a mapping from the security requirements and controls in ISO/IEC 27001 to the security controls in Special Publication 800-53 including mappings of ISO/IEC 27001 requirements and controls to control enhancements.³ Please review the introductory text provided above before employing the mappings in Table 2.

TABLE 2: MAPPING ISO/IEC 27001:2022 TO NIST SP 800-53, REVISION 5

ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS	NIST SP 800-53, REVISION 5 CONTROLS <i>Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.</i>
ISO/IEC 27001 Requirements	
4. Context of the Organization	
4.1 Understanding the organization and its context	PM-1, PM-11
4.2 Understanding the needs and expectations of interested parties	PM-1
4.3 Determining the scope of the information security management system	PM-1, PM-9, PM-28
4.4 Information security management system	PM-1, PM-9, PM-30, PM-31
5. Leadership	
5.1 Leadership and commitment	PM-2, PM-3, PM-29
5.2 Policy	All XX-1 controls
5.3 Organizational roles, responsibilities, and authorities	All XX-1 controls, PM-2, PM-6, PM-29
6. Planning	
6.1 Actions to address risks and opportunities	
6.1.1 General	PM-1, PM-4, PM-6, PM-9
6.1.2 Information security risk assessment	PM-9, PM-28, RA-3
6.1.3 Information security risk treatment	RA-7
6.2 Information security objectives and planning to achieve them	PM-1, PM-3, PM-4, PM-6, PM-9, PM-14, PM-28, PM-30, PM-31
7. Support	
7.1 Resources	PM-3
7.2 Competence	PM-13
7.3 Awareness	AT-2, PS-8
7.4 Communication	PM-1, PM-15, PM-28, PM-31
7.5 Documented information	
7.5.1 General	All XX-1 controls, CP-2, IR-8, PL-2, PM-4, PM-9, PM-28, PM-30, PM-31, SA-5
7.5.2 Creating and updating	All XX-1 controls, CP-2, IR-8, PL-2, PM-4, PM-9, PM-28, PM-30, PM-31, SA-5
7.5.3 Control of documented information	All XX-1 controls, CP-2, IR-8, PL-2, PM-4, PM-9, PM-28, PM-30, PM-31, SA-5
8. Operation	
8.1 Operation planning and control	CM-3, PL-7, PM-1, SA-1, SA-4
8.2 Information security risk assessment	RA-3
8.3 Information security risk treatment	CA-5, PM-4, RA-7
9. Performance evaluation	
9.1 Monitoring, measurement, analysis and evaluation	CA-1, CA-7, PM-6, PM-31
9.2 Internal audit	
9.2.1 General	CA-2*, CA-7*

³ The use of the term *XX-1 controls* in mapping Table 2 refers to the set of security controls represented by the first control in each 800-53 control family, where *XX* is a placeholder for the two-letter family identifier.

ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS	NIST SP 800-53, REVISION 5 CONTROLS <i>Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.</i>
9.2.2 Internal audit programme	CA-1*, CA-2*, CA-2(1)*, CA-7(1)*, PM-31*
9.3 Management review	
9.3.1 General	CA-1*, CA-6*, PM-1*, PM-29
9.3.2 Management review inputs	CA-7*, CA-7(3)*, CA-7(4)*, PM-4*, RA-3*
9.3.3 Management review results	CA-5*, CA-6*, CA-7*, CM-3*
10. Improvement	
10.1 Continual improvement	PM-1, PM-9, PM-30, PM-31
10.2 Nonconformity and corrective action	CA-5, PL-2, PM-4, PM-31, RA-7
ISO/IEC 27001 Controls	
5 Organizational controls	
5.1 Policies for information security	All XX-1 controls
5.2 Information security roles and responsibilities	All XX-1 controls, CM-9, CP-2, PS-7, PS-9, SA-3, SA-9, PM-2, PM-10
5.3 Segregation of duties	AC-5
5.4 Management responsibilities	All XX-1 controls, PM-18*
5.5 Contact with authorities	IR-6
5.6 Contact with special interest groups	PM-15, SI-5
5.7 Threat intelligence	PM-16, PM-16(1), RA-10
5.8 Information security in project management	PL-2, PL-7, PL-8, SA-3, SA-4, SA-9, SA-15
5.9 Inventory of information and other associated assets	CM-8
5.10 Acceptable use of information and other associated assets	MP-2, MP-4, MP-5, MP-6, MP-7, PE-16, PE-18, PE-20, PL-4, SC-8, SC-28
5.11 Return of assets	PS-4, PS-5
5.12 Classification of information	RA-2
5.13 Labelling of information	MP-3, PE-22
5.14 Information transfer	AC-4, AC-17, AC-18, AC-19, AC-20, CA-3, PE-17, PS-6, SA-9, SC-7, SC-8, SC-15
5.15 Access control	AC-1, AC-3, AC-6
5.16 Identity management	AC-2, IA-2, IA-4, IA-5, IA-8
5.17 Authentication information	IA-5
5.18 Access rights	AC-2
5.19 Information security in supplier relationships	SR-1
5.20 Addressing information security within supplier agreements	SA-4, SR-3
5.21 Managing information security in the information and communication technology (ICT) supply chain	SR-3, SR-5
5.22 Monitoring, review and change management of supplier services	RA-9, SA-9, SR-6, SR-7
5.23 Information security for use of cloud services	SA-1, SA-4, SA-9, SA-9(3), SR-5
5.24 Information security incident management planning and preparation	IR-8
5.25 Assessment and decision on information security events	AU-6, IR-4
5.26 Response to information security events	IR-4
5.27 Learning from information security incidents	IR-4
5.28 Collection of evidence	AU-3, AU-4, AU-9, AU-10(3), AU-11*
5.29 Information security during disruption	CP-2, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13
5.30 ICT readiness for business continuity	CP-2(1)*, CP-2(8)*, CP-4*, CP-4(1)*
5.31 Legal, statutory, regulatory and contractual requirements	All XX-1 controls, SC-12, SC-13, SC-17
5.32 Intellectual property rights	CM-10*

ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS	NIST SP 800-53, REVISION 5 CONTROLS <i>Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.</i>
5.33 Protection of records	AC-3*, AC-23, AU-9, CP-9, SC-8, SC-8(1)*, SC-13, SC-28, SC-28(1)*
5.34 Privacy and protection of personal identifiable information (PII)	PM-18, PT-1, PT-3, PT-7, CA-9*, CA-3*, PL-2*, PL-8*
5.35 Independent review of information security	CA-2(1)
5.36 Compliance with policies, rules and standards for information security	All XX-1 controls, CA-2
5.37 Documented operating procedures	All XX-1 controls, SA-5
6 People controls	
6.1 Screening	PS-3, SA-21
6.2 Terms and conditions of employment	PL-4, PS-6
6.3 Information security awareness, education, and training	AT-2, AT-3, CP-3, IR-2, PM-13
6.4 Disciplinary process	PS-8
6.5 Responsibilities after termination or change of employment	PS-4, PS-5
6.6 Confidentiality or non-disclosure agreements	PS-6
6.7 Remote working	None
6.8 Information security event reporting	AU-6, IR-6, SI-2
7 Physical Controls	
7.1 Physical security perimeters	PE-3*
7.2 Physical entry	PE-2, PE-3, PE-4, PE-5, PE-16
7.3 Securing offices, rooms and facilities	PE-3, PE-5
7.4 Physical security monitoring	AU-6(6)*, PE-3, PE-3(3), PE-6, PE-6(1), PE-6(4)*
7.5 Protecting against physical and environmental threats	CP-6, CP-7, PE-9, PE-13, PE-14, PE-15, PE-18, PE-19, PE-23
7.6 Working in secure areas	SC-42*
7.7 Clear desk and clear screen	AC-11, MP-2, MP-4
7.8 Equipment siting and protection	PE-9, PE-13, PE-14, PE-15, PE-18, PE-19, PE-23
7.9 Security of assets off-premises	AC-19, AC-20, MP-5, PE-17
7.10 Storage media	MA-2, MP-2, MP-4, MP-5, MP-6, MP-7, PE-16
7.11 Supporting utilities	CP-8, PE-9, PE-10, PE-11, PE-12, PE-14, PE-15
7.12 Cabling security	PE-4, PE-9
7.13 Equipment maintenance	MA-2, MA-6
7.14 Secure disposal or re-use of equipment	MP-6
8 Technological controls	
8.1 User end point devices	AC-11
8.2 Privileged access rights	AC-2, AC-3, AC-6, CM-5
8.3 Information access restriction	AC-3, AC-24
8.4 Access to source code	AC-3*, AC-3(11), CM-5
8.5 Secure authentication	AC-7, AC-8, AC-9, IA-6
8.6 Capacity management	AU-4, CP-2(2), SC-5(2)*
8.7 Protection against malware	AT-2, SI-3
8.8 Management of technical vulnerabilities	RA-3, RA-5, SI-2, SI-5
8.9 Configuration management	CM-1, CM-2, CM-2(3)*, CM-3, CM-3(7), CM-3(8), CM-4, CM-5, CM-6, CM-8, CM-9, CM-9(1)*, SA-10
8.10 Information deletion	AC-4(25)*, AC-7(2)*, MA-2, MA-3(3)*, MA-4(3)*, MP-4, MP-6, MP-6(1)*, SI-21
8.11 Data masking	AC-4(23), SI-19(4)
8.12 Data leakage prevention	AU-13, PE-3(2)*, PE-19, SC-7(10)*, SI-20
8.13 Information backup	CP-9
8.14 Redundancy of information processing facilities	CP-2, CP-6, CP-7

ISO/IEC 27001:2022 REQUIREMENTS AND CONTROLS	NIST SP 800-53, REVISION 5 CONTROLS <i>Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.</i>
8.15 Logging	AU-3, AU-6, AU-9, AU-11, AU-12, AU-14
8.16 Monitoring activities	AC-2(12), AC-17(1), AU-13*, IR-4(13)*, MA-4(1)*, PE-6*, PE-6(3)*, SI-4, SI-4(4)*, SI-4(13)*, SI-4(16)*
8.17 Clock synchronization	AU-8
8.18 Use of privileged utility programs	AC-3, AC-6
8.19 Installation of software on operational systems	CM-5, CM-7(4)*, CM-7(5)*, CM-11*
8.20 Networks security	AC-3, AC-18, AC-20, SC-7, SC-8, SC-10
8.21 Security of network services	CA-3, SA-9
8.22 Segregation of networks	AC-4, SC-7
8.23 Web filtering	AC-4, SC-7, SC-7(8)
8.24 Use of cryptography	SC-12, SC-13, SC-17
8.25 Secure development life cycle	SA-3, SA-15, SA-17
8.26 Application security requirements	AC-3, SC-8*, SC-13
8.27 Secure system architecture and engineering principles	SA-8
8.28 Secure coding	SA-4(3)*, SA-8, SA-11(1)*, SA-15(5)*, SI-10
8.29 Security testing in development and acceptance	CA-2, SA-4, SA-11, SR-5(2)*
8.30 Outsourced development	SA-4, SA-10, SA-11, SA-15, SR-2, SR-4
8.31 Separation of development, test and production environments	CM-4(1), CM-5*, SA-3*
8.32 Change management	CM-3, CM-5, SA-10, SI-2
8.33 Test information	SA-3(2)*
8.34 Protection of information systems during audit testing	AU-5*

16. Systems hosting webservices must disable deprecated cipher suites - all SSL versions, TLS 1.0 and TLS 1.1

Yes, Volatia is compliant.

17. Systems hosting webservices must uses TLS 1.2 or greater with strong cipher suites.

Yes, Volatia shall be compliant.

18. Systems hosting webservices must assess at least annual against current OWASP Top 10 web application security risks.

Yes, Volatia is compliant.

19. Cloud-based Offeror solutions should be capable of compliance with the Microsoft Azure cloud-based security access broker.

Yes, Volatia is compliant.

20. Cloud-based Offeror solutions should be capable of restricting access based on originating IP address ranges or another whitelisting feature.

Yes, Volatia is compliant.

21. Offeror solution shall be configured to protect against malware and viruses regardless of the host operating system.

Yes, Volatia is compliant.

K. Performance & Elasticity (On-premise and Cloud)

1. Offeror solutions are to be performance tested and validated by the Offeror in meeting business performance requirements before going into production.

Yes, Volatia shall be compliant.

2. Offeror solutions, cloud based or on-premises, should be capable of accommodating load testing by County personnel or other entities as appropriate for the designated platform.

Yes, Volatia is compliant.

3. Systems are required to be tested for acceptable performance under 1.5X typical load.

Yes, Volatia shall be compliant.

4. Offeror must provide service level agreement specifications that define user, batch and backend processing performance and responsiveness of the solution.

Yes, Volatia shall be compliant.

5. Offeror cloud-based solutions should be capable of automatically adding resources in response to increased demand and eroding responsiveness.

Yes, Volatia is compliant.

6. Offer solutions shall provide monitoring and benchmarking tools that enable performance analysis and remediation at all layers of the solution (client, web, database, application, interface, etc.)

Yes, Volatia is compliant.

7. Offeror cloud-based solutions which are multi-tenant or use shared resources shall be architected in such a way as to insulate one customers performance operation from another.

Yes, Volatia is compliant.

8. Upon request, all non-production environments must be dynamically scalable to the resource configuration and performance of the production environment for testing purposes.

Yes, Volatia is compliant.

L. Virtualization

1. Virtual Server

- a. The Offeror's solution must be compatible with the County's virtualization solutions running in VMWare or Azure environments.

Yes, Volatia is compliant.

- b. The Offeror's solution must operate in cloud architectures hosted in the County data center or in the Azure Government or Corporate Cloud tenants.

Yes, Volatia is compliant.

- c. Offeror solutions for other cloud hosted virtual providers (AWS, Google, IBM, etc.) shall be evaluated for compatibility and compliance to County standards.

Yes, Volatia shall be compliant.

- d. The vendor's solution must be compatible with the County's desktop virtualization environments VMWare Horizon and Microsoft Virtual Desktop in Azure.

Yes, Volatia shall be compliant.

2. Virtual Client

- a. All client software must be capable of operating seamlessly on virtual desktop platforms VMWare Horizon and Microsoft Virtual Desktop

Yes, Volatia is compliant.

M. Offeror and Cloud Hosted Implementation

Offeror Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) must meet the following requirements:

1. The Offeror must provide a description of managed services environment and associated service level agreements.

Yes, Volatia is compliant as applicable. All services offered are expressed in the proposal. Volatia does not provide managed services. More information shall be provided, upon request, during the negotiation or implementation phase.

2. All County data and any derivatives or backups must reside within the continental United States.

Yes, Volatia is compliant.

3. Ownership of all data, derivatives and backups is absolute and, in all cases, resides with the County.

Yes, Volatia shall be compliant.

4. Offeror shall provide SOC 2 or ISO 27001 report for hosting environment.

Yes, Volatia shall be compliant.

5. Offeror shall provide SOC 2 or 3 report(s) for internal controls over security, availability, processing integrity and confidentiality.

Yes, Volatia shall be compliant.

6. Offeror shall provide SOC 1 report in the case of financial systems hosting.

Yes, Volatia shall be compliant.

7. Offeror shall provide monitoring, configuration, and issue resolution for system optimization

Yes, Volatia shall be compliant.

8. Offeror shall provide "hot" failover protection for all production environments, with seamless transfer of load and processing to another geographical region.

Yes, Volatia shall be compliant.

9. Offeror shall provide mechanisms to move software configurations, security configurations and code from non-production environments to production environments.

Yes, Volatia shall be compliant.

10. Offeror shall ensure connectivity needs for hybrid environments (on premise to cloud) comply with the network requirements for operating environment (see section 6 above) and do not require the purchase of other third-party tools.

Yes, Volatia shall be compliant.

11. System shall use a web-based authentication process using a SAML compliant federation source, Azure Active Directory or Active Directory Federation Services.

Yes, Volatia shall be compliant.

12. Batch data extractions shall be available on demand or via scheduled process for obtaining some or all County data, including but not limited to JSON, XML or CSV format.

Yes, Volatia shall be compliant.

13. Offeror should provide the full list of industry portable formats currently provided from the proposed solution.

Volatia shall support any format requested by Client. Current formats are XML, CSV, and PDF.

14. Data extraction interfaces and pipelines shall be based on industry standard application programming interfaces (API) in addition to batch mode extractions.

Yes, Volatia shall be compliant.

15. There shall be no extra cost incurred for data extractions, regardless of the amount of exfiltrated data.

Yes, Volatia shall be compliant.

16. Offeror environments shall be configured with cloud-based firewalls and intrusion prevention devices implementing a hardening standard that is consistent with the security classification of the most sensitive data in the system compliant with an industry standard. The Offeror must name the configuration hardening standard applied to their solution.

Yes, Volatia shall be compliant.

17. Offeror solution shall be configured to protect against malware and viruses regardless of the host operating system.

Yes, Volatia shall be compliant.

N. Chesterfield Hosted Implementation (County-Hosted, On-Premise, or Cloud)

1. The solution must run on Chesterfield VMware, Azure virtual servers, Azure networking components and/or Azure platform services.

Yes, Volatia shall be compliant.

2. Server-side components of system should host on Microsoft Internet Information Services (IIS) most recent supported general release. No client software should be required or installed on server.

Yes, Volatia shall be compliant.

3. If the solution is based on .NET, the technology, the solution must utilize current version of the .NET framework.

Yes, Volatia is compliant.

O. Web-Based Solutions

1. Customer Facing Browser – system should be compatible with current and immediate previous release of the following browsers: Edge, Chrome and Safari.

Yes, Volatia is compliant.

2. System should not make use of permanent cookies on external web components.

Yes, Volatia is compliant.

3. Publicly accessible internet solutions accessible by staff and constituents alike, must meet County web standards in order to deliver acceptable search results.

Yes, Volatia is compliant.

- a. Largest Contentful Paint (LCP), or loading performance, should occur and resolve within 2.5 seconds of when a page first starts loading for most users.

Yes, Volatia is compliant.

- b. First Input Delay (FID), or interactivity within a page or application, should occur within 100 milliseconds or less for most users.

Yes, Volatia is compliant.

- c. Cumulative Layout Shift (CLS), or visual stability of a page or application on load, should maintain a shift of 0.1 or less for most users.

Yes, Volatia is compliant.

- d. The County requires that web solutions must utilize HTTPS

Yes, Volatia is compliant.

- e. The County requires web solutions should be mobile-responsive

Yes, Volatia is compliant.
 - f. The County requires web solutions should not utilize intrusive interstitials, or popups

Yes, Volatia is compliant.
4. The Offeror's solution must comply with most currently adopted Web Content Accessibility Guideline (WCAG) (2.1 as of May 2022) standards for American Disabilities Act (ADA) accessibility and usability that have been adopted as County standards:
- a. Text Alternatives: Provide text alternatives for any non-text content so that it can be changed into other forms people need, such as large print, braille, speech, symbols or simpler language.

Yes, Volatia is compliant.
 - b. Time-based Media: Provide alternatives for time-based media.

Yes, Volatia is compliant.
 - c. Adaptable: Create content that can be presented in different ways (for example simpler layout) without losing information or structure.

Yes, Volatia is compliant.
 - d. Distinguishable: Make it easier for users to see and hear content including separating foreground from background.

Yes, Volatia is compliant.
 - e. Keyboard Accessible: Make all functionality available from a keyboard.

Yes, Volatia is compliant.
 - f. Enough Time: Provide users enough time to read and use content.

Yes, Volatia is compliant.
 - g. Seizures: Do not design content in a way that is known to cause seizures.

Yes, Volatia is compliant.
 - h. Navigable: Provide ways to help users navigate, find content, and determine where they are.

Yes, Volatia is compliant.

- i. Input Modalities: Make it easier for users to operate functionality through various inputs beyond keyboard.

Yes, Volatia is compliant.

- j. Readable: Make text content readable and understandable.

Yes, Volatia is compliant.

- k. Predictable: Make Web pages appear and operate in predictable ways.

Yes, Volatia is compliant.

- l. Input Assistance: Help users avoid and correct mistakes.

Yes, Volatia is compliant.

- m. Compatible: Maximize compatibility with current and future user agents, including assistive technologies.

Yes, Volatia is compliant.

P. System Interfaces and Integrations

- 1. System should provide an industry standard application programming interface (API) for integrations to external systems.

Yes, Volatia is compliant. Customizations are necessary based on Client requirements.

- 2. Documentation should be available for any REST endpoints for the County to reference when implementing the solution or integrating with other County solutions.

Yes, Volatia is compliant. Customizations are necessary based on Client requirements.

- 1. Expected URL patterns

Not applicable

- 2. HTTP verbs

Not applicable

3. Input and output expectations

Not applicable

4. Security

Not applicable

3. Batch interfaces should use Microsoft's SQL Server Integration Services, Azure Data Factory, Chesterfield API, and Microsoft or Control-M scheduling options.

