Security Questionnaire

|  |  |
| --- | --- |
| **Response Code** | **Definition** |
| Y = Yes   | Requirement can be implemented “out of box” without customizations or modifications to the existing application  |
| N = No   | Requirement will not be implemented  |
| Cu = Customization   | Requirement can be met by changing existing solution or through use of solution tools (NOTE: In Comments column, describe the customization and the estimated level of complexity – High, Medium, or Low)  |
| F = Future   | Requirement will be met by packaged solution currently under development, in Beta test, or not yet released (NOTE: In Comments column, indicate expected release date and any anticipated additional cost)  |
| 3 = 3rd Party  | Requirement will be met by 3rd party solution package that is included in this proposal (NOTE: In Comments column, indicate name of proposed 3rd party solution package and proposed interface/integration services)  |
| Co = Configuration   | Requirement can be met through changes to setting of tables, switches, and rules without modification to source code (NOTE: In Comments, describe any changes to “out of box” workflow functionality)  |

|  |  |  |
| --- | --- | --- |
| **City of Cleveland Requirements**  | **Response to Requirements**  | **Comments/Clarifications**  |
| **Application & Interface Security**  | **Y**  | **N**  | **CU**  | **F**  | **3**  | **CO**  |
| Do you use OWASP guidelines or another standard to build your application securely?  |    |    |    |    |    |    |    |
| Do you review your application for security vulnerabilities and address any issues prior to deployment?  |    |    |    |    |    |    |    |
| **Business Continuity Management & Operational Resilience**  |   |   |   |   |   |   |   |
| Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated in your disaster recovery plan?  |    |    |    |    |    |    |    |
| Do you test your backup or redundancy mechanisms at least annually?  |    |    |    |    |    |    |    |
| **Change Control & Configuration Management**  |   |   |   |   |   |   |   |
| Are there procedures in place to triage and remedy reported bugs and security vulnerabilities?  |    |    |    |    |    |    |    |
| **Datacenter Security**  |   |   |   |   |   |   |   |
| Are physical security perimeters (e.g., fences, walls, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols and/or alarms) implemented at the data center storing City data?  |    |    |    |    |    |    |    |
| **Governance and Risk Management**  |   |   |   |   |   |   |   |
| Do you maintain an Information Security Management Program (ISMP)?  |    |    |    |    |    |    |    |
| Do you have a risk assessment process, performed at least annually, calculating the likelihood and impact of all identified risks?  |    |    |    |    |    |    |    |
| **Human Resources**  |   |   |   |   |   |   |   |
| Are systems in place to monitor for privacy breaches and notify City expeditiously if our data is exposed or compromised?  |    |    |    |    |    |    |    |
| Are all employees, contractors and third parties with access to data, systems, and networks, subject to background verification?  |    |    |    |    |    |    |    |
| Do you train your employees regarding their information security roles and responsibilities?  |    |    |    |    |    |    |    |
| Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?  |    |    |    |    |    |    |    |
| Are personnel trained and provided with awareness programs at least once every 3 years?  |    |    |    |    |    |    |    |
| Are documented policies, procedures and guidelines in place to govern change in employment and/or termination?  |    |    |    |    |    |    |    |
| Do the above procedures and guidelines account for timely revocation of access and return of assets?  |    |    |    |    |    |    |    |
| Do you access and share City data/metadata?  |    |    |    |    |    |    |    |
| Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?  |    |    |    |    |    |    |    |
| **Identity & Access Management**  |   |   |   |   |   |   |   |
| Do you restrict, log and monitor access to your information security management systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)  |    |    |    |    |    |    |    |
| Do you monitor and log privileged access (administrator level) to information security management systems?  |    |    |    |    |    |    |    |
| Are controls in place to prevent unauthorized access to your application, program or object source code?  |    |    |    |    |    |    |    |
| Do you provide multi-failure disaster recovery capability?  |    |    |    |    |    |    |    |
| Do you have more than one provider for each service you depend on?  |    |    |    |    |    |    |    |
| Do you review entitlements for all system users and administrators at least annually?  |    |    |    |    |    |    |    |
| Do you revoke or modify access upon any change in status of employees, contractors, business partners or involved third parties (termination, transfer or contract end)?  |    |    |    |    |    |    |    |
| Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?  |    |    |    |    |    |    |    |
| Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?  |    |    |    |    |    |    |    |
| Do you support password (minimum length of 10, age, history of greater than 25, complexity upper/lower/digit/symbol) and account lockout (lockout threshold 5 attempts, lockout duration 15 or greater) policy enforcement?  |    |    |    |    |    |    |    |
| Do you allow tenants/customers to define password and account lockout policies for their accounts?  |    |    |    |    |    |    |    |
| Do you support the ability to force password changes upon first logon?  |    |    |    |    |    |    |    |
| Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?  |    |    |    |    |    |    |    |
| Are utilities that can manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?  |    |    |    |    |    |    |    |
| Do you have a capability to detect and respond to attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?  |    |    |    |    |    |    |    |
| **Infrastructure & Virtualization Security**  |   |   |   |   |   |   |   |
| Are file integrity (host) and network intrusion detection (IDS) tools implemented?  |    |    |    |    |    |    |    |
| Is physical and logical user access to audit logs restricted to authorized personnel?  |    |    |    |    |    |    |    |
| Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?  |    |    |    |    |    |    |    |
| Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?  |    |    |    |    |    |    |    |
| Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?  |    |    |    |    |    |    |    |
| Do your system capacity requirements take into account current, projected and anticipated capacity needs for all systems?  |    |    |    |    |    |    |    |
| Are security vulnerability assessment tools or services virtualization aware?  |    |    |    |    |    |    |    |
| Do you regularly review allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?  |    |    |    |    |    |    |    |
| Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs?  |    |    |    |    |    |    |    |
| Do you logically and physically segregate production and non-production environments?  |    |    |    |    |    |    |    |
| Are wireless security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings)  |    |    |    |    |    |    |    |
| Can you detect the presence of unauthorized (rogue) network devices and immediately disconnect them from the network?  |    |    |    |    |    |    |    |
| Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?  |    |    |    |    |    |    |    |
| Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?  |    |    |    |    |    |    |    |
| **Mobile Security**  |   |   |   |   |   |   |   |
| Do you allow mobile devices (such as smartphone and tablets) to access your private networks?  |    |    |    |    |    |    |    |
| **Security Incident Management, E-Discovery & Cloud Forensic**  |   |   |   |   |   |   |   |
| Do you maintain liaisons and points of contact with local authorities to contact immediately in the case of a serious attack or incident (e.g., DDoS or Ransomware)?  |    |    |    |    |    |    |    |
| Do you have a documented security incident response plan?  |    |    |    |    |    |    |    |
| Does your logging and monitoring framework allow isolation of an incident to specific tenants?   |    |    |    |    |    |    |    |
| **Supply Chain Management, Transparency and Accountability**  |   |   |   |   |   |   |   |
| Do you have cloud supply chain providers (i.e., SaaS sits on top of a PaaS or IaaS provided by a 3rd party)?  |    |    |    |    |    |    |    |
| Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?  |    |    |    |    |    |    |    |
| Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?  |    |    |    |    |    |    |    |
| Do you collect capacity and use data for all relevant components of your cloud service offering?  |    |    |    |    |    |    |    |
| Do you provide tenants with capacity planning and use reports?  |    |    |    |    |    |    |    |
| Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?  |    |    |    |    |    |    |    |
| Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?  |    |    |    |    |    |    |    |
| Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?  |    |    |    |    |    |    |    |
| Does legal counsel review all third-party agreements?  |    |    |    |    |    |    |    |
| Do third-party agreements include provision for the security and protection of information and assets?  |    |    |    |    |    |    |    |
| Do you provide the client with a list and copies of all sub-processing agreements and keep this updated?  |    |    |    |    |    |    |    |
| Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?  |    |    |    |    |    |    |    |
| Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?  |    |    |    |    |    |    |    |
| Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?  |    |    |    |    |    |    |    |
| Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?  |    |    |    |    |    |    |    |
| Do you review all agreements, policies and processes at least annually?  |    |    |    |    |    |    |    |
| Do you assure reasonable information security across your information supply chain by performing an annual review?  |    |    |    |    |    |    |    |
| Does your annual review include all partners/third-party providers upon which your information supply chain depends?  |    |    |    |    |    |    |    |
| Do you permit tenants to perform independent vulnerability assessments?  |    |    |    |    |    |    |    |
| Do you have external third-party services conduct vulnerability scans and periodic penetration tests on your applications and networks?  |    |    |    |    |    |    |    |
| **Threat and Vulnerability Management**  |   |   |   |   |   |   |   |
| Do you have anti-malware programs installed on all of your systems, with at least daily updates?  |    |    |    |    |    |    |    |
| Do you conduct vulnerability scans at least monthly?  |    |    |    |    |    |    |    |
| Do you conduct application-layer vulnerability scans at least semi-annually?  |    |    |    |    |    |    |    |
| Can you rapidly deploy patches across all of your computing devices, applications and systems?  |    |    |    |    |    |    |    |