**SCHEDULE C-3-2 – CLOUD SECURITY RISK ASSESSMENT QUESTIONNAIRE**

**My Surrey Portal Identity Management Software**

**Cloud Security Risk Assessment Questionnaire**

|  |  |
| --- | --- |
| **Date:** |  |
| **Vendor Contact Name:** |  |

# Contents

[Contents 2](#_Toc449357552)

[1. Cloud Security 3](#_Toc449357553)

[1.1. Cloud Security Certification & Assurance 3](#_Toc449357554)

[1.2. Cloud Security Certification & Assurance 4](#_Toc449357555)

# Cloud Security

|  |  |
| --- | --- |
| **This section must be completed for any CLOUD BASED solution or solution that has a CLOUD BASED COMPONENT. If your product does not have any cloud based components, then this section does not need to be completed.** | |
|  | **Please Check this box if your product has no cloud based components. Otherwise, please answer the questions below.** |

|  |
| --- |
| Cloud Security Certification & Assurance |

|  |  |  |
| --- | --- | --- |
| **Cloud Security Certification** | **Yes** | **No** |
| Has the cloud service undergone any third party cloud security assurance or certification (example: ISO/IEC 27001/27002:2013, ISO 27018, IRAP, SOC 2, UK G-Cloud, etc.)?  **If yes, please indicate which certification was achieved and provide a copy of the certification or assurance certificate.** |  |  |
| It the cloud service provider registered with the Cloud Security Alliance “Security, Trust & Assurance Registry”?  **If yes, please indicate which level of assurance has achieved.** |  |  |
| Is your cloud service PCI Certified?  **If yes, please provide a copy of the PCI certification.** |  |  |
| Has the cloud service organization completed any industry standard cloud security self-assessment (example: Cloud Security Alliance Cloud Controls Matrix).  **If yes, please provide a copy of the self-assessment.** |  |  |

**If you answered yes to ANY of the four (4) questions in the “1.1 Cloud Security Certification & Assurance” section above, then you do not have to complete the remainder of this section. If you answered no to ALL the questions above, you MUST complete the rest of this section.**

**The questionnaire below is based on the Cloud Security Alliance’s “Cloud Controls Matrix”**

|  |  |  |
| --- | --- | --- |
| Cloud Security Certification & Assurance | | |
| **Application & Interface Security** | **Yes** | **No** |
| Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)? |  |  |
| Do you use an automated source code analysis tool to detect security defects in code prior to production? |  |  |
| Do you use manual source-code analysis to detect security defects in code prior to production? |  |  |
| Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security? |  |  |
| (SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production? |  |  |
| Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems? |  |  |
| Are all requirements and trust levels for customers’ access defined and documented? |  |  |
| Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data? |  |  |
| Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)? |  |  |
| **Audit Assurance & Compliance** | **Yes** | **No** |
| Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance? |  |  |
| Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance? |  |  |
| Do you conduct internal audits regularly as prescribed by industry best practices and guidance? |  |  |
| Do you conduct external audits regularly as prescribed by industry best practices and guidance? |  |  |
| Are the results of the penetration tests available to tenants at their request? |  |  |
| Are the results of internal and external audits available to tenants at their request? |  |  |
| Do you have an internal audit program that allows for cross-functional audit of assessments? |  |  |
| Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data? |  |  |
| Do you have capability to recover data for a specific customer in the case of a failure or data loss? |  |  |
| Do you have the capability to restrict the storage of customer data to specific countries or geographic locations? |  |  |
| Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements? |  |  |
| **Change Control & Configuration Management** | **Yes** | **No** |
| Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities? |  |  |
| Is documentation available that describes the installation, configuration and use of products/services/features? |  |  |
| Do you have controls in place to ensure that standards of quality are being met for all software development? |  |  |
| Do you have controls in place to detect source code security defects for any outsourced software development activities? |  |  |
| Do you provide your tenants with documentation that describes your quality assurance process? |  |  |
| Is documentation describing known issues with certain products/services available? |  |  |
| Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings? |  |  |
| Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions? |  |  |
| Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems? |  |  |
| Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it? |  |  |