Yes, Volatia shall be compliant.

4. Offeror solutions that leverage Microsoft 365 for email, calendar, Teams, Microsoft Dynamics, and Microsoft Power Platform features must use the Microsoft Graph API and M365 APIs.

Yes, Volatia shall be compliant.

5. All GIS integrations should use geo-enabled web services hosted either by Chesterfield on ArcGIS Server or hosted by ArcGIS Online.

Yes, Volatia shall be compliant.

6. Standard geo-processing scripts should use the current release of Python.

Yes, Volatia shall be compliant.

Q. Data Management, Data Analysis, Machine Learning, Business Intelligence & Reporting

1. The system must store information in an industry standard database system, not a proprietary system, and prefer the Microsoft family of solutions including Microsoft SQL Server, Azure SQL, Azure Managed SQL, or Azure Data Lake storage.

Yes, Volatia is compliant.

2. The Offeror solution must not require Microsoft Access or other client/desktop-based database software to operate or produce reports for the solution.

Yes, Volatia is compliant.

3. Offeror must provide a data dictionary of customer specific data structures and user-friendly definitions, including an entity relationship diagram of the database entities or data access options for the County.

Yes, Volatia is compliant.

4. System must allow connection with standard business intelligence and reporting tools such as Microsoft Power BI or SQL Server Reporting Services.

Yes, Volatia is compliant.

5. Solution must provide capability for the County to integrate and extract all County-specific data to the County's enterprise data warehouse estate in for master data management, data historical archival, machine learning, business intelligence and reporting needs.

Yes, Volatia is compliant.

6. The Offeror must provide reports and process flows to the County as evidence of data quality management and/or profiling of their data or details of their data governance processes demonstrated in data validation quality reports.

Yes, Volatia is compliant.

R. Document Management

1. All documents and electronic content will be stored in the County's enterprise document management systems using security and storage best practices.

Yes, Volatia is compliant.

2. All access to documents should be done through the APIs available through the Microsoft Graph API for SharePoint Online or Laserfiche API. No direct access to documents, images, or databases will be acceptable.

Yes, Volatia shall be compliant.

3. Chesterfield's Information System Technology department and the customer departments have final approval on the design of the document storage, metadata, configuration, document retention, security, features used, system load, templates and index fields, record management design, and other aspects of electronic content management.

Yes, Volatia shall be compliant.

4. Documents should be stored in their native formats where available. TIFF images are preferred over PDF due to TIFF's open standard conventions.

Yes, Volatia shall be compliant.

5. API access and development support if needed should be purchased and licensed directly through the appropriate vendors. The County will not procure these licenses or support agreements on behalf of the Offeror.

Yes, Volatia shall be compliant.

6. Documents must be stored with meaningful metadata so that the documents may be accessed and searched from outside the system and/or integrated with other systems.

Yes, Volatia is compliant.

7. Edits in the system must be reflected in the documents and metadata in Laserfiche or SharePoint.

Yes, Volatia shall be compliant.

8. Appropriate indexes should be generated to reference the documents. Internal document IDs or other system references are not guaranteed to be constant and should not be relied upon.

Yes, Volatia shall be compliant.

9. Documents should be stored implementing the records management features of the document management system.

Yes, Volatia shall be compliant.

10. County should be able to move/delete/modify documents directly in the document management system without affecting the Offeror's system, with exceptions for the specific linking metadata.

Yes, Volatia shall be compliant.

11. Access of the documents should be handled by the individual end user accounts and not service accounts where possible to preserve the audit record of the documents.

Yes, Volatia shall be compliant.

12. Configuration options should be in place to govern the rate at which the system can add/query/view documents in the connected document management systems.

Yes, Volatia shall be compliant.

13. Configuration options must be parameterized (not hard coded into document management configuration). This includes but is not limited to server, repository, templates, fields, and other configuration options necessary for the integration with Laserfiche or SharePoint such that the County might maintain flexibility to make changes to the environments in the future.

Yes, Volatia shall be compliant.

5. Offeror Support and Remote Management

1. Offeror must provide notification of upcoming releases, patches, and fixes with details on changes.

Volatia will comply with this requirement.

2. Offeror must provide release within 30 days of Microsoft operating system release

Volatia will comply with this requirement.

3. Offeror must provide release within 30 days of web browser updates the detrimentally impact functionality of browser-based tools

Volatia will comply with this requirement.

4. Product common Offeror exploits (CVE) must have release provided within seven days of exploit identification.

Volatia will comply with this requirement.

5. Offeror software must be provided at the latest, generally available release level that the Offeror provides

Volatia will comply with this requirement.

6. The product must be warranted to operate on currently supported release of Microsoft and all other operating system versions and latest Microsoft applications or other 3rd party applications.

Volatia will comply with this requirement.

7. The Offeror must provide roadmap for product suite end of life and roadmaps to remain current with operating systems and applications the product is dependent upon.

Volatia will comply with this requirement.

8. Upon request the Offeror must agree to source code and escrow arrangement.

Volatia will comply with this requirement.

9. Vendor will be required to administer server solutions through County Securelink implementation and/or Microsoft Teams for collaborative administration sessions with County staff.

Volatia will comply with this requirement.

10. The County must be notified at least 30 days in advance of general release solution changes and releases unless otherwise specified.

Volatia will comply with this requirement.

Attachment C – Proprietary/Confidential Information Identification

As indicated in General Term and Condition 25. Proprietary Information - *Code of Virginia* Section 2.2-4342(F), as amended, states: "Trade secrets or proprietary information submitted by a bidder, offeror, or Contractor in connection with a procurement transaction or prequalification application submitted pursuant to subsection B of §2.2-4317 shall not be subject to the Virginia Freedom of Information Act (2.2-3700 et seq.); **however, the bidder, offeror, or Contractor shall (i) invoke the protections of this section prior to or upon submission of the data or other materials, (ii) identify the data or other materials to be protected, and (iii) state the reasons why protection is necessary.** **If the exemption from disclosure provided by Code of Virginia Section 2.2-4342(F), as amended, is not properly invoked then the proposals will be subject to disclosure pursuant to applicable law.**

The proprietary or trade secret material submitted in the original and all copies of the proposal must be identified by some distinct method such as highlighting or underlining and must indicate only the specific words, figures, or paragraphs that constitute trade secret or proprietary information. In addition, a summary of proprietary information submitted shall be submitted on this form. The classification of an entire proposal document, line item prices, and/or total proposal prices as proprietary or trade secrets is not acceptable. If, after being given reasonable time, the Offeror refuses to withdraw such a classification designation, the proposal will be rejected.

Name of Offeror: Volatia Language Network, Inc. invokes the protections of § 2.2-4342F of the *Code of Virginia* for the following portions of my proposal submitted on October 31, 2023

Date

Signature: Jessica Kent

Title: Proposals Manager

DATA/MATERIAL TO BE PROTECTED	SECTION NO., & PAGE NO.	REASON WHY PROTECTION IS NECESSARY
None		

Use continuation sheet(s) if necessary

EXHIBIT A
QUESTIONNAIRE FOR NATIONAL CONSIDERATION

Suppliers are required to meet specific qualifications. Please respond to each qualification statement on this questionnaire.

1. Will the pricing for all Products and/or Services offered be equal to or better than any other pricing options it offers to Participating Public Agencies nationally?
Yes No
2. Does your company have the ability to provide service to any Participating Public Agencies in all 50 states?
Yes *No
(*If no, identify the states where you do not have the ability to provide service to Participating Agencies.)
3. Does your company have a national sales force, dealer network or distributor with the ability to call on Participating Public Agencies in at least 35 states?
Yes *No
(*If no, identify the states where you have the ability to call on Participating Public Agencies.)
4. Will your company assign a dedicated Senior Management level Account Manager to support the resulting GovMVMT contract?
Yes No
5. Does your company maintain records of your overall Participating Public Agencies' sales that you can and will share with GovMVMT to monitor contract implementation progress?
Yes No
6. Does your company have the ability to provide electronic and ecommerce ordering and billing?
Yes No
7. Will the GovMVMT contract be your lead public offering to Participating Public Agencies?
Yes No
8. Check which applies for your company sales last year in the United States:
 Sales between \$0 - \$25 Million
 Sales greater than \$25 Million to \$50 Million
 Sales greater than \$50 Million to \$100 Million
 Sales greater than \$100 Million

Submitted by:

Jessica Kent

(Printed Name)

Jessica Kent

(Signature)

Proposals Manager

(Title)

October 31, 2023

(Date)

EXHIBIT B SUPPLIER RESPONSE

Supplier must provide the following information in order for the Lead Public Agency to determine Supplier's qualifications to extend the resulting Master Agreement to Participating Public Agencies thru GovMVMT.

A. National Commitments

1. Please provide a written narrative of your understanding and acceptance of the Supplier Representations and Covenants in Section 1 of this Attachment.

Volatia understands and accepts all of the terms and conditions expressed in the Supplier Representations and Covenants in Section 1 of this Attachment.

B. Company

1. Provide a brief history and description of Supplier, including Supplier's experience in providing similar products and services.

History

Volatia's beginnings can be traced back to the personal experiences of founder and CEO, Baraka Kasongo. Born in Rwanda Africa, Baraka became a refugee at the age of eight and lived in refugee camps for seven years in five different countries. In 2001, Baraka and his family arrived in the United States and began their immigration journey to citizenship.

Within two years, Baraka had learned enough English that local hospitals and government agencies would use him to interpret for others who spoke his native languages, Kinyarwanda and Swahili. Baraka became the point of contact for many organizations. His passion to help people moved him to create a network of volunteers that provided community interpretation and translation services.

This was the impetus for a corporation that has at its foundation the vision to create a world with no language barriers, a world with cultural harmony, and the mission to bridge linguistic and cultural barriers.

Due to Baraka's experiences, at Volatia, our main focus is to foster an inclusive workplace to unleash the synergy of diversity. We pride ourselves on being an Equal Opportunity Employer that will not discriminate against qualified applicants or employees. Our philosophy is that people should be treated fairly, with dignity; and upon the belief that citizens in a free society have the right to self-determination without fear of discrimination as to personal preference or characteristics beyond their control.

Volatia continues to transform the language industry through its innovative approach to meeting customer requirements while helping them discover the tools and services that fulfill hidden needs to deliver the most value.

Service Catalog

Reliable language solutions in crucial industries are what establish Volatia as a leading innovator in the language services industry. As an integrated network of linguists and language service providers, we support more than 280 languages that are the driving force behind our interpreter (video remote, over the phone, and on-site), document translation, and audiovisual translation solutions.

In addition to our language services, Volatia also provides educational classes, diversity training, workshops, program courses, coaches, and keynote speeches on topics such as diversity, equity, inclusion, how to work with an interpreter, laws, and regulations (Title VI, Executive Order 13166, ACA Section 1557, etc.).

Through our innovations and strategic partnerships, we are on the cutting edge of delivering cultural equality in a rapidly changing industry. Our clients enjoy a combination of the latest technology, data privacy, and security, plus a network of thousands of professional interpreters, translators, cultural coaches and trainers who are fully tested and trained to ensure reliability, confidentiality, and ease of access. Our services are available throughout the United States of America and in key markets around the world.

2. Provide the total number and location of sales persons employed by your company in the United States.

STATE	Number of Sales Representatives
AL	2
AK	1
AZ	2
AR	2
CA	4
CO	2
CT	2
DE	1
DC	2
FL	2
GA	2
HI	1
ID	2

IL	2
IN	2
IA	2
KS	2
KY	2
LA	2
ME	2
MD	2
MA	1
MI	2
MN	2
MS	2
MO	2
MT	1
NE	2

NV	2
NH	1
NJ	1
NM	2
NY	2
NC	2
ND	1
OH	2
OK	2
OR	2
PA	2
RI	1
SC	2
SD	2
TN	2

TX	4
UT	2
VT	2
VA	2

VI	1
WA	2
WV	2
WI	2

WY	1
Total = 97	

3. Please provide a narrative of how these sales people would be used to market the contract to eligible agencies across the country. Please describe what you have in place today and your future plans, if you were awarded the contract.

1. Present Infrastructure and Sales Force Allocation

Volatia's Current Resources: A Strong National Footprint

Volatia has established a strong, widespread presence across the United States with a dedicated sales force of 97 agents. These agents are strategically located based on state size and potential market reach, ensuring optimal coverage for all regions. For instance, smaller states like Wyoming are served by a single dedicated agent, while larger states such as California and Texas are catered to by a team of 4 agents each. This arrangement ensures that every region, regardless of size, receives specialized attention.

2. Initial Outreach and Awareness Campaign

Raising Contract Awareness: Proactive Engagement with Qualified Entities

Upon being awarded the contract, Volatia's agents will swing into immediate action. Their primary mission will be to reach out to eligible agencies and entities within their respective states. With the combination of local knowledge and Volatia's market expertise, these agents will be instrumental in raising awareness about the new contract opportunity. They will provide essential information, address queries, and guide potential clients through the initial stages of the process.

3. Onboarding Assistance and Continued Support

Beyond Awareness: A Commitment to Seamless Integration

Raising awareness is just the first step. Volatia recognizes the importance of providing continuous support throughout the onboarding process. As such, our agents are equipped to assist agencies in understanding the intricacies of the contract, ensuring that all documentation is in order, and facilitating a smooth transition. Their local presence further ensures that help is always nearby, making the process as efficient and hassle-free as possible.

4. Scalability and Future Plans

Adapting to the Needs of the Contract: Dynamic Resource Allocation

Volatia remains committed to delivering the highest level of service. With a clear understanding that contract demands can evolve, we have provisions in place to scale our resources accordingly. If there arises a need for enhanced outreach or intensified support in certain states or regions, Volatia is prepared to augment its sales force,

ensuring that every agency, regardless of its size or challenges, receives the support it needs. Our flexible strategy underscores our commitment to the success of this contract and the satisfaction of all involved agencies.

5. Concluding Commitment

Volatia's Pledge: Excellence Today, Preparedness for Tomorrow

In conclusion, Volatia's existing infrastructure, combined with our proactive approach and readiness to adapt, makes us the ideal partner to market this contract to agencies across the U.S. We are excited about the prospect of working closely with all eligible entities, ensuring that the benefits of the contract are fully realized. Awarding this contract to Volatia is an investment in a proven, strategic, and future-ready approach.

4. Provide the number and location of support centers.

Volatia remains committed to delivering the highest level of service. With a clear understanding that contract demands can evolve, we have provisions in place to scale our resources accordingly. If there arises a need for enhanced outreach or intensified support in certain states or regions, Volatia is prepared to augment its sales force, ensuring that every agency, regardless of its size or challenges, receives the support it needs. Our flexible strategy underscores our commitment to the success of this contract and the satisfaction of all involved agencies.

5. Provide company annual sales for the three previous fiscal years in the United States. Sales reporting should be segmented into the following categories:

SUPPLIER ANNUAL SALES IN THE UNITED STATES FOR 2020, 2021, AND 2022			
SEGMENT	2020 SALES	2021 SALES	2022 SALES
Cities	147,310	191,498	237,410
Counties	123,499	257,724	260,724
K-12 (Public/Private)	207,200	512,494	600,828
Higher Education (Public/Private)	48,210	88,244	80,614
States	120,551	140,371	235,401
Other Public Sector and Nonprofits	182,242	318,001	323,835
Federal	59,899	43,021	50,992
Private Sector	591,813	675,392	680,312
<i>Total Supplier Sales</i>	1,480,724	2,226,745	2,470,116

6. For the proposed products and services included in the scope of your response, provide annual sales for the last three fiscal years in the United States. Sales reporting should be segmented into the following categories:

SUPPLIER ANNUAL SALES IN THE UNITED STATES FOR 2020, 2021, AND 2022			
SEGMENT	2020 SALES	2021 SALES	2022 SALES

Cities	147,310	191,498	237,410
Counties	123,499	257,724	260,724
K-12 (Public/Private)	207,200	512,494	600,828
Higher Education (Public/Private)	48,210	88,244	80,614
States	120,551	140,371	235,401
Other Public Sector and Nonprofits	182,242	318,001	323,835
Federal	59,899	43,021	50,992
Private Sector	591,813	675,392	680,312
<i>Total Supplier Sales</i>	<i>1,480,724</i>	<i>2,226,745</i>	<i>2,470,116</i>

7. Provide a list of your company's ten largest public agency customers, including contact information.

1. Henrico County Public Schools
 Amy R. Ladd
 Secretary - Exceptional Education
 804-652-3600
arladd@henrico.k12.va.us

2. Orange County
 Carlos Corona, Deputy Purchasing Agent
 Procurement Services
 Orange County Social Services Agency
 Office (714) 541-7834
Carlos.Corona@ssa.ocgov.com

3. City of Roanoke
 Katie Hedrick
 Community Inclusion Coordinator
 City Manager's Office, City of Roanoke
 Office: 540-853-1283
Kathryn.hedrick@roanokeva.gov

4. Waynesboro City Public Schools
 Ryan N. Barber, Ed.D.
 Assistant Superintendent
 Waynesboro Public Schools
 Phone: 540-946-4600, Ext. 112
rbarber@waynesboro.k12.va.us

5. Knox County Health Department
 Scott White, MBA, MSN, RN
 Employee Health Nurse & Clinical Educator, LEP Coordinator, KCHD OSHA Compliance &
 Workforce Safety Chair

Health Department
Office: 865-215-5368
scott.white@knoxcounty.org

6. Arlington County
Jim Baker, MPA
Administrative Officer
Department of Human Services
Aging & Disability Services Division
703-228-1713 (Office)
jbaker@arlingtonva.us
7. Roanoke City Public Schools
Corey Allder
Supervisor of EL and World Language Programs
Title III Coordinator
Roanoke City Public Schools
(540) 853-1394
callder@rcps.info
8. West Virginia Division of Rehabilitation Services
Crystal Law
Phone: 304-625-6044 ext. 60567
Email: Crystal.G.Law@wv.gov
9. South Dakota Department of Human Services
Misty Black Bear
LTSS Assistant Director
Phone: 605 773-5433
E-mail: misty.blackbear@state.sd.us
10. Bristol Tennessee City Schools
Kimberly Amos
(423) 652-9451
amosk@btcs.org

8. Describe any green or environmental initiatives or policies.

2015 - Pledge for a Greener Tomorrow In 2015, Volatia took a monumental step by pledging to significantly reduce our paper usage and reliance to less than 1%. At that time, our operations were heavily dependent on paper, with a 100% usage rate due to the necessity of printing forms for various transactional, documentation, and approval processes.

2015-2018 - Embracing Digital Transformation To fulfill our commitment, Volatia embarked on a transformative journey to automate all of our workflows. This strategic shift allowed us to completely eliminate paper usage in any Volatia-initiated workflows within just three years. As a result, today, paper is only utilized when absolutely necessary, such as responding to RFPs that mandate physical copies or when supporting clients who specifically request certain forms in physical formats.

2015-Present - Fostering a Remote Work Culture Alongside our digital transformation, Volatia has also fostered a supportive employment environment that encourages our workforce to adopt remote work practices. This initiative aims to reduce the environmental impact associated with daily commutes, thereby contributing further to our green initiative.

By seamlessly integrating sustainability into our core operations and work culture, Volatia continues to lead by example in the realm of environmental stewardship. We are proud of the strides we have made and remain committed to exploring and adopting new ways to minimize our environmental footprint.

9. Describe any diversity programs or partners Supplier does business with and how Participating Public Agencies may use diverse partners through the Master Agreement. Indicate how, if at all, pricing changes when using the diversity program. If there are any diversity programs, provide a listing of diversity alliances and a copy of their certifications.

Affiliate Program Overview:

Volatia has developed an innovative affiliate program, which empowers small language companies by providing them access to Volatia's cutting-edge technological resources and infrastructure. This inclusive approach enables these businesses to thrive and efficiently serve their clients, all while bolstering local economies.

Commitment to Local and Diverse Partnerships:

Volatia is committed to including at least one local affiliate in every state across the nation on every contract opportunity we have active. Among these affiliates, we proudly partner with women and minority-owned businesses that hold certificates verifying their status. We meticulously choose our affiliates based on the services used, the frequency of those services, and the volume of work provided.

Transparency and Accountability:

We are willing and ready to provide documentation that clearly demonstrates these partnerships at any time during the contract term. We also pledge to make these partnerships a condition of the contract award. Following the award, upon request, we will provide a list of all affiliates who meet the diversity criteria, along with copies of their certifications.

Seamless Workflow for Public Agencies:

Participating Public Agencies can easily engage with our diverse partners through the Master Agreement by simply creating work orders in the usual manner. The client-facing

workflow remains unchanged; however, in the background, resources are shared and optimized among affiliates to meet specific needs or requests.

