



Hexnode Responses to cloud security alliance consensus assessments initiative questionnaire

hexnode

111 Pine St #1225, San Francisco, CA 94111
+1-833-HEXNODE (439-6633)

| Control Group | CID | Consensus Assessment Questions | Hexnode response |
|---|----------|--|---|
| Application & Interface Security <i>Application Security</i> | AIS-01.1 | 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)? | Hexnode Secure Development Lifecycle include well-defined practices in accordance with industry standards and regulations. All prospective features are thoroughly reviewed for security and GDPR-based privacy concerns before going into development. |
| | AIS-01.2 | Do you use an automated source code analysis tool to detect security defects in code prior to production? | Every line of code goes through a series of automatic and manual reviews and threat analysis tests. This allows the developers to detect and remediate for any vulnerabilities identified during the process. |
| | AIS-01.3 | Do you use manual source-code | Yes, source-codes go through a series of |

| | | | |
|--|----------|---|--|
| | | analysis to detect security defects in code prior to production? | manual reviews throughout its lifecycle. Weekly review meetings are held to analyze the integrity of the code prior to production. |
| | AIS-01.4 | Do you verify that all your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security? | Hexnode keeps tabs over all its vendors through constant reviews over vendor's security policies, SDLC strategies, privacy controls and certifications. |
| | AIS-01.5 | (SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production? | Yes, at Hexnode we exercise a series of stringent reviews and vulnerability testing (both manual and automated) before deployment. An effective feedback system is in place to address vulnerabilities before release. |
| | AIS-02.1 | Are all identified security, | Yes. Customers agree to Hexnode's SaaS Services |

| | | | |
|---|----------|--|--|
| Application & Interface Security <i>Customer Access Requirements</i> | | contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems? | Agreement in a clickwrap format before being granted access to Hexnode software. We also have other agreements in place to contractually bind customers and ensure meeting regulatory requirements. |
| | AIS-02.2 | Are all requirements and trust levels for customers' access defined and documented? | Hexnode solutions are available as SaaS. There is a precise demarcation of Hexnode's own administrative responsibilities and that of customers. They are clearly communicated during customer onboarding and documented in our help. |
| Application & Interface Security <i>Data Integrity</i> | AIS-03.1 | Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application | Hexnode MDM performs routine integrity checks in order to prevent manual or systematic processing errors, data corruption or misuse. Hexnode validates the |

| | | | |
|---|----------|---|---|
| | | interfaces and databases to prevent manual or systematic processing errors or corruption of data? | <p>inputs received from its users or other systems to limit the potential of malicious actions.</p> <p>The databases are backed up on a daily basis. The data backups are tested for recovery every month.</p> |
| Application & Interface Security <i>Data Security / Integrity</i> | AIS-04.1 | Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)? | <p>Hexnode exercises a set of layered security services and cryptographic framework that are in accordance with Industry standards.</p> <p>Hexnode's Data Security Architecture is designed to implement preventive, detective and remediation policies ensuring robust architectural security.</p> |
| Audit Assurance & Compliance <i>Audit Planning</i> | AAC-01.1 | Do you produce audit assertions using a structured, industry accepted | Hexnode conducts risk analysis tests to ensure industry compliances that aligns with GDPR, |

| | | | |
|---|----------|---|---|
| | | format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)? | HIPAA and other standards. Periodic internal and third-party audits are utilized to ensure full compliance. |
| Audit Assurance & Compliance <i>Independent Audits</i> | AAC-02.1 | Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports? | Our ISMS is based on ISO 27001 standard and we are conducting third-party audits for a formal certification. We also have SOC 2 and similar certifications on our roadmap. Summary of the relevant reports can be made available to customers under an NDA, once the ISO Certification process is complete. |
| | AAC-02.2 | Do you conduct network penetration tests of your cloud service infrastructure regularly as | The penetration tests are conducted periodically at an interval of three months. They are handled by our security team in |

| | | | |
|--|----------|--|--|
| | | prescribed by industry best practices and guidance? | accordance with the industry's best practices. |
| | AAC-02.3 | Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance? | Yes. They are conducted periodically at an interval of three months. They are handled by our security team in accordance with the industry's best practices. |
| | AAC-02.4 | Do you conduct internal audits regularly as prescribed by industry best practices and guidance? | Hexnode conducts periodic internal audits and risk analysis to identify vulnerabilities and has an effective feedback system in place for remediation. |
| | AAC-02.5 | Do you conduct external audits regularly as prescribed by industry best practices and guidance? | Hexnode's pursuit of ISO 27001 compliance requires mandatory third-party audits based on industry best practices. |

| | | | |
|--|----------|--|---|
| | AAC-02.6 | Are the results of the penetration tests available to tenants at their request? | The results of the penetration tests are confidential and hence are currently not made available to tenants upon request. These tests are conducted with the aim to improve Hexnode's overall security posture with regards to its infrastructure and application. At present, only authorized personnel will have access to the information. |
| | AAC-02.7 | Are the results of internal and external audits available to tenants at their request? | Certification for ISO 27001 is currently an ongoing process, a summary of the report will be made available to interested customers once the process is complete. Internal audit reports are classified as containing sensitive data |
| | AAC-02.8 | Do you have an internal audit program that allows for cross-functional audit of assessments? | |