|  |  |  |
| --- | --- | --- |
| **Datacenter Location** | **Yes** | **No** |
| Are your datacenters located and backed up exclusively in Canada?  If yes, please identify Canadian datacenter locations:  Click here to enter text.  If no, please identify the locations (including the country in which data will reside):  Click here to enter text. |  |  |
| **Data Security & Information Lifecycle Management** | **Yes** | **No** |
| Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)? |  |  |
| Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)? |  |  |
| Do you have a capability to use system geographic location as an authentication factor? |  |  |
| Can you provide the physical location/geography of storage of a tenant’s data upon request? |  |  |
| Can you provide the physical location/geography of storage of a tenant's data in advance? |  |  |
| Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)? |  |  |
| Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation? |  |  |
| Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems? |  |  |
| Can you ensure that data does not migrate beyond a defined geographical residency? |  |  |
| Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)? |  |  |
| Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)? |  |  |
| Are policies and procedures established for labeling, handling and the security of data and objects that contain data? |  |  |
| Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data? |  |  |
| Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments? |  |  |
| Are the responsibilities regarding data stewardship defined, assigned, documented and communicated? |  |  |
| Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant? |  |  |
| Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource? |  |  |
| **Datacenter Security** | **Yes** | **No** |
| Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? |  |  |
| Do you maintain a complete inventory of all of your critical supplier relationships? |  |  |
| Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented? |  |  |
| Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? |  |  |
| Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another? (e.g., offsite backups, business continuity failovers, replication) |  |  |
| Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment? |  |  |
| Can you provide evidence that policies, standards and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas? |  |  |
| Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures? |  |  |
| Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)? |  |  |
| Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process? |  |  |
| Do you restrict physical access to information assets and functions by users and support personnel? |  |  |
| **Encryption & Key Management** | **Yes** | **No** |
| Do you provide encryption for data while in transit and while at rest for tenant data?  If yes, please list the encryption algorithms used for:  Data in Transit: Click here to enter text.  Data at Rest: Click here to enter text. |  |  |
| Do you have key management policies binding keys to identifiable owners? |  |  |
| Do you have a capability to allow creation of unique encryption keys per tenant? |  |  |
| Do you have a capability to manage encryption keys on behalf of tenants? |  |  |
| Do you maintain key management procedures? |  |  |
| Do you have documented ownership for each stage of the lifecycle of encryption keys? |  |  |
| Do you utilize any third party/open source/proprietary frameworks to manage encryption keys? |  |  |
| Do you encrypt tenant data at rest (on disk/storage) within your environment? |  |  |
| Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances? |  |  |
| Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g. identity-based encryption)? |  |  |
| Do you have documentation establishing and defining your encryption management policies, procedures and guidelines? |  |  |
| Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms? |  |  |
| Are your encryption keys maintained by the cloud consumer or a trusted key management provider? |  |  |
| Do you store encryption keys in the cloud? |  |  |
| Do you have separate key management and key usage duties? |  |  |