Revenue Sharing Model:

Our revenue sharing model guarantees that each affiliate receives a minimum of fifteen percent (15%) of the applicable spend on the supported account(s). Additionally, affiliates are paid fifty percent (50%) of the difference between the client billable amount and the interpreter payment balance. For example, if the client is invoiced \$50, and the interpreter is paid \$30, the affiliate receives \$10 as participation revenue, leaving \$10 for Volatia.

Diversity Program Pricing:

It's important to note that there are no pricing changes for Participating Public Agencies when utilizing our diversity program.

In conclusion, Volatia's affiliate program and our commitment to diverse partnerships exemplify our dedication to supporting local economies and promoting inclusivity in the language services industry. Through our innovative model, we ensure that both our clients and affiliates thrive, ultimately contributing to the richness and diversity of the communities we serve.

10. Indicate if Supplier holds any of the below certifications in any classified areas and include proof of such certification in your response:

a. Minority Women Business Enterprise (MBE or WBE)

Yes No

b. Small Business Enterprise (SBE) or Disadvantaged Business (DBE)

Yes No

c. Historically Underutilized Business (HUB)

Yes No

d. Historically Underutilized Business Zone Enterprise (HUBZone)

Yes No

e. Veteran Business Enterprise (VBE)

Yes No

f. Service-Disabled Veteran's Business Enterprise (SDVBE)

Yes ___ No X

If you responded yes to any designations in a-f, please list certifying agency(ies):

Commonwealth of Virginia, Department of Small Business & Supplier Diversity

11. Please describe any Affirmative Action Policy your company has in place.

Though Volatia places a large emphasis on the diversity of our interpreter workforce, at this time we do not have an Affirmative Action Plan in place. We are in process of preparing a compliant plan that meets the needs of our company, and upon contract award, will share this plan with GovMVMT once vetted and published. In lieu of this minor setback, we have provided a copy of our Equal Opportunity Policy which will provide you an overview of the steps Volatia takes to ensure the equal treatment of qualified applicants and employees.

C. Order Processing and Distribution

1. Describe your company's normal order processing procedure from point of customer contact through delivery and billing.

Information regarding this item can be found in number 3, below.

2. In what formats do you accept orders (telephone, ecommerce, etc.)?

Information regarding this item can be found in number 3, below.

3. Please describe your single system or platform for all phases of ordering, processing, delivery and billing.

On-Demand OPI and VRI – Access to on-demand over the phone and video remote interpretation services has never been easier. Through the use of Volatia's mobile and web applications, both available for download in the Apple and Google Play stores, all the County has to do is "plug and play", and they have direct access to language services.

- **Web App** – Accessing terpX through our web-based platform has a six-step user friendly process:

1. Login by going to <https://ims.volatia.com/Account/Login>.
2. Select the "On Demand OPI And VRI" tab from the Management Menu.



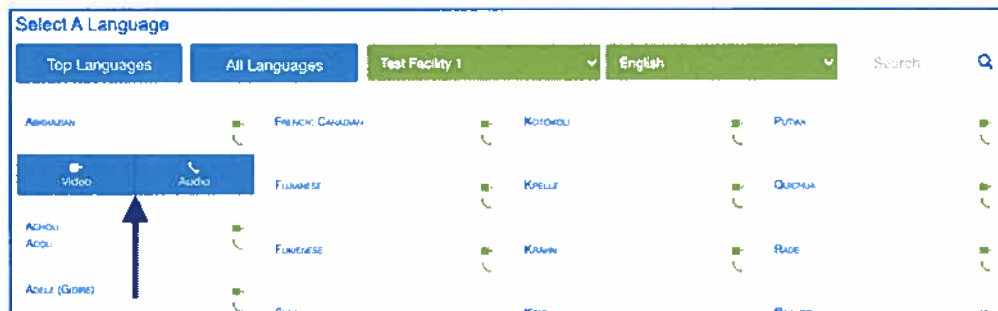
3. Select the client worksite facility from the dropdown menu.



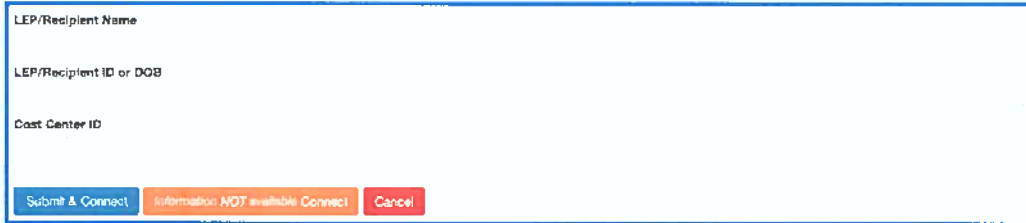
4. Select the desired language by either using the search box in the top right hand corner, or by scrolling through the list of languages.



5. Once you have chosen your desired language, you will be presented with the option to connect via video or phone.



6. Enter the LEP's name, ID or DOB, and Cost Center ID (if applicable). If you do not have this information, you can still proceed by selecting, "Information NOT Available: Connect."



A screenshot of a web form with three input fields: "LEP/Recipient Name", "LEP/Recipient ID or DOB", and "Cost Center ID". Below the fields are three buttons: "Submit & Connect" (blue), "Information NOT available: Connect" (orange), and "Cancel" (red).

- **Mobile App** – When using the terpX mobile platform, the County user follows this simple, four-step process:

1. Login to the Volatia app using the unique username and password that you, the user, have created.



2. Select your worksite facility by clicking the icon in the top right hand corner of the screen and choosing your facility from the dropdown menu.



- From the main menu, select your desired language and connection type.



- Enter the LEP's name, ID or DOB, and Cost Center ID (if applicable). If you do not have this information, you can still proceed by selecting, "Information NOT Available: Connect."

 A screenshot of a 'Work Order Form'. The form has several input fields for text entry. At the bottom of the form, there are three buttons: a blue 'Submit & Connect' button, an orange 'Information NOT Available: Connect' button, and a red 'Cancel' button.

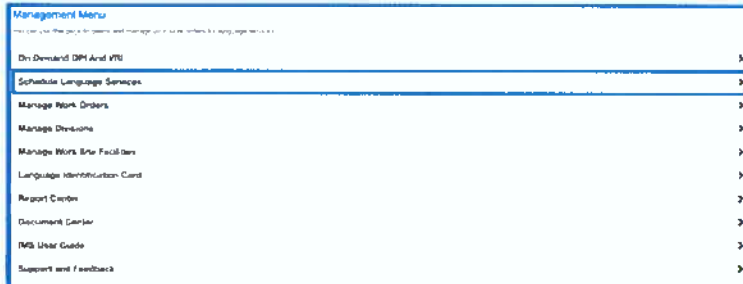
- Toll-Free Access** – In addition to access through our terpx platform, Volatia also provides on-demand over the phone interpretation services (only) through the use of a toll-free number and access code(s). The County will have the ability to assign an unlimited number of access codes to their facilities, departments, and/or individuals who will be utilizing these services. Clients dial the toll-free number, say their desired language, enter their access code, and are connected to an interpreter in 30 seconds or less. A Quick Reference Guide (QRG) with all access codes will be provided to the County that will outline this step-by-step process.

Schedule Language Services – To schedule a linguist for On-Site Interpretation (OSI), Over the Phone Interpretation (OPI), Video Remote Interpretation (VRI), and/or Document Translation, the County may use

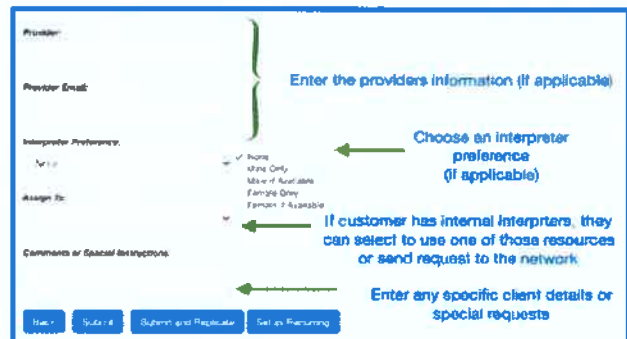
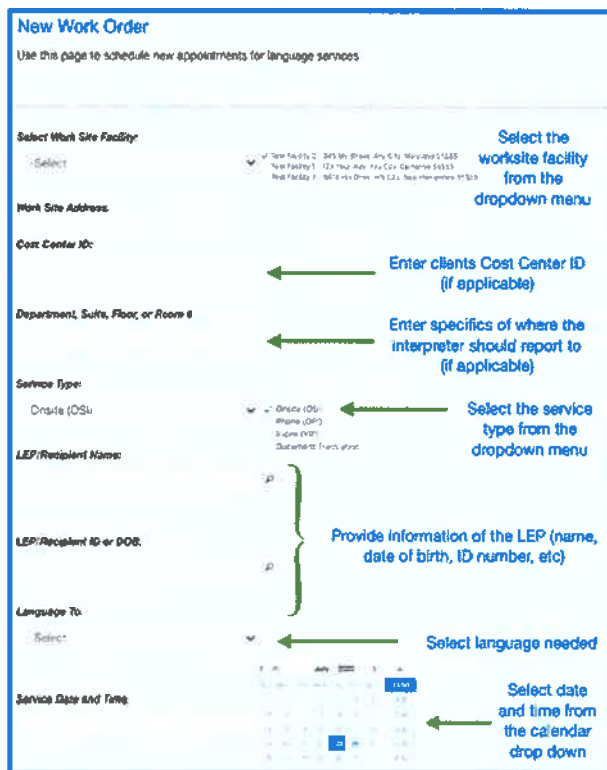


any of the three methods listed below.

- **TerpX Platform** - The County user will login to the terpX platform (<https://ims.volatia.com/Account/Login>) and select "Schedule Language Services" from the Management Menu.

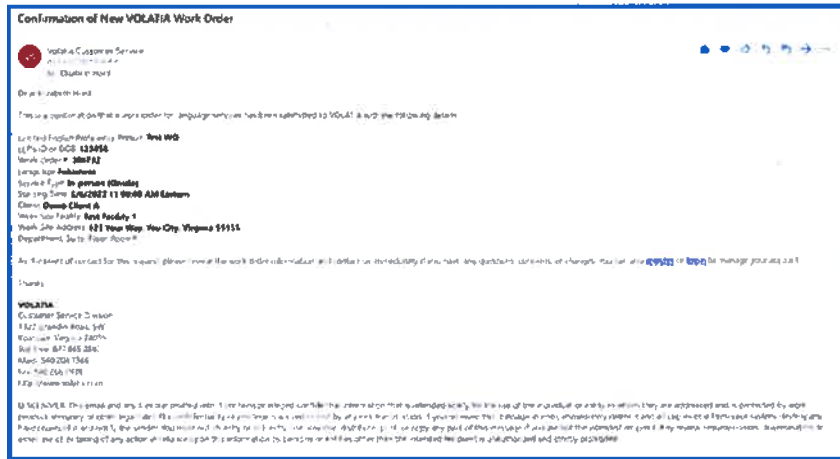


This will then prompt the user to complete a work order form, as displayed below.

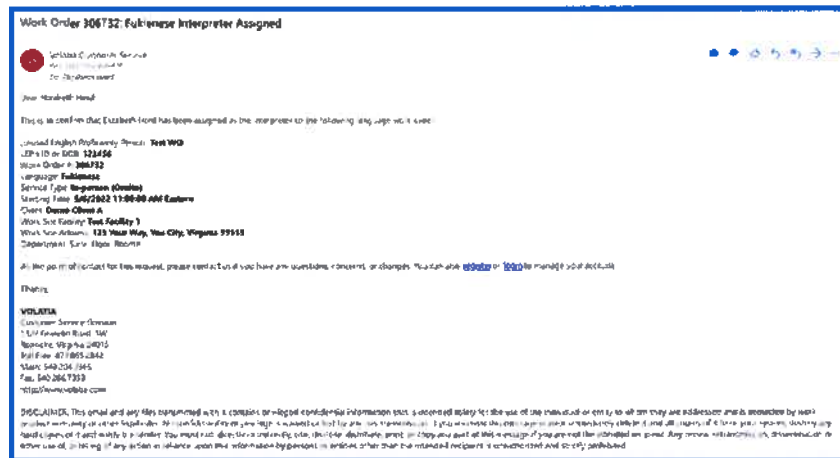


When choosing "Document Translation" from the "Service Type" dropdown, the County will be provided the selectable option to "Upload Attachments". The client user will then attach all applicable documents requiring translation services and select the preferred translation delivery date and time.

Every work order that is submitted through terpX will receive a confirmation email that includes the applicable assignment details and Volatia’s contact information.



Once an interpreter has been assigned to the work order, the County’s service requester will receive an “Interpreter Assigned” email with the work order information and name of the interpreter that will be fulfilling the assignment.



- **Email** – The County can also request services by emailing the below template to the Volatia Customer Service Team at customerservice@volatia.com.

1. Name of Service Requester:
2. Phone & Email Address of Service Requester:
3. Name of Facility:
4. Dept., Suite, Floor, or Room:
5. Service Type (OSI, OPI, VRI, or Document Translation):
6. Name of LEP Individual:
7. LEP DOB or ID #:

8. Date & Time of Service:
9. Language Needed:
10. Expected Duration:
11. Additional Information or Special Instructions:

- Phone – The County may also contact Volatia Customer Service at 540-562-8600 or toll-free at 877-VOLATIA (865-2842) to request and schedule their language services.

By accessing the following link (<https://www.volatia.com/grg>), the County can review further step by step instructions on how to access and use our services. Please note that these QRGs must be used with the unique account information that was provided to your organization's POC. The POC has the assigned phone number, access code(s), and the registration code for those desiring to create a terpX user profile.

4. Please state your normal payment terms and any quick-pay incentives available to Participating Public Agencies.

Payment terms are net 30 days.

5. State which forms of ordering allow the use of a procurement card and the accepted banking (credit card) affiliation.

All ordering methods as described allow the use of a procurement card for payments. Please note, there is a 3% processing fee for invoices that are over \$500 when reconciled with a credit card payment.

6. Describe how your company proposes to distribute the Products and Services nationwide.

1. Present Infrastructure and Sales Force Allocation

Volatia's Current Resources: A Strong National Footprint

Volatia has established a strong, widespread presence across the United States with a dedicated sales force of 97 agents. These agents are strategically located based on state size and potential market reach, ensuring optimal coverage for all regions. For instance, smaller states like Wyoming are served by a single dedicated agent, while larger states such as California and Texas are catered to by a team of 4 agents each. This arrangement ensures that every region, regardless of size, receives specialized attention.

2. Initial Outreach and Awareness Campaign

Raising Contract Awareness: Proactive Engagement with Qualified Entities

Upon being awarded the contract, Volatia's agents will swing into immediate action. Their primary mission will be to reach out to eligible agencies and entities within their respective states. With the combination of local knowledge and Volatia's market expertise, these agents will be instrumental in raising awareness about the new contract opportunity. They will provide essential information, address queries, and guide potential clients through the initial stages of the process.

3. Onboarding Assistance and Continued Support

Beyond Awareness: A Commitment to Seamless Integration

Raising awareness is just the first step. Volatia recognizes the importance of providing continuous support throughout the onboarding process. As such, our agents are equipped to assist agencies in understanding the intricacies of the contract, ensuring that all documentation is in order, and facilitating a smooth transition. Their local presence further ensures that help is always nearby, making the process as efficient and hassle-free as possible.

4. Scalability and Future Plans

Adapting to the Needs of the Contract: Dynamic Resource Allocation

Volatia remains committed to delivering the highest level of service. With a clear understanding that contract demands can evolve, we have provisions in place to scale our resources accordingly. If there arises a need for enhanced outreach or intensified support in certain states or regions, Volatia is prepared to augment its sales force, ensuring that every agency, regardless of its size or challenges, receives the support it needs. Our flexible strategy underscores our commitment to the success of this contract and the satisfaction of all involved agencies.

5. Concluding Commitment

Volatia's Pledge: Excellence Today, Preparedness for Tomorrow

In conclusion, Volatia's existing infrastructure, combined with our proactive approach and readiness to adapt, makes us the ideal partner to market this contract to agencies across the U.S. We are excited about the prospect of working closely with all eligible entities, ensuring that the benefits of the contract are fully realized. Awarding this contract to Volatia is an investment in a proven, strategic, and future-ready approach.

7. Identify all other companies that will be involved in the processing, handling or shipping of the Products and Services to the end user.

Volatia will be the sole processor and handler of all services, as provided.

8. Describe how Participating Public Agencies are ensured they will receive the Master Agreement pricing with your company's distribution channels, such as direct ordering, retail or in-store locations, distributors, etc. Describe how Participating Public Agencies verify and audit pricing to ensure its compliance with the Master Agreement.

At Volatia, we are committed to providing our Participating Public Agencies (PPAs) with the most transparent and efficient process when it comes to receiving the Master Agreement pricing.

Ensuring Master Agreement Pricing for Participating Public Agencies

1. Account Creation & Group ID Assignment

- As a first step, our agents will create accounts for new entities and assign them to a sector or account type. Following this, Volatia will generate a Group ID for each entity. This ID will serve as an automatic identifier for all participating agencies.
- 2. Access to Master Agreement Pricing**
 - Upon successful account creation and Group ID assignment, all entities will have access to the master agreement pricing. This ensures that each participating agency is aware of the negotiated rates and can benefit from the pricing structure agreed upon.
 - 3. Verification of Billing Rates**
 - Our system is designed to allow PPAs to verify their billing rates against the master agreement in real-time. This feature is vital in ensuring that the pricing is always compliant with the agreement.
 - 4. Distribution Channels**
 - Volatia utilizes various distribution channels, such as direct ordering, retail or in-store locations, and distributors. Our national sales force has been given the master agreement and is fully equipped to market it to participating agencies. This ensures that the master agreement pricing is consistently offered through all our channels, providing PPAs with various options to access the agreed-upon rates.
 - 5. Audit and Compliance**
 - Volatia has implemented a robust system for PPAs to verify and audit pricing to ensure its compliance with the Master Agreement. Our transparent process allows PPAs to have full visibility and control over the pricing they are charged, ensuring that it is always in line with the master agreement.

By following this chronological process, Volatia ensures that Participating Public Agencies are always receiving the Master Agreement pricing and have the tools necessary to verify and audit pricing for compliance. We are committed to maintaining transparency and integrity in our dealings with all participating agencies, ensuring that they can confidently partner with us.

9. Provide the number, size and location of your company's distribution facilities, warehouses and retail network, as applicable.

Volatia's services are provided through a network of linguists nationwide. As we are supplying a service, we do not operate via distribution facilities, warehouses, or retail networks.

10. Describe your ability to provide customized reports (i.e. commodity histories, purchase histories by department, etc.) for each Participating Public Agency.

Report Center – The County will also have access to a Report Center that is specific to your organization’s language usage. If a specific report is not already available, Volatia can customize any report, upon request.



The extensive reporting capabilities of the terpX platform will provide the County the ability to view their language service usage reports in real time.



In the “Rate Summary” tab, terpX displays our contracted rates in a clear and concise manner, displaying the service, units, rates, effective date, minimums, and increments, so the County always has visibility to what they are being billed.

Rate Summary
 The following chart provides a summary of current language service billing rates

Service	Units	Rate	Effective Date	Minimum	Increment
Onsite (OS)	Minutes	\$0.6333	2/1/2019	60	30
Phone (DP)	Minutes	\$1.0000	9/17/2019	1	1
Video (VR)	Minutes	\$1.0000	3/1/2021	1	1

Through access of the “Billing Summary” tab, the County is able to view all current outstanding balances. There is a tier breakdown with selectable options to view balances that are 0-30, 31-60, 61-90, 91-120, and >120 days past due. There is also an invoice history ledger that shows all past invoices. To view the details for any particular invoice, all the County has to do is click on the bill date.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK

Current Outstanding Balance

0-30 Days	31-60 Days	61-90 Days	91-120 Days	120+ Days	None
\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00

Private History

The following table lists all of the invoices that have been generated for this account. Click on the invoice number to view the invoice details.

Bill Date	Invoice	Hours	Service	Due Date	Paid	Balance
4/10/17	11	1	\$125.00	5/10/17	\$125	\$0.00
4/12/17	12	1	\$125.00	5/12/17	\$125	\$0.00
4/13/17	13	1	\$125.00	5/13/17	\$125	\$0.00
4/14/17	14	1	\$125.00	5/14/17	\$125	\$0.00
4/15/17	15	1	\$125.00	5/15/17	\$125	\$0.00
4/16/17	16	1	\$125.00	5/16/17	\$125	\$0.00
4/17/17	17	1	\$125.00	5/17/17	\$125	\$0.00
4/18/17	18	1	\$125.00	5/18/17	\$125	\$0.00
4/19/17	19	1	\$125.00	5/19/17	\$125	\$0.00
4/20/17	20	1	\$125.00	5/20/17	\$125	\$0.00
4/21/17	21	1	\$125.00	5/21/17	\$125	\$0.00

As detailed in the images below, County reports can be broken down by Language, Division, Facility, and Cost Center. Each report displays the number of requests (Work Orders), recipients (LEPs), facilities, total hours, and the total charge. Each report summary also has the capability of filtering data using the month and year dropdown options.