|  |  |  |
| --- | --- | --- |
| **Governance and Risk Management** | **Yes** | **No** |
| Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)? |  |  |
| Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? |  |  |
| Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards? |  |  |
| Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)? |  |  |
| Do you conduct risk assessments associated with data governance requirements at least once a year? |  |  |
| Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility? |  |  |
| Do you provide tenants with documentation describing your Information Security Management Program (ISMP)? |  |  |
| Do you review your Information Security Management Program (ISMP) least once a year? |  |  |
| Do you ensure your providers adhere to your information security and privacy policies? |  |  |
| Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)? |  |  |
| Do you have agreements to ensure your providers adhere to your information security and privacy policies? |  |  |
| Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards? |  |  |
| Do you disclose which controls, standards, certifications and/or regulations you comply with? |  |  |
| Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures? |  |  |
| Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures? |  |  |
| Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective? |  |  |
| Do you notify your tenants when you make material changes to your information security and/or privacy policies? |  |  |
| Do you perform, at minimum, annual reviews to your privacy and security policies? |  |  |
| Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods? |  |  |
| Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)? |  |  |
| Do you have a documented, organization-wide program in place to manage risk? |  |  |
| **Human Resources** | **Yes** | **No** |
| Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data? |  |  |
| Is your Privacy Policy aligned with industry standards? |  |  |
| Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates, contractors and involved third parties subject to background verification? |  |  |
| Do you specifically train your employees regarding their specific role and the information security controls they must fulfill? |  |  |
| Do you document employee acknowledgment of training they have completed? |  |  |
| Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information? |  |  |
| Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems? |  |  |
| Are personnel trained and provided with awareness programs at least once a year? |  |  |
| 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? |  |  |
| Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g. laptops, cell phones and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization’s facilities)? |  |  |
| Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals? |  |  |
| Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? |  |  |
| Do you provide documentation regarding how you may or access tenant data and metadata? |  |  |
| Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)? |  |  |
| Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies? |  |  |
| Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant data? |  |  |
| Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity? |  |  |
| Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements? |  |  |
| Are users made aware of their responsibilities for maintaining a safe and secure working environment? |  |  |
| Are users made aware of their responsibilities for leaving unattended equipment in a secure manner? |  |  |
| Do your data management policies and procedures address tenant and service level conflicts of interests? |  |  |
| Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data? |  |  |
| Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine? |  |  |
| **Identity & Access Management** | **Yes** | **No** |
| 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? |  |  |
| Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes? |  |  |
| Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes? |  |  |
| Do you use dedicated secure networks to provide management access to your cloud service infrastructure? |  |  |
| Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access? |  |  |
| Do you manage and store the user identity of all personnel who have network access, including their level of access? |  |  |
| Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering? |  |  |
| Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only? |  |  |
| Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only? |  |  |
| Do you provide multi-failure disaster recovery capability? |  |  |
| Do you monitor service continuity with upstream providers in the event of provider failure? |  |  |
| Do you have more than one provider for each service you depend on? |  |  |
| Do you provide access to operational redundancy and continuity summaries, including the services you depend on? |  |  |
| Do you provide the tenant the ability to declare a disaster? |  |  |
| Do you provide a tenant-triggered failover option? |  |  |
| Do you share your business continuity and redundancy plans with your tenants? |  |  |
| Do you document how you grant and approve access to tenant data? |  |  |
| Do you have a method of aligning provider and tenant data classification methodologies for access control purposes? |  |  |
| Does your management provision the authorization and restrictions for user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components? |  |  |

|  |  |  |
| --- | --- | --- |
| Do your provide upon request user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components? |  |  |
| Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)? |  |  |
| If users are found to have inappropriate entitlements, are all remediation and certification actions recorded? |  |  |
| Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data? |  |  |
| Is timely de-provisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties? |  |  |
| Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization? |  |  |
| Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service? |  |  |
| Do you use open standards to delegate authentication capabilities to your tenants? |  |  |
| Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users? |  |  |
| Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access? |  |  |
| Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data? |  |  |
| Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access? |  |  |
| Do you allow tenants to use third-party identity assurance services? |  |  |
| Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) 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 significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored? |  |  |
| Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)? |  |  |
| Are attacks that target the virtual infrastructure prevented with technical controls? |  |  |
| **Infrastructure & Virtualization Security** | **Yes** | **No** |
| Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents? |  |  |
| Is physical and logical user access to audit logs restricted to authorized personnel? |  |  |
| Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done? |  |  |
| Are audit logs centrally stored and retained? |  |  |
| 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)? |  |  |
| Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g. portals or alerts)? |  |  |
| Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? |  |  |
| Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios? |  |  |
| Do you restrict use of the memory oversubscription capabilities present in the hypervisor? |  |  |
| Do your system capacity requirements take into account current, projected and anticipated capacity needs for all systems used to provide services to the tenants? |  |  |
| Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants? |  |  |
| Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g. virtualization aware)? |  |  |
| For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution? |  |  |
| Do you regularly update network architecture diagrams that include data flows between security domains/zones? |  |  |
| Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network? |  |  |
| Are all firewall access control lists documented with business justification? |  |  |
| Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e. antivirus, file integrity monitoring and logging) as part of their baseline build standard or template? |  |  |
| For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes? |  |  |
| For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments? |  |  |
| Do you logically and physically segregate production and non-production environments? |  |  |
| Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements? |  |  |
| Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory and contractual requirements? |  |  |
| Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments? |  |  |
| Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data? |  |  |
| Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers? |  |  |
| Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers? |  |  |

|  |  |  |
| --- | --- | --- |
| Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g. two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)? |  |  |
| Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic? |  |  |
| Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings) |  |  |
| Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect 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? |  |  |
| **Interoperability & Portability** | **Yes** | **No** |
| Do you publish a list of all APIs available in the service and indicate which are standard and which are customized? |  |  |
| Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)? |  |  |
| Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications? |  |  |
| Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service? |  |  |
| Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols? |  |  |
| Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved? |  |  |
| Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability? |  |  |
| Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review? |  |  |
| **Mobile Security** | **Yes** | **No** |
| Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training. |  |  |
| A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data. |  |  |
| The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store. |  |  |
| The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage. |  |  |
| The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program. |  |  |
| All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data. |  |  |
| The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues. |  |  |
| The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage. |  |  |
| An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD), will be included for each device in the inventory. |  |  |
| A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data. |  |  |
| The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls. |  |  |

|  |  |  |
| --- | --- | --- |
| The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting) and is enforced through detective and preventative controls on the device or through a centralized device management system (e.g. mobile device management). |  |  |
| The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case a wipe of the device is required. |  |  |
| BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls. |  |  |
| Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes. |  |  |
| Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements. |  |  |
| The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported). |  |  |
| All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT. |  |  |
| Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely. |  |  |
| The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. |  |  |
| **Security Incident Management, E-Discovery & Cloud Forensics** | **Yes** | **No** |
| Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations? |  |  |
| Do you have a documented security incident response plan? |  |  |
| Do you integrate customized tenant requirements into your security incident response plans? |  |  |
| Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents? |  |  |
| Have you tested your security incident response plans in the last year? |  |  |
| Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting? |  |  |
| Does your logging and monitoring framework allow isolation of an incident to specific tenants? |  |  |
| Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls? |  |  |
| Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques? |  |  |
| Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data? |  |  |
| Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas? |  |  |
| Do you monitor and quantify the types, volumes and impacts on all information security incidents? |  |  |
| Will you share statistical information for security incident data with your tenants upon request? |  |  |
| **Supply Chain Management, Transparency and Accountability** | **Yes** | **No** |
| Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them? |  |  |
| 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 & Vulnerability Management** | **Yes** | **No** |
| Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems? |  |  |
| Do you ensure that security threat detection systems using signatures, lists or behavioral patterns are updated across all infrastructure components within industry accepted time frames? |  |  |
| Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices? |  |  |
| Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices? |  |  |

|  |  |  |
| --- | --- | --- |
| Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices? |  |  |
| Will you make the results of vulnerability scans available to tenants at their request? |  |  |
| Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems? |  |  |
| Will you provide your risk-based systems patching time frames to your tenants upon request? |  |  |
| Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy? |  |  |
| Is all unauthorized mobile code prevented from executing? |  |  |
| **Business Continuity Management & Operational Resilience** | | |
| Do you provide tenants with geographically resilient hosting options? |  |  |
| Do you provide tenants with infrastructure service failover capability to other providers? |  |  |
| Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness? |  |  |
| Do you provide tenants with documentation showing the transport route of their data between your systems? |  |  |
| Can tenants define how their data is transported and through which legal jurisdictions? |  |  |
| Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system? |  |  |
| Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied? |  |  |
| Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)? |  |  |
| If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities? |  |  |
| If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time? |  |  |
| If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider? |  |  |
| If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location? |  |  |
| Does your cloud solution include software/provider independent restore and recovery capabilities? |  |  |
| Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)? |  |  |
| Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance? |  |  |
| Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants? |  |  |
| Do you provide customers with ongoing visibility and reporting of your SLA performance? |  |  |
| Are policies and procedures established and made available for all personnel to adequately support services operations’ roles? |  |  |
| Do you have technical control capabilities to enforce tenant data retention policies? |  |  |
| Do you have a documented procedure for responding to requests for tenant data from governments or third parties? |  |  |
| Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements? |  |  |