Language Summary

The following chart provides a statistical summary of language services segmented by language. The Work Order column shows the number of all unique work orders for that language. The Recipients column shows the number of all unique recipients for that language. The Facilities column shows the number of different work site facilities that requested services for that language. The Total Hours column shows the total number of hours devoted to that language. Click on the column headings to sort the data by that particular column.

Select Calendar Year: 2017

Select Calendar Month: March

Language	Work Orders	Recipients	Facilities	Total Hours	Total Charge
Spanish	22	3	2	0	\$11.64
Berber (Chimberbi)	16	16	2	33	\$1,000.31
French	7	2	2	0	\$8.04
Totals:	45	21		33	\$1,000.19

Division Summary

The following chart provides a statistical summary of division services segmented by division. The Work Order column shows the number of all unique work orders for that division. The Recipients column shows the number of all unique recipients for that division. The Facilities column shows the number of different work site facilities that requested services for that division. The Total Hours column shows the total number of hours devoted to that division. Click on the column headings to sort the data by that particular column.

Select Calendar Year: All

Select Calendar Month: All

Division	Work Orders	Recipients	Facilities	Total Hours	Total Charge
Division 1	151	78	8	183	\$7,435.02
Division 2	315	162	3	440	\$16,187.02
Totals:	466	240		623	\$23,622.04

Facility Summary

The following chart provides a statistical summary of facility services segmented by facility. The Work Order column shows the number of all unique work orders for that facility. The Recipients column shows the number of all unique recipients for that facility. The Facilities column shows the number of different work site facilities that requested services for that facility. The Total Hours column shows the total number of hours devoted to that facility. Click on the column headings to sort the data by that particular column.

Select Calendar Year: All

Select Calendar Month: All

Facility	Work Orders	Recipients	Facilities	Total Hours	Total Charge
Facility 1	150	64	5	110	\$4,345.81
Facility 2	52	42	1	3	\$298.42
Facility 3	21	39	1	4	\$248.72
Facility 4	52	14	1	1	\$107.12
Facility 5	25	7	1	1	\$174.10
Facility 6	1	4	1	2	\$207.75
Facility 7	3	3	1	2	\$5.00
Facility 8	145	101	7	191	\$42,245.39
Facility 9	145	102	7	192	\$42,245.39
Totals:	1211	344	22	700	\$89,210.99

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK

Cost Center Summary

The following chart provides a statistical summary of cost center services segmented by cost center.
 The Work Order column shows the number of all work orders for that cost center.
 The Requests column shows the number of all unique requests for that cost center.
 The Facilities column shows the number of different work, and facilities that required services for that cost center.
 The Total Hours column shows the total number of hours devoted to that cost center.
 Click on the column headings to sort the data by that particular column.

Select Calendar Year:
 2010

Select Calendar Month:
 All

Cost Center	Work Orders	Requests	Facilities	Total Hours	Total Charge
Unassigned	166	66	0	203	\$7,540.81
1234	1	1	1	0	\$4.56
Not Provided	14	1	2	0	\$19.00
Total:	181	68		203	\$7,564.37

11. Describe your company's ecommerce capabilities:

Volatia's services are not sold through a shopping store. Rather, Volatia offers OnDemand language solutions in over 300 languages, 24/7/365. Our services can be accessed by phone, mobile app, or through our proprietary platform, terpX. We have created quick reference guides that seamlessly provide training to your staff on how to access our solutions both for schedule and OnDemand needs (<https://www.volatia.com/qrg>).

- a. Include details about your company's ability to create punch out sites and accept orders electronically.

Volatia accepts work order electrically by email or via terpX. We have created quick reference guides that seamlessly provide training to your staff on how to access our solutions both for schedule and OnDemand needs (<https://www.volatia.com/qrg>).

- b. Provide detail on your company's ability to integrate with a Public Agency's ERP/purchasing system (Oracle, SAP, Jaggaer, etc.). Please include some details about the resources you have in place to support these integrations.

At this time, Volatia allows users to export reports in any format needed. API integration can be provided upon request. Volatia shall provide an implementation timeline once the scope of work has been clearly defined by Client.

D. Sales and Marketing

1. Provide a detailed ninety-day plan beginning from award date of the Master Agreement describing the strategy to immediately implement the Master Agreement as Supplier's preferred go-to market strategy for Public Agencies to Supplier's teams nationwide, including, but not limited to:

See 90 Day Implementation Plan for both A & B questions:

- a. Executive leadership endorsement and sponsorship of the award as the Supplier's go-to-market strategy within the first 10 days.

- b. Training and education of Supplier's national sales force with participation from the Supplier's executive leadership, along with the GovMVMТ team within the first 90 days.

90-Day Implementation Plan for Master Agreement as Supplier's Go-To Market Strategy for Public Agencies

Days 1-10: Executive Leadership Endorsement and Initial Preparations

- Day 1: Official contract award announcement to the entire organization.
- Days 2-3: An executive meeting will be conducted to discuss the strategic importance of the Master Agreement, establishing it as the Supplier's preferred go-to-market strategy for public agencies.
- Days 4-5: Drafting and sending out official internal communications, endorsed by the executive leadership, to inform all teams about the new strategy and its importance to the organization's objectives.
- Days 6-7: Organization of a launch event to mark the beginning of this initiative, with attendance from the executive leadership and the GovMVMТ team, to demonstrate high-level commitment and support.
- Days 8-10: Meetings with department heads to ensure alignment and to prepare for the training and education phase.

Days 11-60: Training and Education of National Sales Force - Phase 1

- Days 11-20: Development and finalization of the training program, in consultation with the GovMVMТ team, to include relevant content, case studies, and real-world applications.
- Days 21-30: Roll-out of the training program to the first batch of national sales force teams, which will include sessions conducted by executive leadership and the GovMVMТ team.
- Days 31-40: Collecting feedback from the first batch and making any necessary adjustments to the program.
- Days 41-50: Roll-out of the adjusted training program to the second batch of the national sales force.
- Days 51-60: Further feedback collection and final adjustments to the training program.

Days 61-90: Training and Education of National Sales Force - Phase 2 and Evaluation

- Days 61-70: Roll-out of the final training program to the remaining batches of the national sales force.
- Days 71-80: Continued support and additional resources provided to the sales force teams as they start implementing the new strategy in their respective markets.
- Days 81-90: Evaluation of the overall training program, gathering success stories, and identifying areas for improvement. A comprehensive report will

be prepared and shared with the executive leadership and the GovMVMT team.

Throughout this 90-day period, constant communication and support will be provided to the sales force teams to ensure they are equipped with the necessary knowledge, skills, and resources to effectively implement the Master Agreement as the Supplier's preferred go-to-market strategy for public agencies nationwide.

2. Provide a detailed 90-day plan beginning from award date of the Master Agreement describing the strategy to market the Master Agreement to current Participating Public Agencies, existing Public Agency customers of Supplier, as well as to prospective Public Agencies nationwide immediately upon award, including, but not limited to:

90-Day Plan to Market the Master Agreement To Current Participating Public Agencies for A & G questions:

- a. Creation and distribution of a co-branded press release to trade publications.
- b. Announcement, Master Agreement details and contact information published on the Provider's website within the first 90 days.
- c. Commitment to attendance and participation with GovMVMT at national (i.e. NIGP Annual Forum, etc.), regional (i.e. Regional NIGP Chapter meetings, Regional Summits, etc.) and provider-specific trade shows, conferences and meetings throughout the term of the Master Agreement.
- d. Commitment to attend, exhibit and participate at the NIGP Annual Forum in an area reserved by GovMVMT for partner providers. Booth space will be purchased and staffed by Supplier.
- e. Design and publication of national and regional advertising in trade publications throughout the term of the Master Agreement.
- f. Ongoing marketing and promotion of the Master Agreement throughout its term (case studies, collateral pieces, presentations, promotions, etc.)
- g. Dedicated GovMVMT internet web-based homepage on Supplier's website with:
 - GovMVMT Partners standard logo;
 - Copy of original Request for Proposal, including all addenda;
 - Copy of Master Agreement all amendments between Lead Public Agency and Supplier;
 - Marketing Materials;
 - Electronic link to GovMVMT website including the online registration page;

- A dedicated toll-free number and email address for GovMVMT.

90-Day Plan to Market the Master Agreement To Current Participating Public Agencies

Days 1-10: Creation and Distribution of Co-Branded Press Release, Website Announcement and Initial Contact with Current and Prospective Public Agencies

- Day 1-3: Creation of a co-branded press release with GovMVMT, detailing the Master Agreement and its benefits.
- Day 4-5: Distribution of the press release to various trade publications and key industry stakeholders.
- Day 6: Announcement of the Master Agreement details and contact information on Volatia's website.
- Day 7-10: Initiate contact with current Participating Public Agencies and existing Public Agency customers of Volatia to inform them of the new Master Agreement and its benefits.

Days 11-30: National and Regional Commitments and Designing of Advertising Materials

- Days 11-15: Commit to attendance and participation with GovMVMT at national and regional events, including the NIGP Annual Forum, Regional NIGP Chapter meetings, and regional summits.
- Days 16-20: Purchase booth space and start preparations for the NIGP Annual Forum, in cooperation with GovMVMT.
- Days 21-25: Design of national and regional advertising materials for trade publications.
- Days 26-30: Start the development of the dedicated GovMVMT internet web-based homepage on Volatia's website.

Days 31-60: Ongoing Marketing Efforts and Finalizing Dedicated Web-Based Homepage

- Days 31-40: Continuous marketing and promotion of the Master Agreement, including development of case studies, collateral pieces, presentations, and promotions.
- Days 41-50: Finalization and publication of the dedicated GovMVMT internet web-based homepage on Volatia's website, with all necessary elements as mentioned in the requirements.
- Days 51-60: Initiate the design and publication of national and regional advertising in trade publications.

Days 61-90: Strengthening Relationship with Government Accounts and Finalizing Marketing Initiatives

- Days 61-70: Emphasize to all current qualifying government accounts the benefits and better rates available through the Master Agreement.

- Days 71-80: Finalize all ongoing marketing initiatives and ensure they are in full swing, including the national and regional advertising in trade publications.
 - Days 81-90: Review and analyze the effectiveness of the marketing initiatives, making necessary adjustments and improvements for future promotions.
3. Describe how Provider will transition any existing Public Agency customers' accounts to the Master Agreement available nationally through GovMVM. Include a list of current cooperative contracts (regional and national) Supplier holds and describe how the Master Agreement will be positioned among the other cooperative agreements.

1. Communication and Offer of New Rates:

- Within the first 30 days, Volatia will send written communication to all current participating accounts, informing them of the new lower pricing structure available under the Master Agreement.
- The communication will clearly explain the benefits of transitioning to the Master Agreement, including access to preferred rates for all Volatia services.
- All current participating accounts will be given the option to move to the new agreement, thereby accepting the resulting terms and conditions.

2. Documentation and Reporting of Interactions:

- Volatia will document all efforts made to encourage entities to transition to the Master Agreement.
- A report of these interactions will be maintained, detailing the entities that have elected to move to the Master Agreement, as well as those that have chosen to retain their current agreement.

3. Provision of New Pricing for Covered Services and Products:

- For entities that elect to remain on their original agreement because a certain service they require is not covered under the new Master Agreement, Volatia shall provide the new pricing for all covered services and products.
- This ensures that entities are fully informed of their options and can make an educated decision regarding their agreement choice.

List of Current Cooperative Contracts:

- Norfolk Public School – Contract #2023000030
- Arlington County - AGREEMENT NO. 18-162-2-ITB
- Austin ISD - 22RFP080

Positioning of the Master Agreement Among Other Cooperative Agreements:

- The Master Agreement will be positioned as the premier agreement option, offering the lowest pricing structure for all Volatia services.

- It will be highlighted that the Master Agreement has been specially negotiated to provide the best value for Public Agencies nationwide.
 - Existing cooperative agreements will remain in place for entities that have specific needs not covered by the Master Agreement. However, the benefits of transitioning to the Master Agreement will be clearly communicated to all current participating accounts.
4. Acknowledge Supplier agrees to provide its logo(s) to GovMVMT and agrees to provide permission for reproduction of such logo in marketing communications and promotions. Acknowledge that use of GovMVMT logo will require permission for reproduction as well.

Volatia shall comply with this requirement.

5. Confirm Supplier will be proactive in direct sales of Supplier's Products and Services to Public Agencies nationwide and the timely follow up to leads established by GovMVMT. All sales materials are to use the GovMVMT logo. At a minimum, the Supplier's sales initiatives should communicate:

Volatia shall comply with this requirement.

- a. Master Agreement was competitively solicited and publicly awarded by a Lead Public Agency

Yes, Volatia agrees to this fact.

- b. Pricing Equal to or better than Supplier's Best available government pricing

Yes, Volatia agrees to this fact.

- c. No cost to participate

Yes, Volatia agrees to this fact.

- d. Non-exclusive

Yes, Volatia agrees to this fact.

6. Confirm Supplier will train its national sales force on the Master Agreement. At a minimum, sales training should include:

- a. Key features of Master Agreement

Yes, Volatia agrees to this fact.

- b. Working knowledge of the solicitation process

Yes, Volatia agrees to this fact.

- c. Awareness of the range of Public Agencies that can utilize the Master Agreement through GovMVM

Yes, Volatia agrees to this fact.

- d. Knowledge of benefits of the use of cooperative contracts

Yes, Volatia agrees to this fact.

7. Provide the name, title, email and phone number for the person(s) who will be responsible for:

- a. Executive Support

Baraka Kasongo

- b. Sales

Nancy Reichard

- c. Sales Support

Anna Hirshfield

- d. Marketing

Tyler Lyon

- e. Financial Reporting

Elizabeth Hord

- f. Accounts Payable

Vicki Risser

- g. Contracts

Jessica Kent

8. Describe how Supplier's national sales force is structured, including contact information for the highest level executive responsible for the sales team.

Volatia's national sales force is strategically structured to provide optimal coverage and specialized attention to every region across the United States.

1. Geographical Allocation: Our sales agents are distributed based on state size and potential market reach. This ensures that every state, regardless of its size, receives the attention it requires. Larger states like California and Texas are served by a team of four agents each, while smaller states like Wyoming have a single dedicated agent.

2. Executive Oversight: The national sales force is overseen by the highest-level executive responsible for sales, ensuring that the sales strategy is aligned with the company's overall objectives. At the pinnacle of the sales force structure is our founder and CEO, Baraka Kasongo. He not only oversees the operations of the sales team but also sets the strategic direction for the entire sales operation.

- Contact Information:
Phone: 540-562-8600
Email: baraka@volatia.com (copy sales@volatia.com)

3. Regional Sales Managers: Reporting directly to the CEO are the Regional Sales Managers. They are responsible for managing sales operations in various regions across the country. Their role includes setting regional targets, monitoring sales performance, and ensuring that the sales strategy aligns with the organization's objectives.

4. Sales Team Structure: Each state team is led by a Regional Sales Manager, who is responsible for overseeing the operations of the agents within that state, ensuring they meet their targets, and providing them with the necessary support and resources.

5. Support and Resources: Our sales agents are equipped with comprehensive training and access to a wide range of resources to help them effectively reach out to and support public agencies and other potential clients. This includes detailed information about our services, marketing materials, and case studies demonstrating our past successes.

9. Explain how your company's sales team will work with the GovMVMt team to implement, grow and service the national program.

To effectively implement, grow, and service the national program in partnership with the GovMVMt team, Volatia's sales team will engage in the following strategies:

1. Clear Communication and Collaboration:

- Establish open and transparent communication channels between Volatia's sales team and the GovMVMt team to ensure effective collaboration.
- Conduct regular joint meetings to discuss the program's progress, share insights, and strategize for future growth.

2. Integrated Training and Education:

- Organize joint training sessions where both teams can learn from each other's

expertise and experiences.

- Ensure that Volatia's sales team is well-versed in the specifics of the national program, including its objectives, benefits, and operational procedures.

3. Unified Marketing and Sales Strategy:

- Collaborate with the GovMVMT team to develop a unified marketing and sales strategy that leverages the strengths of both teams.
- Work together to identify key market segments and tailor the sales approach accordingly.

4. Customer Onboarding and Support:

- Work together to streamline the customer onboarding process, ensuring that new customers are seamlessly integrated into the national program.
- Provide ongoing support and assistance to customers, addressing their needs and resolving any issues promptly.

5. Data Sharing and Analysis:

- Share relevant data and insights between the two teams to better understand market trends, customer behavior, and program performance.
- Use the collected data to make informed decisions and optimize the program for better results.

6. Continuous Improvement:

- Regularly review the program's performance and gather feedback from both teams and customers.
- Use the feedback and performance data to make continuous improvements to the program, ensuring it remains competitive and delivers maximum value to customers.

In conclusion, Volatia's sales team will work closely with the GovMVMT team to implement, grow, and service the national program successfully. Through clear communication, integrated training, unified marketing and sales strategies, and continuous improvement, the partnership will drive the program to new heights, delivering exceptional value to customers nationwide.

10. Explain how your company will manage the overall national program throughout the term of the Master Agreement, including ongoing coordination of marketing and sales efforts, timely new Participating Public Agency account set-up, timely contract administration, etc.

Management of the Overall National Program Throughout the Term of the Master Agreement

1. Ongoing Coordination of Marketing and Sales Efforts:

- We will establish a dedicated team responsible for coordinating and managing the marketing and sales efforts for the national program.
- Regular strategy sessions will be conducted to assess the effectiveness of our marketing and sales efforts and to ensure alignment with the program's objectives.
- The marketing and sales teams will work collaboratively to develop and execute targeted campaigns aimed at increasing program participation and customer

engagement.

2. Timely New Participating Public Agency Account Set-Up:

- We will streamline the account set-up process to ensure that new Participating Public Agencies can quickly and easily join the program.
- A dedicated customer support team will be available to assist new Participating Public Agencies with the account set-up process and to answer any questions they may have.
- We will utilize technology, such as online forms and automated processes, to expedite the account set-up process.

3. Timely Contract Administration:

- A contract administration team will be responsible for managing all aspects of the contract, including compliance, reporting, and performance monitoring.
- Regular audits will be conducted to ensure compliance with the terms of the Master Agreement.
- We will utilize contract management software to track performance, manage documentation, and ensure timely delivery of services.

4. Customer Support and Relationship Management:

- A dedicated customer support team will be available to assist Participating Public Agencies with any questions or issues they may have.
- Regular check-ins will be conducted to ensure customer satisfaction and to gather feedback on the program.
- We will also establish a relationship management program to build and maintain strong relationships with Participating Public Agencies.

5. Data Analysis and Reporting:

- We will utilize data analysis tools to assess the performance of the national program and to identify areas for improvement.
- Regular reports will be generated to provide insights into program performance, customer satisfaction, and other key metrics.
- The data and insights gathered will be used to make informed decisions and to continuously improve the program.

In conclusion, we have a comprehensive plan in place to manage the overall national program throughout the term of the Master Agreement. Through ongoing coordination of marketing and sales efforts, timely account set-up, efficient contract administration, and a strong focus on customer support and relationship management, we are committed to delivering a successful and impactful program for Participating Public Agencies nationwide.

11. While it is anticipated many Public Agencies will be able to utilize the Master Agreement without further formal solicitation, there may be circumstances where Public Agencies will issue their own solicitations. The following options are available when responding to a solicitation for Products covered under the Master Agreement. Describe your company's strategies under these options when responding to a solicitation.

a. Respond with Master Agreement pricing (Contract Sales reported to GovMVMt).

Volatia shall support this option.

b.If competitive conditions require pricing lower than the standard Master Agreement not-to-exceed pricing, Supplier may respond with lower pricing through the Master Agreement. If Supplier is awarded the Contract, the sales are reported as contract sales to GovMVMT under the Master Agreement.

Volatia shall support this option.

c. Respond with pricing higher than Master Agreement online in the unlikely event that the Public Agency refuses to utilize Master Agreement (Contract sales are not reported to GovMVMT).

Volatia shall support this option.

d.If alternative or multiple proposals are permitted, respond with pricing higher than Master Agreement, and include Master Agreement as the alternate or additional proposal.

Volatia shall support this option.

12. Describe your company's sales goals for this Contract if awarded the Master Agreement, including targeted dollar volume by year:

\$1,500,000.00 in year one
\$2,500,000.00 in year two
\$4,000,000.00 in year three

E. Additional Information

1. Please use this opportunity to describe any other offerings your organization can provide that you feel will provide additional value and benefit to a Participating Public Agency.

A featured product that set's Volatia apart is our ability to provide and support bi-directional language access program (<https://www.volatia.com/leplines>). With Volatia's technology, you can now empower your Limited English Proficient (LEP) clients to access your services whenever they want. With an LEP Call-In line, your client will be able to connect to an interpreter of his or her native language first, and then connect to your staff. Here is how it works:

When an LEP individual calls the LEP line, he or she will be able to connect to an interpreter of his or her native language first. The interpreter will greet the LEP caller and then then conference a member of your staff into the call.

When your staff answers, the interpreter will introduce you to the LEP caller and begin interpreting the session. If no one answers the call to the facility or department the LEP

caller wishes to reach, the interpreter can call as many other contacts as the LEP caller would like to try.

Set Up

Standard Set Up: Volatia assigns a local number to each facility or department in your organization. Your organization simply provides the number(s) to your LEP clients for use as needed.

Optional Set Up: Volatia provides the local number(s) for each facility or department to your IT for them to use in your Interactive Voice Response (IVR) Phone System. An example IVR menu might say something to the effect of "Thank you for calling XYZ. For English press 1, for all other languages press 2." The IVR system then routes the call to the number issued by Volatia.

Billing

A work order is generated each time a call is placed by an LEP individual to your organization. As soon as the interpreter connects, your organization will be invoiced for the call per minute at the rate established in our services agreement for phone interpreter services.

The billing starts when the interpreter connects to the call from the LEP individual, and it ends when the LEP individual hangs up. A report of the call can be found in your terpx account at any time.

Awareness Campaign

Once the LEP Call-In Lines are set up, we recommend that a formal communication be sent to all of to your existing LEP clients as part of your awareness campaign. Many organizations have found it beneficial to do a press release and showcase this program to various media outlets as a DEI (Diversity, Equity, and Inclusion) initiative for the communities they serve.

Thereafter, it is a best practice to add your LEP Call-In Line number on your website and any other marketing information that display your organization's contact information.

EXHIBIT C
ADMINISTRATION AGREEMENT

This ADMINISTRATION AGREEMENT ("Agreement") is made as of (Insert Date), by and between GovMVMT ("GovMVMT Purchasing Cooperative") and ("Supplier").

RECITALS

WHEREAS, the ("Lead Public Agency") has entered into a certain Master Agreement dated as of (enter date), referenced as Agreement (No.#), by and between Lead Public Agency and Supplier (as amended from time to time in accordance with the terms thereof, the "Master Agreement") for the purchase of (the "Products and Services");

WHEREAS, the Master Agreement provides that any state, county, city, special district, local government, school district, private K-12 school, technical or vocational school, higher education institution (including community colleges, colleges and universities, both public and private), other government agency or nonprofit organization (each a "Public Agency" and collectively, "Public Agencies") may purchase Products and Services at the prices indicated in the Master Agreement upon prior registration with GovMVMT, in which case the Public Agency becomes a "Participating Public Agency";

WHEREAS, GovMVMT has the administrative and legal capacity to administer purchases under the Master Agreement to Participating Public Agencies;

WHEREAS, GovMVMT serves in an administrative capacity for the Lead Public Agency and other lead public agencies in connection with other master agreements offered by GovMVMT;

WHEREAS, Lead Public Agency desires GovMVMT to proceed with administration of the Master Agreement on the same basis as other master agreements;

WHEREAS, "GovMVMT Purchasing Cooperative" is a trade name licensed by IGSA

WHEREAS, GovMVMT and Supplier desire to enter into this Agreement to make available the Master Agreement to Participating Public Agencies.

NOW, THEREFORE, in consideration of the mutual covenants contained in this Agreement, GovMVMT and Supplier hereby agree as follows:

ARTICLE I
GENERAL TERMS AND CONDITIONS

1.1 The Master Agreement, attached hereto as Exhibit A and incorporated herein by reference as though fully set forth herein, and the terms and conditions contained therein shall apply to this Agreement except as expressly changed or modified by this Agreement.

1.2 GovMVMT shall be afforded all of the rights, privileges and indemnifications afforded to Lead Public Agency under the Master Agreement, and such rights, privileges and indemnifications shall accrue and apply with equal effect to GovMVMT under this Agreement including, without limitation, Supplier's obligation to provide insurance and indemnifications to Lead Public Agency.

1.3 Supplier shall perform all duties, responsibilities and obligations required under the Master Agreement.

1.4 GovMVMT shall perform all of its duties, responsibilities and obligations as administrator of purchases under the Master Agreement as set forth herein, and Supplier acknowledges that GovMVMT shall act in the capacity of administrator of purchases under the Master Agreement.

1.5 With respect to any purchases made by Lead Public Agency or any Participating Public Agency pursuant to the Master Agreement, GovMVMT (a) shall not be construed as a dealer, re- marketer, representative, partner, or agent of any type of Supplier, Lead Public Agency or such Participating Public Agency, (b) shall not be obligated, liable or responsible (i) for any orders made by Lead Public Agency, any Participating Public Agency or any employee of Lead Public Agency or a Participating Public Agency under the Master Agreement, or (ii) for any payments required to be made with respect to such order, and (c) shall not be obligated, liable or responsible for any failure by a Participating Public Agency to (i) comply with procedures or requirements of applicable law or ordinance, or (ii) obtain the due authorization and approval necessary to purchase under the Master Agreement. GovMVMT makes no representations or warranties with respect to any minimum purchases required to be made by Lead Public Agency, any Participating Public Agency, or any employee of Lead Public Agency or a Participating Public Agency under the Master Agreement.

ARTICLE II

TERM OF AGREEMENT

2.1 This Agreement is effective as of (Insert Date) and shall terminate upon termination of the Master Agreement or any earlier termination in accordance with the terms of this Agreement, provided, however, that the obligation to pay all amounts owed by Supplier to GovMVMT through the termination of this Agreement and all indemnifications afforded by Supplier to GovMVMT shall survive the term of this Agreement.

ARTICLE III

REPRESENTATIONS AND COVENANTS

3.1 GovMVMT views the relationship with Supplier as an opportunity to provide benefits to the Lead Public Agency, Participating Public Agencies and the Supplier. The successful foundation of the relationship requires certain representations and covenants from both GovMVMT and Supplier.

3.2 GovMVMT Representations and Covenants.

(a) **Marketing**. GovMVMT shall proactively market the Master Agreement to Public Agencies using resources such as a network of sponsors or sponsorships including the Advisory Council which is comprised of procurement professionals from around the country. In addition, the GovMVMT staff shall make best efforts to enhance Supplier's marketing efforts through meetings with Public Agencies, participation in key events and tradeshow and other marketing activity such as advertising, articles and promotional campaigns.

(b) **Training and Knowledge Management Support**. GovMVMT shall provide support for the education, training and engagement of Supplier's sales force as provided herein. Through its staff (each, a "**Program Manager**" and collectively, the "**Program Managers**"), GovMVMT shall, with scheduling assistance from Supplier, conduct training sessions and conduct calls jointly with Supplier to Public Agencies. GovMVMT shall also provide Supplier with access to GovMVMT' private intranet website which provides presentations, documents and information to assist Supplier's sales force in effectively promoting the Master Agreement.

3.3 **Supplier's Representations and Covenants**. Supplier hereby represents and covenants as follows in order to ensure that Supplier is providing the highest level of public benefit to Participating Public Agencies (such representations and covenants are sometimes referred to as "**Supplier's Commitments**" and are comprised of the Executive Commitment, Value Commitment, Differentiator Commitment and Sales and Marketing Commitment):

(a) **Executive Commitment**

(i) A true partnership: Supplier shall have full commitment of the Master Agreement from the highest executive level of the organization at any given time. This includes being supported by the supplier's senior executive management.

(ii) The pricing, terms and conditions of the Master Agreement shall be the Supplier's preferred contractual offering of Products and Services to all eligible Public Agencies. All of Supplier's direct and indirect marketing and sales efforts to Public Agencies shall demonstrate that the Master Agreement is Supplier's preferred offering and not just one of Supplier's contract options.

(iii) Supplier's sales force (including inside, direct and/or authorized dealers, distributors, and representatives) shall always present the Master Agreement when marketing Products or Services to Public Agencies.

(iv) Supplier shall advise all Public Agencies that are existing customers of Supplier as to the pricing and other value offered through the Master Agreement.

(v) Upon authorization by a Public Agency, Supplier shall transition such Public Agency to the pricing, terms and conditions of the Master Agreement.

(vi) Supplier shall provide a national/senior management level representative with the authority and responsibility to ensure that the Supplier's Commitments are maintained at all times. Supplier shall also designate a lead referral contact person who shall be responsible for receiving communications from GovMVMT concerning new Participating Public Agency registrations and for

ensuring timely follow-up by Supplier's staff to requests for contact from Participating Public Agencies. Supplier shall also provide the personnel necessary to implement and support a supplier-based internet web page dedicated to Supplier's GovMVMT program and linked to GovMVMT' website and shall implement and support such web page.

(vii) Supplier shall demonstrate in its procurement solicitation response and throughout the term of the Master Agreement that national/senior management fully supports the GovMVMT program and its commitments and requirements. National/Senior management is defined as the executive(s) with companywide authority.

(viii) Where Supplier has an existing contract for Products and Services with a state, Supplier shall notify the state of the Master Agreement and transition the state to the pricing, terms and conditions of the Master Agreement upon the state's request. Regardless of whether the state decides to transition to the Master Agreement, Supplier shall offer the Master Agreement to all Public Agencies located within the state.

(b) **Value Commitment**

(i) Supplier represents to GovMVMT that the overall pricing in the scope of products and services offered under the Master Agreement is equal to or better than any other pricing options it offers to public agencies. Supplier's pricing shall be evaluated on either an overall project basis or the Public Agency's actual usage for more frequently purchased Products and Services.

(ii) **Contracts Offering Lower Prices.** If a pre-existing contract and/or a Public Agency's unique buying pattern provide one or more Public Agencies a lower price than that offered under the Master Agreement, Supplier shall match that lower pricing under the Master Agreement and inform the eligible Public Agencies that the lower pricing is available under the Master Agreement. If an eligible Public Agency requests to be transitioned to the Master Agreement, Supplier shall do so and report the Public Agency's purchases made under the Master Agreement going forward. The price match only applies to the eligible Public Agencies. Below are three examples of Supplier's obligation to match the pricing under Supplier's contracts offering lower prices.

(A) Supplier holds a state contract with lower pricing that is available to all Public Agencies within the state. Supplier would be required to match the lower state pricing under the Master Agreement and make it available to all Public Agencies within the state.

(B) Supplier holds a regional cooperative contract with lower pricing that is available only to the ten cooperative members. Supplier would be required to match the lower cooperative pricing under the Master Agreement and make it available to the ten cooperative members.

(C) Supplier holds a contract with an individual Public Agency. The Public Agency contract does not contain any cooperative language and therefore other Public Agencies are not eligible to utilize the contract. Supplier would be required to match the lower pricing under the Master Agreement and make it available only to the individual Public Agency.

(iii) **Deviating Buying Patterns.** Occasionally GovMVMT and Supplier may interact

with a Public Agency that has a buying pattern or terms and conditions that considerably deviate from the normal Public Agency buying pattern and terms and conditions and causes Supplier's pricing under the Master Agreement to be higher than an alternative contract held by Supplier. This could be created by a unique end-user preference or requirements. In the event that this situation occurs, Supplier may address the issue by lowering the price under the Master Agreement on the item(s) causing the large deviation for that Public Agency. Supplier would not be required to lower the price for other Public Agencies.

(iv) **Supplier's Options in Responding to a Third-Party Procurement Solicitation.** While it is the objective of GovMVM T to encourage Public Agencies to piggyback on to the Master Agreement rather than issue their own procurement solicitations, GovMVM T recognizes that for various reasons some Public Agencies will issue their own solicitations. The following options are available to Supplier when responding to a Public Agency solicitation:

(A) Supplier may opt not to respond to the procurement solicitation. Supplier may make the Master Agreement available to the Public Agency as a comparison to its solicitation responses.

(B) Supplier may respond with the pricing, terms and conditions of the Master Agreement. If Supplier is awarded the contract, the sales would be reported as sales under the Master Agreement.

(C) If competitive conditions require pricing lower than the standard Master Agreement pricing, Supplier may submit lower pricing through the Master Agreement. If Supplier is awarded the contract, the sales would be reported as sales under the Master Agreement. Supplier would not be required to extend the lower price to other Public Agencies.

(D) Supplier may respond to the procurement solicitation with pricing that is higher (net to buyer) than the pricing offered under the Master Agreement. If awarded a contract, Supplier shall still be bound by all obligations set forth in this Section 3.3, including, without limitation, the requirement to continue to advise the awarding Public Agency of the pricing, terms and conditions of the Master Agreement.

(E) Supplier may respond to the procurement solicitation with pricing that is higher (net to buyer) than the pricing offered under the Master Agreement and if an alternative response is permitted, Supplier may offer the pricing under the Master Agreement as an alternative for consideration.

c) **Differentiator Commitment.** Supplier shall demonstrate the value, competitive scope, and differentiating factors of the agreement against alternative procurement options in the marketplace at every opportunity. The success of this program lies directly with properly positioning this contract vehicle as the premier cooperative purchasing option for public agencies.

Supplier can accomplish this by highlighting such facts as:

- Lead Public Agency process
- Non-profit structure
- Public Benefit Programs
- Value Commitments

- Advisory Council Oversight
- Dedicated Field Team

Supplier agrees that while this agreement brings significant value to Public Agencies, it is not an exclusive agreement and can be utilized at the discretion of the participating Public Agencies.

(d) **Sales and Marketing Commitment.** Supplier shall market the Master Agreement through Supplier's sales force or dealer network that is properly trained, engaged and committed to properly position the value of the Master Agreement as Supplier's preferred contract for Public Agencies. Supplier's sales force compensation and incentives shall be greater than or equal to the compensation and incentives earned under other contracts to Public Agencies.

(i) **Supplier Sales.** Supplier shall be responsible for proactive sales of Supplier's Products and Services to Public Agencies and the timely follow-up to sales leads identified by GovMVMT. Use of product catalogs, targeted advertising, direct mail, online marketing and other sales initiatives are encouraged. Supplier's sales materials targeted towards Public Agencies should include the GovMVMT logo. GovMVMT hereby grants to Supplier, during the term of this Agreement, a non-exclusive, revocable, non-transferable, license to use the GovMVMT name, trademark, and logo solely to perform its obligations under this Agreement, and for no other purpose. Any goodwill, rights, or benefits derived from Supplier's use of the GovMVMT name, trademark, or logo shall inure to the benefit of GovMVMT. GovMVMT shall provide Supplier with its logo and the standards to be employed in the use of the logo. During the term of the Agreement, the Supplier shall provide GovMVMT with its logo and the standards to be employed in the use of the logo for purposes of reproducing and using Supplier's name and logo in connection with the advertising, marketing and promotion of the Master Agreement to Public Agencies. Supplier shall assist GovMVMT by providing camera-ready logos and by participating in related trade shows and conferences. At a minimum, Supplier's sales initiatives shall communicate that (i) the Master Agreement was competitively solicited by the Lead Public Agency, (ii) the Master Agreement provides pricing equal to or better than the Supplier's best available pricing and value to eligible agencies, (iii) there is no cost to Participating Public Agencies, and (iv) the Master Agreement is a non-exclusive contract.

(ii) **Branding and Logo Compliance.** Supplier shall be responsible for complying with the GovMVMT branding and logo standards and guidelines. Prior to use by Supplier, all GovMVMT related marketing material must be submitted to GovMVMT for review and approval.

(iii) **Sales Force Training.** Supplier shall train its national sales force on the Master Agreement and GovMVMT program. GovMVMT shall be available to train on a national, regional or local level and generally assist with the education of sales personnel.

(iv) Participating Public Agency Access. Supplier shall establish the following communication links to facilitate customer access and communication:

(A) A dedicated GovMVMT internet web-based homepage that is accessible from Supplier's homepage or main menu navigation containing:

- (1) GovMVMT standard logo;
- (2) Copy of original procurement solicitation and all addenda;
- (3) Copy of Master Agreement including all amendments.
- (4) Summary of Products and Services pricing.
- (5) Electronic link to GovMVMT' online registration page;
- (6) Other promotional material as requested by GovMVMT.
- (7) A dedicated toll-free national hotline for inquiries regarding GovMVMT.
- (8) A dedicated email address for general inquiries in the following format: GovMVMT@(name of supplier).com.

(v) Electronic Registration. Supplier shall be responsible for ensuring that each Public Agency has completed GovMVMT's online registration process prior to processing the Public Agency's first sales order.

(vi) Supplier's Performance Review. Upon request by GovMVMT, Supplier shall participate in a performance review meeting with GovMVMT to evaluate Supplier's performance of the covenants set forth in this Agreement.

(vii) Supplier Content. Supplier may, from time to time, provide certain graphics, media, and other content to GovMVMT (collectively "Supplier Content") for use on GovMVMT websites and for general marketing and publicity purposes. During the term of the Agreement, Supplier hereby grants to GovMVMT and its affiliates a non-exclusive, worldwide, free, transferrable, license to reproduce, modify, distribute, publicly perform, publicly display, and use Supplier Content in connection with GovMVMT websites and for general marketing and publicity purposes, with the right to sublicense each and every such right. Supplier warrants that: (a) Supplier is the owner of or otherwise has the unrestricted right to grant the rights in and to Supplier Content as contemplated hereunder; and (b) the use of Supplier Content and any other materials or services provided to GovMVMT as contemplated hereunder will not violate, infringe, or misappropriate the intellectual property rights or other rights of any third party

3.4 Breach of Supplier's Representations and Covenants. The representations and covenants set forth in this Agreement are the foundation of the relationship between GovMVMT and Supplier. If Supplier is found to be in violation of, or non-compliance with, one or more of the representations and covenants set forth in this Agreement, Supplier shall have ninety (90) days from the notice of default to cure such violation or non-compliance and, if Supplier fails to cure such violation or non-compliance within such notice period, it shall be deemed a cause for immediate

termination of the Master Agreement at Lead Public Agency's sole discretion or this Agreement at GovMVMT's sole discretion.

3.5 Indemnity. Supplier hereby agrees to indemnify and defend GovMVMT, and its parent companies, subsidiaries, affiliates, shareholders, member, manager, officers, directors, employees, agents, and representatives from and against any and all claims, costs, proceedings, demands, losses, damages, and expenses (including, without limitation, reasonable attorney's fees and legal costs) of any kind or nature, arising from or relating to, any actual or alleged breach of any of Supplier's representations, warranties, or covenants in this Agreement.

ARTICLE IV **PRICING AUDITS**

4.1 Supplier shall, at Supplier's sole expense, maintain an accounting of all purchases made by Lead Public Agency and Participating Public Agencies under the Master Agreement. GovMVMT and Lead Public Agency each reserve the right to audit the accounting for a period of three (3) years from the time such purchases are made. This audit right shall survive termination of this Agreement for a period of one (1) year from the effective date of termination. GovMVMT shall have the authority to conduct random audits of Supplier's pricing that is offered to Participating Public Agencies at GovMVMT's sole cost and expense. Notwithstanding the foregoing, in the event that GovMVMT is made aware of any pricing being offered to three (3) or more Participating Public Agencies that is materially inconsistent with the pricing under the Master Agreement, GovMVMT shall have the ability to conduct a reasonable audit of Supplier's pricing at Supplier's sole cost and expense during regular business hours upon reasonable notice. GovMVMT may conduct the audit internally or may engage a third-party auditing firm on a non-contingent basis. Supplier shall solely be responsible for the cost of the audit. In the event of an audit, the requested materials shall be provided in the format and at the location where kept in the ordinary course of business by Supplier.

ARTICLE V **FEES & REPORTING**

5.1 Administrative Fees. Supplier shall pay to GovMVMT a monthly administrative fee based upon the total sales price of all purchases shipped and billed pursuant to the Master Agreement, excluding taxes, in the amount of one and three-quarter percent (1.75% or lower according to the volume tiers below) of aggregate purchases made during each calendar month (individually and collectively, "Administrative Fees"). GovMVMT was founded on the principle of large volumes of purchases resulting in aggressive discounts and a great resulting value for those purchasing entities. We believe in additional value and increased savings that result from growth in the program and larger spend volume. This value should exist for the public agency and the supplier, and thus an incentivized tier structure has been developed to assure that these savings are passed along to the agencies and suppliers in the program. Tiered Administrative fees are outlined below based on Suppliers

Annual sales volume. Supplier's annual sales shall be measured on a calendar year basis. All Administrative Fees shall be payable in U.S. Dollars and shall be made by wire to GovMVMT, or its designee or trustee as may be directed in writing by GovMVMT.

Administrative Fees shall be due and payable within thirty (30) days of the end of each calendar month for purchases shipped and billed during such calendar month. GovMVMT agrees to pay to Lead Public Agency five percent (5%) of all Administrative Fees received from Supplier to help offset Lead Public Agency's costs incurred in connection with managing the Master Agreement nationally.

Administrative Fee Tiers*

Annual Contract Spend Low	Annual Contract Spend High	Administrative Fee
\$0	\$15,000,000	1.75%
\$15,000,001	\$25,000,000	1.5%
\$25,000,001	\$75,000,000	1.25%
\$75,000,001	> \$75,000,001	1.00%

*Tiered administrative fee structure is based on annual reported sales volume. Sales volume is calculated from January 1st – December 31st of the current calendar year. When a tier level is met, supplier will be moved to subsequent fee percentage on the next reported monthly report.

5.2 Sales Reports. Within thirty (30) days of the end of each calendar month, Supplier shall deliver to GovMVMT an electronic accounting report, in the format prescribed by Exhibit B, attached hereto, summarizing all purchases made under the Master Agreement during such calendar month ("Sales Report"). All purchases indicated in the Sales Report shall be denominated in U.S. Dollars. All purchases shipped and billed pursuant to the Master Agreement for the applicable calendar month shall be included in the Sales Report. Submitted reports shall be verified by GovMVMT against its registration database. Any data that is inconsistent with the registration database shall be changed prior to processing. GovMVMT reserves the right upon reasonable advance notice to Supplier to change the prescribed report format to accommodate the distribution of the Administrative Fees to its future potential program sponsors and state associations.

5.3 Exception Reporting/Sales Reports Audits. GovMVMT or its designee may, at its sole discretion, compare Supplier's Sales Reports with Participating Public Agency records or other sales analysis performed by Participating Public Agencies, future potential sponsors, advisory council members or GovMVMT staff. If there is a material discrepancy between the Sales Report and such records or sales analysis as determined by GovMVMT, GovMVMT shall notify Supplier in writing and Supplier shall have thirty (30) days from the date of such notice to resolve the discrepancy to

GovMVMT's reasonable satisfaction. Upon resolution of the discrepancy, Supplier shall remit payment to GovMVMT's trustee within fifteen (15) calendar days. Any questions regarding an exception report should be directed to GovMVMT in writing to reporting@govmvt.org. If Supplier does not resolve the discrepancy to GovMVMT's reasonable satisfaction within thirty (30) days, GovMVMT shall have the right to engage outside services to conduct an independent audit of Supplier's reports. Supplier shall solely be responsible for the cost of the audit.

5.4 Online Reporting. Within forty-five (45) days of the end of each calendar month, GovMVMT shall provide online reporting to Supplier containing Supplier's sales reporting for such calendar month. Supplier shall have access to various reports through the GovMVMT intranet website. Such reports are useful in resolving reporting issues and enabling Supplier to better manage their Master Agreement.

5.5 Usage Reporting. Within thirty (30) days of the end of each contract year, Supplier shall deliver to GovMVMT an electronic usage report of all sales under the Master Agreement, including:

- (i) Supplier's Product Number
- (ii) Product Description
- (iii) Manufacturer Name
- (iv) Manufacturer Number
- (v) Unit of Measure
- (vi) GovMVMT Price
- (xx) Number of times ordered
- (xxi) Units sold
- (ix) Sales by Manufacturer

5.6 Supplier's Failure to Provide Reports or Pay Administrative Fees. Failure to provide a Sales Report or pay Administrative Fees within the time and in the manner specified herein shall be regarded as a material breach under this Agreement and if not cured within thirty (30) days of written notice to Supplier, shall be deemed a cause for termination of the Master Agreement at Lead Public Agency's sole discretion or this Agreement at GovMVMT's sole discretion. All Administrative Fees not paid within thirty (30) days of the end of the previous calendar month shall bear interest at the rate of one and one-half percent (1.5%) per month until paid in full.

ARTICLE VI

MISCELLANEOUS

6.1 Entire Agreement. This Agreement supersedes any and all other agreements, either oral or in writing, between the parties hereto with respect to the subject matter hereof, and no other agreement, statement, or promise relating to the subject matter of this Agreement which is not contained herein shall be valid or binding.

6.2 Assignment.

(a) Supplier. Neither this Agreement nor any rights or obligations hereunder shall be assignable by Supplier without prior written consent of GovMVMT, and any assignment without such consent shall be void.

(b) GovMVMT. This Agreement and any rights or obligations hereunder may be assigned by GovMVMT in GovMVMT's sole discretion, to an existing or newly established legal entity that has the authority and capacity to perform GovMVMT's obligations hereunder.

6.3 Notices. All reports, notices or other communications given hereunder shall be delivered by first-class mail, postage prepaid, or overnight delivery requiring signature on receipt to the addresses as set forth below. GovMVMT may, by written notice delivered to Supplier, designate any different address to which subsequent reports, notices or other communications shall be sent.

GovMVMT:	GovMVMT 7629 NW 143 rd St Alachua, FL 32615 Attn: Program Manager Administration
----------	--

Supplier:	<u>Volatia Language Network, Inc.</u> <u>1327 Grandin Rd. SW</u> <u>Roanoke, VA 24015</u> <hr/> <u>Attn: GovMVMT Program Manager</u>
-----------	---

6.4 Severability. If any provision of this Agreement shall be deemed to be, or shall in fact be, illegal, inoperative, or unenforceable, the same shall not affect any other provision or provisions herein contained or render the same invalid, inoperative or unenforceable to any extent whatever.

6.5 Waiver. Any failure of a party to enforce, for any period of time, any of the provisions under this Agreement shall not be construed as a waiver of such provisions or of the right of said party thereafter to enforce each and every provision under this Agreement.

6.6 Counterparts. This Agreement may be executed in several counterparts, each of which shall be an original and all of which shall constitute but one and the same instrument.

6.7 Modifications. This Agreement may not be effectively amended, changed, modified, altered or terminated without the prior written consent of the parties hereto.

6.8 Governing Law; Arbitration. This Agreement will be governed by and interpreted in accordance with the laws of the State of Delaware, without regard to conflict of law

principles that would result in the application of any law other than the law of the State of Delaware.

6.9 Attorney's Fees. If any action at law or in equity (including, arbitration) is necessary to enforce or interpret the terms of this Agreement, the prevailing party shall be entitled to reasonable attorney's fees, costs, and necessary disbursements in addition to any other relief to which such party may be entitled.

6.10 Successors and Assigns. This Agreement shall inure to the benefit of and shall be binding upon GovMVT, Supplier and any successor and assign thereto; subject, however, to the limitations contained herein.

*[Remainder of Page Intentionally Left Blank –
Signatures Follow]*

IN WITNESS WHEREOF, GovMVMT has caused this Agreement to be executed in its name and Supplier has caused this Agreement to be executed in its name, all as of the date first written above.

GovMVMT:

GovMVMT PURCHASING COOPERATIVE

By _____

Name: David Kidd

Title: Program Manager

Supplier:

Volatia Language Network, Inc.

(Insert Supplier Name)

By Jessica Kent

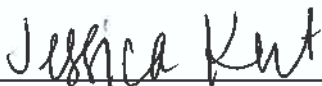
Name: Jessica Kent

Title: Proposals Manager

EXHIBIT E
LEAD PUBLIC AGENCY CERTIFICATE

In its capacity as a Lead Public Agency for GovMVMT Purchasing Cooperative, **Volatia Language Network, Inc.** has read and agrees to the general terms and conditions set forth in the Master Intergovernmental Cooperative Purchasing Agreement ("MICPA") regulating the use of the Master Agreements and purchase of Products and Services that from time to time are made available by Lead Public Agency to Participating Public Agencies nationwide through GovMVMT. Copies of Master Agreements and any amendments thereto made available by Lead Public Agency will be provided to Suppliers and GovMVMT to facilitate use by Participating Public Agencies.

I understand that the purchase of one or more Products and Services under the provisions of MICPA is at the sole and complete discretion of the Participating Public Agency.



Authorized Signature, Lead Public Agency

Jessica Kent

(Printed Name)

Proposals Manager

(Title)

October 31, 2023

(Date)

EXHIBIT F
FEDERAL FUNDS CONTRACT PROVISIONS

The following certifications and provisions may be required and apply with a Participating Public Agency spends federal funds for any purchase resulting from this procurement process. Pursuant to 2 CFR § 200.237, all contracts, including small purchases, awarded by the Participating Public Agency and the Participating Public Agency's Contractors and Subcontractors shall contain the procurement provisions of Appendix II to CFR Part 200, as applicable.

APPENDIX II TO 2 CFR 200

1. **Remedies.** Contracts for more than the federal simplified acquisition threshold (SAT), the dollar amount below which a Non-Federal Entity ("NFE") may purchase property or services using small purchase methods, currently set at \$250,000 for procurements made on or after June 20, 2018, must address administrative, contractual, or legal remedies in instances where contractors violate or breach contract terms, and must provide for sanctions and penalties as appropriate.

Pursuant to this Federal Rule, 1, Remedies, above, when a Participating Public Agency spends federal funds, the Participating Public Agency reserves all rights and privileges under the applicable laws and regulations with respect to this procurement in the event of breach of contract by either party.

JK _____ agrees
(Initial of Supplier's Authorized Representative)

2. **Termination for Cause and Convenience.** Contracts for cause and for convenience by the grantee or subgrantee, including the manner by which it will be carried out and the basis for settlement. This applies to contracts that are more than \$10,000.

Pursuant to this Federal Rule, 2, Termination for Cause and Convenience above, when a Participating Public Agency spends federal funds, the Participating Public Agency reserves the right to immediately terminate any agreement in excess of \$10,000 resulting from this procurement process in the event of a breach or default of the agreement by Supplier or for convenience as detailed in the terms of the contract.

JK _____ agrees
(Initial of Supplier's Authorized Representative)

3. **Equal Employment Opportunity.** Except as otherwise provided under 41 CFR Part 60, all contracts that meet the definition of "federally assisted construction contract" must include the equal opportunity clause found in 2 CFR Part 200.

Pursuant to this Federal Rule, 3, Equal Employment Opportunity above, when a Participating Public Agency spends federal funds on any federally assisted construction contract, the equal opportunity clause is incorporated by reference herein.

JK _____ agrees
(Initial of Supplier's Authorized Representative)

EXHIBIT F
FEDERAL FUNDS CONTRACT PROVISIONS

4. **Davis-Bacon Act.** When required by the federal program legislation, prime construction contracts over \$2,000 awarded by NFEs must include a provision for compliance with the Davis-Bacon Act. In accordance with the statute, contractors must pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in the Secretary of Labor's wage determination. Additionally, contractors are required to pay wages at least once per week. The NFE must place a copy of the Department of Labor's current prevailing wage determination in each solicitation. Contracts or subcontracts must be awarded on the condition that the prevailing wage determination is accepted. The NFE must report all suspected or reported violations to the federal awarding agency. The contracts must also include a provision for compliance with the Copeland "Anti-Kickback" Act for all contracts subject to the Davis-Bacon Act. According to 29 CFR § 5.5(a)(5), the regulatory requirements for the Copeland "Anti-Kickback" Act are incorporated by reference into the required contract provision, so a separate contract provision is not necessary. The NFE must and hereby includes the provisions at 29 CFR § 5.5(a)(1)-(10) in full into all applicable contracts and all applicable contractors must include their provisions in full in any subcontracts.

Pursuant to Federal Rule, 4, Davis-Bacon Act above, when a Participating Public Agency spends federal funds during the term of the award for all contracts and subcontracts for construction or repair, Supplier will be in compliance with all applicable Davis-Bacon Act provisions.

JK

_____ agrees
(Initial of Supplier's Authorized Representative)

5. **Copeland "Anti-Kickback" Act.** The Copeland "Anti-Kickback" Act prohibits workers on construction contracts from giving up wages that they are owed. This Act prohibits each contractor and subcontractor from any form of persuading a person employed in construction, completion, or repair of public work to give up any part of their rightful compensation. The NFE must report all suspected or reported violations of the Copeland "Anti-Kickback" Act the Federal awarding agency. The contractor shall comply with 18 U.S.C § 874, 40 U.S.C § 3145, and the requirements of 29 CFR Part 3 as may be applicable, which are incorporated by reference into this contract. The contractor or subcontractor shall insert in any subcontracts the clause above and such other clauses as the Federal funding agreement instructions require, and also a clause requiring the subcontractors to include these clauses in any lower tier subcontracts. The prime contractor shall be responsible for compliance by any subcontractor or lower tier subcontractor with all of these contract clauses. A breach of the contract clauses above may be grounds for termination of the contract, and for debarment as a contractor and subcontractor as provided in 29 CFR § 5.12.

Pursuant to Federal Rule, 5, Copeland "Anti-Kickback" Act, when a Participating Public Agency spends federal funds during the term of the award for all contracts and subcontracts for construction and repair, Supplier will be in compliance with all applicable Copeland "Anti-Kickback" Act provisions.

JK

_____ agrees
(Initial of Supplier's Authorized Representative)

EXHIBIT F
FEDERAL FUNDS CONTRACT PROVISIONS

6. **Contract Work Hours and Safety Standards Act.** Where applicable, all contracts awarded by the NFE of more than \$100,000 that involve the employment of mechanics or laborers must include a provision for compliance with statutory requirements on work hours and safety standards. Under 40 U.S.C. § 3702, each contractor must base wages for every mechanic and laborer on a standard 40-hour work week. Work over 40 hours is allowed, so long as the worker is paid at least one and a half times the base pay rate for all hours worked over 40 hours in the work week. Additionally, for construction work, under 40 U.S.C. § 3704, work surroundings and conditions for laborers and mechanics must not be unsanitary or unsafe. Relevant definitions are at 40 U.S.C. § 3701 and 29 CFR § 5.2. These requirements do not apply to the purchase of supplies or materials ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

Pursuant to Federal Rule, 6, Contract Work Hours and Safety Standards Act above, when a Participating Public Agency spends federal funds, Supplier certifies that Supplier will be in compliance with all applicable provisions of the Contract Work Hours and Safety Standards Act during the term of an award for all contracts by Participating Public Agency resulting from this procurement process.

JK agrees
(Initial of Supplier's Authorized Representative)

7. **Rights to Inventions Made Under a Contract or Agreement.** This contract provision outlines the rules governing the ownership of inventions created using federal funds. If the Federal award meets the definition of funding agreement and the NFE enters into any contract involving substitution of parties, assignment or performance of experimental, developmental or research work under that funding agreement, then the NFE must comply with the requirements of 37 CFR Part 401 and any implementing regulations issued by the Federal awarding agency. The regulation at 37 CFR § 401.2(a) defines funding agreement as "any contract, grant, or cooperative agreement entered into between any federal agency, other than the Tennessee Valley Authority, and any contractor for the performance of experimental, developmental, or research work funded in whole or in part by the federal government. This term also includes any assignment, substitution of parties, or subcontract of any type entered into for the performance of experimental, development, or research work under a funding agreement as defined in this paragraph.

Pursuant to Federal Rule, 7, Rights to Inventions Made Under a Contract or Agreement above, when federal funds are spent by a Participating Public Agency, the Supplier certifies that during the term of an award for all contracts by Participating Public Agency resulting from this procurement process, the Supplier agrees to comply with all applicable requirements as referenced in this Federal Rule.

JK agrees
(Initial of Supplier's Authorized Representative)

EXHIBIT F
FEDERAL FUNDS CONTRACT PROVISIONS

8. **Clean Air Act and Federal Water Pollution Control Act.** For contracts over \$150,000, contractors must agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S. C. § 7401 and the Federal Water Pollution Control Act, as amended, 33 U.S.C. § 1251. The contractor agrees to include these requirements in each subcontract exceeding \$150,000 financed in whole or in part with federal assistance provided by the Federal awarding agency. Violations must be reported to Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

Pursuant to Federal Rule, 8, Clean Air Act and Federal Water Pollution Control Act above, when federal funds are spent by Participating Public Agency, the Supplier certifies that during the term of an award for all contracts by Participating Public Agency resulting from this procurement process, the Supplier agrees to comply with all applicable requirements as referenced in this Federal Rule.

JK agrees
(Initial of Supplier's Authorized Representative)

9. **Debarment and Suspension.** For all contracts and subcontracts (see 2 CFR § 180.220), an award must not be made to parties listed on the governmentwide exclusions in the System for Award Management (SAM). SAM Exclusions is the list maintained by the General Services Administration that contains the names of parties that are debarred, suspended, or otherwise excluded, or declared ineligible under statutory or regulatory authority other than Executive Order 12549.

Pursuant to Federal Rule, 9, Debarment and Suspension above, when federal funds are spent by Participating Public Agency, the Supplier certifies that during the term of the award for all contracts by Participating Public Agency resulting from this procurement process, the Supplier certifies that none of its principals or its affiliates are debarred, suspended, or otherwise excluded, or ineligible from participation by any federal department or agency. If at any time during the term of the award the Supplier or its principals or affiliates become debarred, suspended, or otherwise excluded, or ineligible by any federal department or agency, the Supplier will notify the Participating Public Agency.

JK agrees
(Initial of Supplier's Authorized Representative)

10. **Byrd Anti-Lobbying Amendment.** Contractors that apply or bid for an award of more than \$100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used federal appropriated funds to pay any person or organization for influencing or attempting to influence an employee of a federal agency, a Member of Congress, an employee of Congress, or an employee of a Member of Congress in connection with receiving any federal contract, grant, or other award covered by 31 U.S.C. § 1352. Each tier must also disclose any lobbying with non-federal funds that takes place in connection with obtaining any federal award. Such disclosures are forwarded from tier to tier, up to the recipient who in turn will forward the certification(s) to the federal awarding agency.

EXHIBIT F
FEDERAL FUNDS CONTRACT PROVISIONS

Pursuant to Federal Rule, 10, Byrd Anti-Lobbying above, when federal funds are expended by Participating Public Agency, the Supplier certifies that during the term and after the awarded term of an award for all contracts by Participating Public Agency resulting from this procurement process, the Supplier certifies that it is in compliance with all applicable provisions of the Byrd Anti-Lobbying Amendment. The undersigned further certifies:

No federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.

If any funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (Including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) exceeding \$100,000 and that all subrecipients shall certify and disclose accordingly.

JK

_____ agrees
(Initial of Supplier's Authorized Representative)

- 11. Procurement of Recovered Materials.** Contractors must comply with Section 6002 of the Solid Waste Disposal Act when the purchase price is greater than \$10,000. In the performance of this contract, Contractor shall make maximum use of products containing recovered material that are EPA-designated items unless the product cannot be acquired (i) competitively within a timeframe providing for compliance with the contract performance schedule; (ii) meeting contract performance requirements; or (iii) at a reasonable price. Information about this requirement, along with the list of EPA-designated items, is available at EPA's Comprehensive Procurement Guidelines webpage: <https://www.epa.gov/smm/comprehensive-procurement-guideling-cpg-program>. The Contractor also agrees to comply with all other applicable requirements of Section 6002 of the Solid Waste Disposal Act.

Pursuant to Federal Rule, 11, Procurement of Recovered Materials above, when federal funds are spent by Participating Public Agency, the Supplier certifies that during the term of an award for all contracts by Participating Public Agency resulting from this procurement process, the Supplier certifies it will be in compliance with Section 6002 of the Solid Waste Disposal Act.

JK

_____ agrees
(Initial of Supplier's Authorized Representative)

EXHIBIT F
FEDERAL FUNDS CONTRACT PROVISIONS

12. **Domestic Preferences for Procurements.** As appropriate, and to the extent consistent with law, the Contractor should, to the greatest extent practicable, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States. This includes, but is not limited to iron, aluminum, steel, cement, and other manufactured products. For the purposes of this clause, produced in the United States means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States. Manufactured products mean items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

Pursuant to Federal Rule, 13, Domestic Preferences for Procurements above, when federal funds are spent by Participating Public Agency, the Supplier certifies that during the term of an award for all contracts by Participating Public Agency resulting from this procurement process, the Supplier certifies that it will comply with this Domestic Preference for Procurements.

JK _____ agrees
(Initial of Supplier's Authorized Representative)

Supplier agrees to comply with all federal, state, and local laws, rules, regulations and ordinances, as applicable. It is further acknowledged that Supplier certifies compliance with all provisions, laws, acts, regulations, etc. as specifically noted above.

Company Name: Volatia Language Network, Inc.

Address, City, State, Zip Code: 1327 Grandin Rd. SW
Roanoke, VA 24015

Phone: 540-562-8600

Fax: 540-204-7366

Printed Name of Authorized Signer: Jessica Kent

Email address of Authorized Signer: bids@volatia.com

Signature of Authorized Signer: Jessica Kent

Date: October 31, 2023

EXHIBIT G
FEMA (FEDERAL EMERGENCY MANAGEMENT AGENCY)
RECOMMENDED CONTRACT PROVISIONS

Awarded Suppliers may need to respond to work that is being funded in whole or in part with emergency assistance provided by FEMA. Emergency assistance may be due to situations including, but not limited to, water damage, fire damage, biohazard cleanup, sewage decontamination, vandalism cleanup, deodorization, and/or wind damage during a disaster or an emergency.

If any purchase made under the Master Agreement is funded in whole or in part by Federal Emergency Management Agency ("FEMA") grants, Supplier agrees to execute work in compliance with all federal laws and regulations applicable to the receipt of FEMA grants, including, but not limited to all FEMA requirements as set forth below when products and services are issued in response to an emergency or for disaster recovery. Supplier also agrees to the requirements in the Federal Funds Contract Provisions above.

Definitions

Federal Emergency Management Agency (FEMA): FEMA's statutory mission is to reduce the loss of life and property and protect the Nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters, by leading and supporting the Nation in a risk-based, comprehensive emergency management system of preparedness, protection, response, recovery, and mitigation. Among other things;

- FEMA administers its programs and carries out its activities through its headquarters offices in Washington, D.C.; ten Regional Offices, Area Offices for the Pacific, Caribbean, and Alaska; various Recovery Offices; and temporary Joint Field Offices (JFO).
- FEMA administers numerous assistance programs annually for on a regular basis to increase the Nation's preparedness, readiness and resilience to all hazards. These assistance programs are typically available to NFEs including, but not limited to, states, local governments, Indian Tribes, universities, hospitals, and certain private nonprofit organizations.
- Each program is governed by the applicable federal law, regulations, executive orders and FEMA program-specific policies. As the Federal awarding agency for these programs, FEMA is responsible for the proper management and administration of these programs as otherwise required by law and enforcing the terms of the agreements it enters with NFEs that receive FEMA financial assistance, consistent with the requirements at 2 CFR Part 200.

2 CFR § 200.237 and 2 CFR Part 200, Appendix II, Required Contract Clauses

1. Remedies

In the event a Participating Public Agency uses FEMA funds for more than the federal simplified acquisition threshold (SAT), currently set at \$250,000 for procurements made on or after June 20, 2018, Participating Public Agency will address the administrative, contractual, and legal remedies with contractors in instances where contractors violate or breach contract terms, and must provide sanctions and penalties as appropriate.

EXHIBIT G
FEMA (FEDERAL EMERGENCY MANAGEMENT AGENCY)
RECOMMENDED CONTRACT PROVISIONS

For FEMA's Assistance to Firefighters Grant (AFG) program, the Contract shall include a clause addressing that non-delivery by the Contract's specified date or other vendor nonperformance will require a penalty of no less than \$100 per day until such time that the vehicle, compliant with the terms of the Contract, has been accepted by the recipient. This penalty clause does not apply for force majeure or acts of God.

2. Termination for Cause and Convenience

When FEMA funds are used, Participating Public Agency reserves the right to terminate any agreement in excess of \$10,000 resulting from this procurement process in the event of a breach or default of the agreement by Contractor or for convenience.

The right to terminate this Contract for convenience of the Participating Public Agency is retained by the Participating Public Agency. In the event of a termination for convenience by the Participating Public Agency, the Participating Public Agency shall, at least ten (10) calendar days in advance, deliver written notice of the termination for convenience to the Contractor. Upon Contractor's receipt of such written notice, Contractor immediately shall cease the performance of the Work and shall take reasonable and appropriate action to secure and protect the Work then in place. Contractor shall then be paid by the Participating Public Agency, in accordance with the terms and provisions of the Contract Documents, an amount not to exceed the actual labor costs incurred, the actual cost of all materials installed and the actual cost of all materials stored at the project site or away from the project site, as approved in writing by the Participating Public Agency but not yet paid for and which cannot be returned, and actual, reasonable and documented demobilization costs, if any, paid by Contractor and approved by the Participating Public Agency in connection with the Scope of Services in place which is completed as of the date of termination by the Participating Public Agency and that is in conformance with the Contract Documents, less all amounts previously paid for the Work. No amount ever shall be owed or paid to Contractor for lost or anticipated profits on any part of the Scope of Services not performed or for consequential damages of any kind.

3. Equal Employment Opportunity

Contracts that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 must include the equal opportunity clause provided under 41 CFR 60-1.4(b).

The Participating Public Agency highly encourages Contractors to implement Affirmative Action practices in their employment programs. This means Contractor should not discriminate against any employee or applicant for employment because of race, color, religion, sex, pregnancy, sexual orientation, political belief or affiliation, age, disability or genetic information.

During the performance of this Contract, the Contractor agrees as follows:

- (1) The Contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. The Contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment without regard to their race, color religion, sex,

EXHIBIT G
FEMA (FEDERAL EMERGENCY MANAGEMENT AGENCY)
RECOMMENDED CONTRACT PROVISIONS

sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following:

Employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided setting forth the provisions of this nondiscrimination clause.

- (2) The Contractor will, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.
- (3) The Contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the contractor's legal duty to furnish information.
- (4) The Contractor will send to each labor union or representative of workers with which he has a collective bargaining agreement or other Contract or understanding, a notice to be provided advising the said labor union or workers' representatives of the Contractor's commitments under this section, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.
- (5) The Contractor will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.
- (6) The Contractor will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to its books, records, and accounts by the administering agency and the Secretary of Labor for purposes of investigation in ascertain compliance with such rules, regulations, and orders.
- (7) In the event of the Contractor's noncompliance with the nondiscrimination clauses of this contract or with any of the said rules, regulations, or orders, this contract may be canceled, terminated, or suspended in whole or in part and the Contractor may be declared ineligible

EXHIBIT G
FEMA (FEDERAL EMERGENCY MANAGEMENT AGENCY)
RECOMMENDED CONTRACT PROVISIONS

for further Government contracts or federally assisted construction contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in Executive Order 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.

- (8) The Contractor will include the portion of the sentence immediately preceding paragraph (1) and the provisions of paragraphs (1) through (8) in every subcontract or purchase order unless exempted by rules, regulations, orders of the Secretary of Labor issued pursuant to section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The Contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions, including sanctions for noncompliance:

Provided, however, that in the event a Contractor becomes involved in, or is threatened with litigation with a subcontractor or vendor as a result of such direction by the administering agency, the Contractor may request the United States to enter into such litigation to protect the interests of the United States.

The applicant further agrees that it will be bound by the above equal opportunity clause with respect to its own employment practice when it participates in federal assisted construction work: *Provided*, that if the applicant so participating is a state or local government, the above equal opportunity clause is not applicable to any agency, instrumentality or subdivision of such government which does not participate in work on or under the Contract.

The applicant agrees that it will assist and cooperate actively with the administering agency and the Secretary of Labor in obtaining the compliance of Contractors and Subcontractors with the equal opportunity clause and the rules, regulations, and relevant orders of the Secretary of Labor, that it will furnish the administering agency and the Secretary of Labor such information as they may require for the supervision of such compliance, and that it will otherwise assist the administering agency in the discharge of the agency's primary responsibility for securing compliance.

The applicant further agrees that it will refrain from entering into any contract or contract modification subject to Executive Order 11246 of September 24, 1965, with a Contractor debarred from, or who has not demonstrated eligibility for, Government contracts and federally assisted construction contracts pursuant to the Executive Order and will carry out such sanctions and penalties for violation of the equal opportunity clause as may be imposed upon Contractors and Subcontractors by the administering agency or the Secretary of Labor pursuant to Part II, Subpart D of the Executive Order. In addition, the applicant agrees that if it fails or refuses to comply with these undertakings, the administering agency may take any or all of the following actions: Cancel, terminate, or suspend in whole or in part this grant (contract, loan, insurance, guarantee); refrain from extending any further

EXHIBIT G
FEMA (FEDERAL EMERGENCY MANAGEMENT AGENCY)
RECOMMENDED CONTRACT PROVISIONS

assistance to the applicant under the program with respect to which the failure or refund occurred until satisfactory assurance of future compliance has been received from such applicant; and refer the case to the Department of Justice for appropriate legal proceedings.

4. Davis-Bacon Act

The Davis-Bacon Act applies to prime construction contracts over \$2,000 and only applies to the Emergency Management Performance Grant Program, Homeland Security Grant Program, Nonprofit Grant Program, Tribal Homeland Security Grant Program, Port Security Grant Program, Transit Security Grant Program, Intercity Passenger Rail Program, and Rehabilitation of High Hazard Potential Dams Program. **It does not apply to other FEMA grant and cooperative agreement programs, including the PA (Public Assistance) Program.**

All prime construction contracts over \$2,000 awarded by NFEs must include a provision for compliance with the Davis-Bacon Act (40 U.S.C. §§ 3141-3144 and 3146-3148). The Davis-Bacon Act is supplemented by Department of Labor regulations at 29 CFR Part 5 (Labor Standards Provisions Applicable to Contracts Covering federally Financed and Assisted Construction). See 2 CFR Part 200, Appendix II, § D.

Contractors are required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in the Secretary of Labor's wage determination. Additionally, Contractors are required to pay wages at least once per week.

The NFE must place a copy of the Department of Labor's current prevailing wage determination in each solicitation. The decision to award must be conditioned on the acceptance of the wage determination. The NFE must report all suspected or reported violations to the federal awarding agency.

For any Contract subject to the Davis-Bacon Act, that Contract must also comply with the Copeland "Anti-Kickback" Act. See Section 5 below for additional information.

If applicable per the standard described above, the Participating Public Agency hereby incorporates the provisions at 29 CFR § 5.5(a)(1)-(5) into the Contract and all applicable Contractors must include these provisions in any Subcontracts.

5. Copeland "Anti-Kickback" Act

The Copeland "Anti-Kickback" Act prohibits workers on construction contracts from giving up wages that they are owed.

Applicability: For all prime construction contracts above \$2,000, when the Davis-Bacon Act applies, the Copeland "Anti-Kickback" Act also applies. In situations where the Davis-Bacon Act does not apply, neither does the Copeland "Anti-Kickback" Act. As with the Davis-Bacon Act, this provision only applies to certain FEMA grant and cooperative agreement programs as noted above in section 4. This Act does not apply to the Public Assistance (PA) Program.

EXHIBIT G
FEMA (FEDERAL EMERGENCY MANAGEMENT AGENCY)
RECOMMENDED CONTRACT PROVISIONS

Contractor. The Contractor shall comply with 18 U.S.C. § 874, 40 U.S.C. § 3145, and the requirements of 29 CFR Part 3 as may be applicable, which are incorporated by reference into this Contract.

Subcontracts. The Contractor or Subcontractor shall insert in any Subcontracts the clause above and such other clauses as FEMA may by appropriate instructions require, and also a clause requiring the Subcontractors to include these clauses in any lower tier Subcontracts. The Prime Contractor shall be responsible for the compliance by any Subcontractor or lower tier Subcontractor with all of these Contract clauses.

Breach. A breach of the Contract clauses above may be grounds for termination of the Contract, and for debarment as a Contractor and Subcontractor as provided in 29 CFR § 5.12.

6. Contract Work Hours and Safety Standards Act

Applicability: This required Contract provision applies to all procurements over \$100,000 that involve the employment of mechanics, laborers, and construction work. These requirements do not apply to the purchase of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

(1) *Overtime requirements.* No Contractor or Subcontractor contracting for any part of the contract work which may require or involve the employment of laborers or mechanics shall require or permit any such laborer or mechanic in any workweek in which he or she is employed on such work to work in excess of forty hours in such workweek unless laborer or mechanic receives compensation at a rate not less than one and one-half times the basic rate of pay for all hours worked in excess of forty hours in such workweek.

(2) *Violation; liability for unpaid wages; liquidated damages.* In the event of any violation of the clause set forth in paragraph (b)(1) of 29 CFR § 5.5(b)(1)-(4) the Contractor and any Subcontractor responsible therefor shall be liable for the unpaid wages. In addition, such Contractor and Subcontractor shall be liable to the United States (in the case of work done under Contract for the District of Columbia or a territory, to such District or to such territory), for liquidated damages. Such liquidated damages shall be computed with respect to each individual laborer or mechanic, including watchmen and guards, employed in violation of the clause set forth in paragraph (b)(1), in the sum of \$27 for each calendar day on which such individual was required or permitted to work in excess of the standard workweek of forty hours without payment of the overtime wages required by the clause set forth in paragraph (b)(1).

(3) *Withholding for unpaid wages and liquidated damages.* The Participating Public Agency shall upon its own action or upon written request of an authorized representative of the Department of Labor withhold or cause to be withheld, from any moneys payable on account of work performed by the Contractor or Subcontractor under any such Contract or any other federal Contract with the same Prime Contractor, or any other federally-assisted

EXHIBIT G
FEMA (FEDERAL EMERGENCY MANAGEMENT AGENCY)
RECOMMENDED CONTRACT PROVISIONS

Contract subject to the Contract Work Hours and Safety Standards Act, which is held by the same Prime Contractor, such sums as may be determined to be necessary to satisfy any liabilities of such Contractor or Subcontractor for unpaid wages and liquidated damages as provided in the clause set forth in paragraph (b)(2).

- (4) *Subcontracts.* The Contractor or Subcontractor shall insert in any Subcontracts the clauses set forth in paragraph (b)(1) through (4) of this section and also a clause requiring the subcontractors to include these clauses in any lower tier Subcontracts. The Prime Contractor shall be responsible for compliance by any Subcontractor or lower tier Subcontractor with the clauses set forth in paragraphs (b)(1) through (4).

Where contracts that are only subject to Contract Work Hours and Safety Standards Act and are not subject to the other statutes in 29 CFR § 5.1, the below additional compliance is required:

- (1) The Contractor or Subcontractor shall maintain payrolls and basic payroll records during the course of the work and shall preserve them for a period of three years from the completion of the Contract for all laborers and mechanics, including guards and watchmen, working on the Contract. Such records shall contain the name and address of each such employee, social security number, correct classifications, hourly rates of wages paid, daily and weekly number of hours worked, deductions made, and actual wages paid.
- (2) Records to be maintained under this provision shall be made available by the Contractor or Subcontractor for inspection, copying, or transcription by authorized representatives of the Department of Homeland Security, the Federal Emergency Management Agency, and the Department of Labor, and the Contractor or Subcontractor will permit such representatives to interview employees during working hours on the job.

7. Rights to Inventions Made Under a Contract or Agreement

This contract provision outlines the rules governing the ownership of inventions created using federal funds. If the FEMA award meets the definition of funding agreement and the NFE enters into any contract involving substitution of parties, assignment or performance of experimental, developmental, or research work under that funding agreement, then the 37 CFR Part 401 applies.

This clause is not required for procurements under FEMA's Public Assistance (PA) Program and does not apply to all FEMA grant and cooperative agreement programs. The NFE will need to check with their applicable FEMA grant representative to determine if this provision is required for the procurement.

Funding Agreements: The regulation at 37 CFR § 401.2 defines funding agreement as "any contract, grant, or cooperative agreement entered into between any federal agency, other than the Tennessee Valley Authority, and any Contractor for the performance of experimental, developmental, or research work funded in whole or in part by the federal government. This

EXHIBIT G
FEMA (FEDERAL EMERGENCY MANAGEMENT AGENCY)
RECOMMENDED CONTRACT PROVISIONS

term also includes any assignment, substitution of parties, or subcontract of any type entered into for the performance of experimental, developmental, or research work under a funding agreement as defined in the first sentence of this paragraph.”

8. Clean Air Act and Federal Water Pollution Control Act

This contract provision applies for all procurements over \$150,000.

“Clean Air Act”

The Contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. § 7401 et seq.

The Contractor agrees to report each violation to the Participating Public Agency and understands and agrees that the Participating Public Agency will, in turn report each violation as required to assure notification to the Federal Emergency Management Agency (FEMA), and the appropriate Environmental Protection Agency Regional Office.

The Contractor agrees to include these requirements in each Subcontract exceeding \$150,000 financed in whole or in part with federal assistance provided by FEMA.

“Federal Water Pollution Control Act”

The Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the federal Water Pollution Control Act, as amended, 33 U.S.C. § 1251 et seq.

The Contractor agrees to report each violation to the Participating Public Agency and understands and agrees that the Participating Public Agency will, in turn, report each violation as required to assure notification to the Participating Public Agency, Federal Emergency Management Association (FEMA), and the appropriate Environmental Protection Agency Regional Office.

The Contractor agrees to include these requirements in each Subcontract exceeding \$150,000 financed in whole or in part with federal assistance provided by FEMA.

9. Debarment and Suspension

Applicability: This clause applies to all FEMA grant and cooperative agreement programs.

This Contract is a covered transaction for purposes of 2 CFR Part 180 and 2 CFR Part 3000. As such, the Contractor is required to verify that none of the Contractor’s principals (defined at 2 CFR § 180.995) or its affiliates (defined at 2 CFR § 180.905) are excluded (defined at 2 CFR § 180.940) or disqualified (defined at 2 CFR § 180.935).

The Contractor must comply with 2 CFR Part 180, subpart C and 2 CFR Part 3000, subpart C, and must include a requirement to comply with these regulations in any lower tier covered transaction it enters into.

EXHIBIT G
FEMA (FEDERAL EMERGENCY MANAGEMENT AGENCY)
RECOMMENDED CONTRACT PROVISIONS

This certification is a material representation of fact relied upon by Participating Public Agency. If it is later determined that the Contractor did not comply with 2 CFR Part 180, subpart C and 2 CFR Part 3000, subpart C, in addition to remedies available to Participating

Public Agency, the federal government may pursue available remedies, including but not limited to suspension and/or debarment.

The bidder or proposer agrees to comply with the requirements of 2 CFR Part 180, subpart C and 2 CFR Part 3000, subpart C while this offer is valid and throughout the period of any contract that may arise from this offer. The bidder or proposer further agrees to include a provision requiring compliance in its lower tier covered transactions.

10. Byrd Anti-Lobbying Amendment

Applicability: The Byrd Anti-Lobbying Amendment clause and certification are required for contracts of more than \$100,000, and for subcontracts of more than \$100,000.

Byrd Anti-Lobbying Amendment, 31 U.S.C. § 1352 (as amended)

Contractors who apply or bid for an award of more than \$100,000 shall file the required certification. Each tier certifies to the tier above that it will not and has not used federally appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, officer or employee of Congress, or an employee of a Member of Congress in connection with obtaining any federal contract, grant, or any other award covered by 31 U.S.C. § 1352. Each tier shall also disclose any lobbying with non-federal funds that takes place in connection with obtaining any federal award. Such disclosures are forwarded from tier to tier up to the recipient who in turn will forward the certification(s) to the federal awarding agency.

APPENDIX A, 44 CFR PART 18 – CERTIFICATION REGARDING LOBBYING

Certification for Contracts, Grants, Loans, and Cooperative Agreements

The undersigned certifies, to the best of her or her knowledge and belief, that:

No federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any federal grant, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.

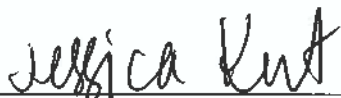
EXHIBIT G
FEMA (FEDERAL EMERGENCY MANAGEMENT AGENCY)
RECOMMENDED CONTRACT PROVISIONS

If any funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representative of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, Title 31, U.S.C. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

The Contractor, Volatia Language Network, Inc., certifies or affirms the truthfulness and accuracy of each statement of its certification and disclosure, if any. In addition, the Contractor understands and agrees that the provisions of 31 U.S.C Chap. 38, Administrative Remedies for False Claims and Statements, apply to this certification and disclosure, if any.



Signature of Contractor's Authorized Official

Jessica Kent, Proposals Manager

Name and Title of Contractor's Authorized Official

October 31, 2023

Date

11. Procurement of Recovered Materials

Applicability: This provision applies to all procurements over \$10,000 made by a state agency or an agency of a political subdivision of a state and its contractors.

In the performance of this Contract, the Contractor shall make maximum use of products containing recovered materials that are EPA-designated items unless the product cannot be acquired:

- a. Competitively within a timeframe providing for compliance with the contract performance schedule;

EXHIBIT G
FEMA (FEDERAL EMERGENCY MANAGEMENT AGENCY)
RECOMMENDED CONTRACT PROVISIONS

- b. Meeting contract performance requirements; or
- c. At a reasonable price.

Information about this requirement, along with the list of EPA-designated items, is available at EPA's Comprehensive Procurement Guidelines webpage: <https://www.epa.gov/smm/comprehensive-procurement-guideline-cpg-program>.

The Contractor also agrees to comply with all other applicable requirements of Section 6002 of the Solid Waste Disposal Act.

12. Prohibition on Contracting for Covered Telecommunications Equipment or Services

Applicability: This provision is required for all awards/purchases issued on or after November 12, 2020.

(a) *Definitions.* As used in this clause, the terms backhaul; covered foreign country; covered telecommunications equipment or services; interconnection arrangements; roaming; substantial or essential component; and telecommunications equipment or services have the meaning as defined in FEMA Policy 405-143-1, Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services (Interim), as used in this clause.

(b) *Prohibitions.*

(1) Section 889(b) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, and 2 CFR § 200.216 prohibit the head of an executive agency on or after Aug. 13, 2020, from obligating or expending grant, cooperative agreement, loan, or loan guarantee funds on certain telecommunications products or from certain entities for national security reasons.

(2) Unless an exception in paragraph (c) of this clause applies, the Contractor and its Subcontractors may not use grant, cooperative agreement, loan, or loan guarantee funds from the Federal Emergency Management Agency to:

- (i) Procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system;
- (ii) Enter into, extend, or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system;
- (iii) Enter into, extend, or renew contracts with entities that use covered telecommunications equipment or services as a substantial or essential

EXHIBIT G
FEMA (FEDERAL EMERGENCY MANAGEMENT AGENCY)
RECOMMENDED CONTRACT PROVISIONS

component of any system, or as critical technology as part of any system;
or

- (iv) Provide, as part of its performance of this contract, subcontract, or other contractual instrument, any equipment, system, or service that used covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

(c) Exceptions.

(1) This clause does not prohibit contractors from providing:

- (i) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or
- (ii) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(2) By necessary implication and regulation, the prohibitions also do not apply to:

- (i) Covered telecommunications equipment or services that:
 - i. Are not used as a substantial or essential component of any system;
and
 - ii. Are not used as critical technology of any system.
- (ii) Other telecommunications equipment or services that are not considered covered telecommunications equipment or services.

(d) Reporting Requirements.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a Subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the recipient or subrecipient, unless elsewhere in this contract are established procedures for reporting the information.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause:

- (i) Within one business day from the date of such identification or notification:
The Contract number, the order number(s), if applicable; supplier name,

EXHIBIT G
FEMA (FEDERAL EMERGENCY MANAGEMENT AGENCY)
RECOMMENDED CONTRACT PROVISIONS

supplier unique entity identifier (if known); supplier commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

- (ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: Any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered
- (iii) telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments.

13. Domestic Preferences for Procurements

Applicability: Applies for purchases in support of FEMA declarations and awards issued on or after November 12, 2020.

As appropriate, and to the extent consistent with the law, the Contractor, should to the greatest extent practicable, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States. This includes, but is not limited to iron, aluminum, steel, cement, and other manufactured products.

For the purposes of this clause:

Produced in the United States means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States.

Manufactured products mean items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

14. Access to Records

The Contractor agrees to provide Participating Public Agency, the FEMA Administrator, the Comptroller General of the United States, or any of their authorized representatives access to any books, documents, papers, and records of the Contractor which are directly pertinent to this contract for the purposes of making audits, examinations, excerpts, and transcriptions.

EXHIBIT G
FEMA (FEDERAL EMERGENCY MANAGEMENT AGENCY)
RECOMMENDED CONTRACT PROVISIONS

The Contractor agrees to permit any of the foregoing parties to reproduce by any means whatsoever or to copy excerpts and transcriptions as reasonably needed.

The Contractor agrees to provide the FEMA Administrator or its authorized representatives access to construction or other work sites pertaining to the work being completed under the Contract.

In compliance with section 1225 of the Disaster Recovery Reform Act of 2018, the Participating Public Agency and the Contractor acknowledge and agree that no language in this Contract is intended to prohibit audits or internal reviews by the FEMA Administrator or the Comptroller General of the United States.

15. Changes

To be allowable under a FEMA grant or cooperative agreement award, the cost of any contract change, modification, amendment, addendum, change order, or constructive change must be necessary, allocable, within the scope of the grant or cooperative agreement, reasonable for the scope of work, and otherwise allowable. See 2 CFR § 200.403.

FEMA recommends that all contracts include a changes clause that describes how, if at all, changes can be made by either party to alter the method, price, or schedule of the work without breaching the Contract. The language of the clause may depend on the nature of the contract and the procured item(s) or service(s). Participating Public Agency should also consult with counsel to determine whether and how contract changes are permissible under applicable state, local, or tribal laws or regulations.

16. DHS Seal, Logo, and Flags

The Contractor shall not use the DHS seal(s), logos, crests, or reproductions of flags or likenesses of DHS agency officials without specific FEMA pre-approval. The Contractor shall include this provision in any Subcontracts.

17. Compliance with Federal Law, Regulations, and Executive Orders and Acknowledgement of Federal Funding

This is an acknowledgement that FEMA financial assistance will be used to fund all or a portion of the Contract. The Contractor will comply with all applicable federal law, regulations, executive orders, FEMA policies, procedures, and directives.

18. No Obligation by Federal Government

The federal government is not a party to this Contract and is not subject to any obligations or liabilities to the NFE, Contractor, or any other party pertaining to any matter resulting from the Contract. See 2 CFR § 200.318(k).

19. Program Fraud and False or Fraudulent Statements or Related Acts

EXHIBIT G
FEMA (FEDERAL EMERGENCY MANAGEMENT AGENCY)
RECOMMENDED CONTRACT PROVISIONS

The Contractor acknowledges that 31 U.S.C Chap. 38 (Administrative Remedies for False Claims and Statements) applies to the Contractor's actions pertaining to this Contract.

20. Affirmative Socioeconomic Steps

Applicability: For procurements under FEMA declarations and awards issued on or after November 12, 2020.

If Subcontracts are to be let, the Prime Contractor is required to take all necessary steps identified in 2 CFR § 200.321(b)(1)-(5) to ensure that small and minority businesses, women's business enterprises, and labor surplus area firms are used when possible. The necessary steps are as follows:

- 1) Placing qualified small and minority businesses and women's business enterprises on solicitation lists;
- (2) Assuring that small and minority businesses, and women's business enterprises are solicited whenever they are potential sources;
- (3) Dividing total requirements, when economically feasible, into smaller tasks or quantities to permit maximum participation by small and minority businesses, and women's business enterprises;
- (4) Establishing delivery schedules, where the requirement permits, which encourage participation by small and minority businesses, and women's business enterprises; and
- (5) Using the services and assistance, as appropriate, of such organizations as the Small Business Administration and the Minority Business Development Agency of the Department of Commerce.

21. Copyright and Data Rights

Applicability: When a Participating Public Agency enters into a Contract requiring a Contractor or Subcontractor to produce copyrightable subject matter and/or data for the Participating Public Agency under the award, the Participating Public Agency should include appropriate copyright and data licenses to meet its obligations under 2 CFR § 200.315(b) and (d), respectively.

The Contractor grants to the Participating Public Agency, a paid-up, royalty-free, nonexclusive, irrevocable, worldwide license in data first produced in the performance of this contract to reproduce, publish, or otherwise use, including prepare derivative works, distribute copies to the public, and perform publicly and display publicly such data. For data required by the Contract but not first produced in the performance of this Contract, the Contractor will identify such data and grant to the Participating Public Agency or acquires on its behalf a license of the same scope as for data first produced in the performance of this Contract. Data, as used herein, shall include any work subject to copyright under 17 U.S.C. § 102, for example, any written reports or literary works, software and/or source code, music, choreography, pictures or images, graphics, sculptures, videos, motion pictures or other audiovisual works,

EXHIBIT G
FEMA (FEDERAL EMERGENCY MANAGEMENT AGENCY)
RECOMMENDED CONTRACT PROVISIONS

sound and/or video recordings, and architectural works. Upon or before the completion of this Contract, the Contractor will deliver to the Participating Public Agency data first produced in the performance of this Contract and data required by the Contract but not first produced in the performance of this Contract in formats acceptable by the Participating Public Agency.

Supplier agrees to comply will all terms and conditions outlined in the FEMA Special Conditions section of this solicitation.

Company Name: Volatia Language Network, Inc.

Address, City, State, Zip Code: 1327 Grandin Rd. SW
Roanoke, VA 24015

Phone: 540-562-8600

Fax: 540-204-7366

Printed Name of Authorized Signer: Jessica Kent

Email address of Authorized Signer: bids@volatia.com

Signature of Authorized Signer: Jessica Kent

Date: October 31, 2023

**EXHIBIT H
ATTACHMENT 1**

**OWNERSHIP DISCLOSURE FORM
(N.J.S.A. 52:25-24.2)**

Pursuant to the requirements of P.L. 1999, c.440, the Supplier shall complete the form attached to these specifications listing the persons owning 10 percent (10%) or more of the firm presenting the proposal.

Company Name: Volatia Language Network, Inc.

Address: 1327 Grandin Rd. SW, Roanoke VA 24015

1. The Company is a **Sole Proprietor**; and therefore, no disclosure is necessary. Yes No
A sole proprietor is a person who owns an unincorporated business by him/herself.
A limited liability company with a single member is not a Sole Proprietor.
2. The Company is a **Corporation, Partnership, or Limited Liability Company**. Yes No

If you answered YES to Question 2, you must disclose the following: (a) the names and addresses of all stockholders in the corporation who own 10% or more of its stock, of any class; (b) all individual partners in the partnership who own a 10% or greater interest therein; or, (c) all members in the limited liability company who own a 10% or greater interest therein. (Attach additional sheets as necessary.)

If there are no stockholders, partners or members owning 10% or more interest, indicate "none".

Name	Address	Interest
None		

3. For each of the corporations, partnerships, or limited liability companies identified above, are there any individuals, partners, members, stockholders, corporations, partnerships, or limited liability companies owning a 10% or greater interest of those listed business entities? Yes No

If there are no stockholders, partners or members owning 10% or more interest, indicate "none".

**EXHIBIT H
ATTACHMENT 1**

Name	Address	Interest
Baraka Kasongo, 4477 Lewiston NW, Roanoke, VA 24017, 100		

I further certify that the statements and information contained herein, are complete and correct to the best of my knowledge and belief.

**EXHIBIT H
ATTACHMENT 2**

**NON-COLLUSION AFFIDAVIT
N.J.S.A. 52:34-15**

State of North Carolina
~~New Jersey~~
County of Craven

ss:

I, Jessica Kent residing in New Bern in
(name of municipality) (name of affiant)
in the County of Craven and State of North Carolina
North Carolina of full age, being duly sworn according to law on my oath depose
and say that:

I am Proposals Manager of the firm of
(title or position) (name of firm)


Volatia Language Network, Inc. the bidder making this Proposal for the bid
Translation Services, Interpretation Management Systems and Related Products
entitled _____, and that I executed the said proposal with
(title of bid proposal)

full authority to do so that said bidder has not, directly or indirectly entered into any agreement,
participated in any collusion, or otherwise taken any action in restraint of free, competitive
bidding in connection with the above-named project; and that all statements contained in said
proposal and in this affidavit are true and correct, and made with full knowledge that the
State of New Jersey relies upon the truth of the statements
contained in said Proposal
(name of contracting unit)
and in the statements contained in this affidavit in awarding the contract for the said project.

I further warrant that no person or selling agency has been employed or retained to solicit or
secure such contract upon an agreement or understanding for a commission, percentage,
brokerage, or contingent fee, except bona fide employees or bona fide established
commercial or selling agencies maintained by
Volatia Language Network, Inc.
(name of firm)

Subscribed and sworn to
before me this day
Jessica Kent
Signature

31st of October, 2023 Jessica Kent
(Type or print name of affiant under signature)

Tatianne G. Teixeira
Notary public
My Commission expires 09/17/2028
(Seal)


**EXHIBIT H
ATTACHMENT 3****AFFIRMATIVE ACTION AFFIDAVIT
P.L. 1975, c.127**Company Name: Volatia Language Network, Inc.Address: 1327 Grandin Rd. SW, Roanoke, VA 24015

Proposal Certification: Indicate below your company's compliance with New Jersey Affirmative Action regulations. Company's proposal will be accepted even if not in compliance at this time. No contract and/or purchase order may be issued, however, until all Affirmative Action requirements are met.

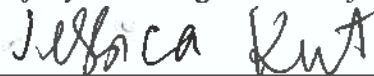
Required Affirmative Action Documentation:The Supplier shall submit with its proposal, **ONE** of the following three documents:

- (1) Letter of Federal Affirmative Action Plan Approval
- (2) Certificate of Employee Information Report
- (3) Employee Information Report Form AA302

Public Work – Project Cost over \$50,000:

- (1) If company has no approved Federal or New Jersey Affirmative Action Plan. Company will complete New Jersey Form AA-201 upon award; or
- (2) Company has a Federal or New Jersey Affirmative Action Plan – certificate is enclosed.

I further certify the statements and information contained herein, are complete and correct to the best of my knowledge and belief.



*Authorized Signature***Jessica Kent**

*Printed Name***Proposals Manager**

*Title***October 31, 2023**

Date

EXHIBIT H
ATTACHMENT 3

recruitment agencies including, but not limited to, employment agencies, placement bureaus, colleges, universities, labor unions, that it does not discriminate on the basis of age, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, and that it will discontinue the use of any recruitment agency which engages in direct or indirect discriminatory practices.

The contractor or subcontractor agrees to revise any of its testing procedures, if necessary, to assure that all personnel testing conforms with the principles of job-related testing, as established by the statutes and court decisions of the State of New Jersey and as established by applicable Federal law and applicable Federal court decisions.

In conforming with the applicable employment goals, the contractor or subcontractor agrees to review all procedures relating to transfer, upgrading, downgrading and layoff to ensure that all such actions are taken without regard to age, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, consistent with the statutes and court decisions of the State of New Jersey, and applicable Federal law and applicable Federal court decisions.

The contractor and its subcontractors shall furnish such reports or other documents to the Div. of Contract Compliance & EEO as may be requested by the office from time to time in order to carry out the purposes of these regulations, and public agencies shall furnish such information as may be requested by the Div. of Contract Compliance & EEO for conducting a compliance investigation pursuant to **Subchapter 10 of the Administrative Code at N.J.A.C. 17:27.**

Signature of Procurement Agent

**EXHIBIT H
ATTACHMENT 4**

**C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM
Required Pursuant to N.J.S.A. 19:44A-20.26**

This form or its permitted facsimile must be submitted to the local unit no later than 10 days prior to the award of the contract.

Part I - Vendor Information

Vendor Name:	Volatia Language Network, Inc.		
Address:	1327 Grandin Rd. SW		
City:	Roanoke	State:	V/
		Zip:	2401!

The undersigned being authorized to certify, hereby certifies that the submission provided herein represents compliance with the provisions of N.J.S.A. 19:44A-20.26 and as represented by the Instructions accompanying this form.

Signature Jessica Kent Printed Name Jessica Kent Title Proposals Manager

Part II - Contribution Disclosure

Disclosure requirement: Pursuant to N.J.S.A. 19:44A-20.26 this disclosure must include all reportable political contributions (more than \$300 per election cycle) over the 12 months prior to submission to the committees of the government entities listed on the form provided by the local unit.

Check here if disclosure is provided in electronic form.

Contributor Name	Recipient Name	Date	Dollar Amount
None			\$

Check here if the information is continued on subsequent page(s)

**EXHIBIT H
ATTACHMENT 5**

STOCKHOLDER DISCLOSURE CERTIFICATION

Name of Business: Volatia Language Network, Inc.

I certify that the list below contains the names and home addresses of all stockholders holding 10% or more of the issued and outstanding stock of the undersigned.

OR

I certify that no one stockholder owns 10% or more of the issued and outstanding stock of the undersigned.

Check the box that represents the type of business organization:

Partnership
Proprietorship

Corporation

Sole

Limited Partnership

Limited Liability Corporation

Limited Liability Partnership

Subchapter S Corporation

Sign and notarize the form below, and, if necessary, complete the stockholder list below. Use more space as necessary.

Stockholders:

Name: _____

Name: _____

Home Address: _____

Home Address: _____

Name: _____

Name: _____

Home Address: _____

Home Address: _____

**EXHIBIT H
ATTACHMENT 5**

Subscribed and sworn before me this 31 day of October, 2023

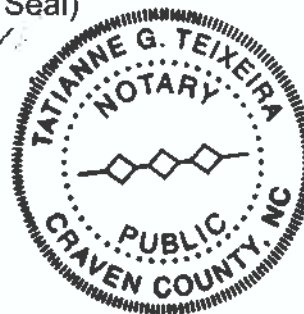
(Notary Public) Tatianne G. Teixeira

My Commission expires: 09/17/2028

Jessica Kent
(Affiant)

Jessica Kent, Proposals Manager
(Print name & title of affiant)

(Corporate Seal)





DISCLOSURE OF INVESTMENT ACTIVITIES IN IRAN FORM

STATE OF NEW JERSEY
DEPARTMENT OF THE TREASURY - DIVISION OF PURCHASE AND PROPERTY
33 WEST STATE STREET, P.O. BOX 230 TRENTON, NEW JERSEY 08625-0230

BID SOLICITATION # AND TITLE: Request for Proposals (RFP) ADMN24000076 for Translation Services, Interpretation Management Systems and Related Products
VENDOR NAME: Volatia Language Network, Inc.

Pursuant to N.J.S.A. 52:32-57, et seq. (P.L. 2012, c.25 and P.L. 2021, c.4) any person or entity that submits a bid or proposal or otherwise proposes to enter into or renew a contract must certify that neither the person nor entity, nor any of its parents, subsidiaries, or affiliates, is identified on the New Jersey Department of the Treasury's Chapter 25 List as a person or entity engaged in investment activities in Iran.

CHECK THE APPROPRIATE BOX

[X] I certify, pursuant to N.J.S.A. 52:32-57, et seq. (P.L. 2012, c.25 and P.L. 2021, c.4), that neither the Vendor/Bidder listed above nor any of its parents, subsidiaries, or affiliates is listed on the New Jersey Department of the Treasury's Chapter 25 List of entities determined to be engaged in prohibited activities in Iran.

OR

[] I am unable to certify as above because the Vendor/Bidder and/or one or more of its parents, subsidiaries, or affiliates is listed on the New Jersey Department of the Treasury's Chapter 25 List. I will provide a detailed, accurate and precise description of the activities of the Vendor/Bidder, or one of its parents, subsidiaries or affiliates, has engaged in regarding investment activities in Iran by completing the information requested below.

Entity Engaged in Investment Activities
Relationship to Vendor/ Bidder
Description of Activities

Blank lines for providing details on investment activities.

Duration of Engagement
Anticipated Cessation Date

*Attach Additional Sheets If Necessary.

CERTIFICATION

I, the undersigned, certify that I am authorized to execute this certification on behalf of the Vendor, that the foregoing information and any attachments hereto, to the best of my knowledge are true and complete. I acknowledge that the State of New Jersey is relying on the information contained herein, and that the Vendor is under a continuing obligation from the date of this certification through the completion of any contract(s) with the State to notify the State in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification. If I do so, I may be subject to criminal prosecution under the law, and it will constitute a material breach of my contract(s) with the State, permitting the State to declare any contract(s) resulting from this certification void and unenforceable.

Handwritten signature: Jessica Kent

10/31/2023

Signature

Date

Jessica Kent, Proposal Manager

Print Name and Title

NEW JERSEY DEPARTMENT OF THE TREASURY
DIVISION OF REVENUE AND ENTERPRISE SERVICES

CERTIFICATE OF AUTHORITY

VOLATIA LANGUAGE NETWORK INC.
0451036125

The above-named FOREIGN FOR-PROFIT CORPORATION was duly filed in accordance with New Jersey State Law on 10/17/2023 and was assigned identification number 0451036125. Following are the articles that constitute its original certificate.

1. **Name:**
VOLATIA LANGUAGE NETWORK INC.
2. **Registered Agent:**
C T CORPORATION SYSTEM
3. **Registered Office:**
820 BEAR TAVERN ROAD
WEST TRENTON, NEW JERSEY 08628
4. **Business Purpose:**
TO PROVIDE INTERPRETATION AND TRANSLATION SERVICES
5. **Incorporated Under the Laws of:**
VIRGINIA ON 02/26/2019
6. **Effective Date of this filing is:**
10/17/2023
7. **Main Business Address:**
1327 GRANDIN RD. SW
ROANOKE, VIRGINIA 24015

Signatures:

BARAKA KASONGO
CEO



Certificate Number : 4222979759

Verify this certificate online at

https://www1.state.nj.us/TYTR_StandngCert/JSP/Verify_Cert.jsp

IN TESTIMONY WHEREOF, I have
hereunto set my hand and
affixed my Official Seal
17th day of October, 2023

A handwritten signature in black ink, appearing to read "Elizabeth Maher Muoio".

Elizabeth Maher Muoio
State Treasurer

THIS PAGE IS INTENTIONALLY LEFT BLANK