| | | | |
|---|----------|---|--|
| | | | and are not available to the public, to ensure data security. |
| Audit Assurance & Compliance <i>Information System Regulatory Mapping</i> | AAC-03.1 | 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? | Hexnode provides a multi-tenant SaaS solution where the customer data will be logically segmented. Dedicated sub-domains will be assigned per tenant (e.g., johndoe.hexnodemdm.com). Each user will have a unique ID and all the data and objects specific to the user will be stored in it. Our application log will consist of log details, IP details and security related administrative and configuration settings. |
| | AAC-03.2 | Do you have capability to recover data for a specific customer in the case of a failure or data loss? | Individual customer data can be recovered from the Hexnode backup. |
| | AAC-03.3 | Do you have the capability to restrict | Currently, Hexnode hosts its cloud services |

| | | | |
|---|----------|--|--|
| | | the storage of customer data to specific countries or geographic locations? | on AWS (Amazon Web Services) and the data centers are segmented to United States and EU. |
| | AAC-03.4 | 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? | Yes, Hexnode continuously monitors changes in regulatory requirements and reports the change to relevant jurisdictions, to ensure legal and regulatory compliance. |
| | | | |
| Business Continuity Management & Operational Resilience <i>Business Continuity Planning</i> | BCR-01.1 | Do you provide tenants with geographically resilient hosting options? | Currently, Hexnode hosts its cloud services on AWS (Amazon Web Services) and the data centers are segmented to United States and EU. |

| | | | |
|--|----------|---|---|
| | BCR-01.2 | Do you provide tenants with infrastructure service failover capability to other providers? | Not applicable |
| Business Continuity Management & Operational Resilience <i>Business Continuity Testing</i> | BCR-02.1 | Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness? | Hexnode has a well-defined disaster recovery and business continuity plans that are subjected to regular testing. |
| Business Continuity Management & Operational Resilience <i>Power / Telecommunications</i> | BCR-03.1 | Do you provide tenants with documentation showing the transport route of their data between your systems? | Tenants can refer to the Hexnode architecture available in our website to get a general idea of data transport and TLS. |
| | BCR-03.2 | Can tenants define how their data is transported and through which legal jurisdictions? | <p>Customers can have a Data processing agreement signed and executed with Hexnode</p> <p>We regularly verify our legal, regulatory and</p> |

| | | | |
|--|----------|---|--|
| | | | contractual obligations to ensure compliance. |
| Business Continuity Management & Operational Resilience Documentation | BCR-04.1 | 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? | Hexnode hosts an internal network of guides and documentations which are made available to authorized personnel. |
| Business Continuity Management & Operational Resilience <i>Environmental Risks</i> | BCR-05.1 | Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied? | Our EU and US data centers are in some amongst the most secure locations available today. Geographically positioned in such a way as to minimize damage cause due to natural and deliberate attacks. |
| Business Continuity Management | BCR-06.1 | Are any of your data centers located in places that have a high | No |

| | | | |
|--|----------|---|---|
| & Operational Resilience <i>Equipment Location</i> | | probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)? | |
| Business Continuity Management & Operational Resilience <i>Equipment Maintenance</i> | BCR-07.1 | If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities? | Virtual infrastructure is not used since Hexnode is a SaaS product. |
| | BCR-07.2 | If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time? | |
| | BCR-07.3 | If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider? | |

| | | | |
|---|----------|---|--|
| | BCR-07.4 | 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? | |
| | BCR-07.5 | Does your cloud solution include software/provider independent restore and recovery capabilities? | |
| Business Continuity Management & Operational Resilience <i>Equipment Power Failures</i> | BCR-08.1 | Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)? | Our data centers receive continuous power supplies and are equipped with back-up power sources in case of a power failure. Tenants can refer the AWS website for detailed documentation on data center security. |

| | | | |
|--|----------|---|--|
| Business Continuity Management & Operational Resilience <i>Impact Analysis</i> | BCR-09.1 | Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance? | Business continuity and disaster recovery plans shall be implemented to ensure the continuity of our operations. Redundancies and other backup facilities will be maintained as well. If any incident that impact the customer occurs, it will be immediately resolved and made known to the customer via relevant teams within the organization |
| | BCR-09.2 | Do you make standards-based information security metrics (CSA, CMM, etc.) available to your tenants? | Hexnode standards-based information are not currently made available to customers. |
| | BCR-09.3 | Do you provide customers with ongoing visibility and reporting of your SLA performance? | Business continuity and disaster recovery plans shall be implemented to ensure the continuity of our operations. Redundancies and other backup facilities will be maintained as well. If any incident that impact the customer occur, it |

| | | | |
|---|----------|--|---|
| | | | will be resolved and made known to the customer via relevant teams within the organization. |
| | | | |
| Business Continuity Management & Operational Resilience Policy | BCR-10.1 | Are policies and procedures established and made available for all personnel to adequately support services operations' roles? | Policies and procedures are well established and made available on the Hexnode internal network, based on roles. It also houses comprehensive guides and documentation on performing operation functions. |
| Business Continuity Management & Operational Resilience Retention Policy | BCR-11.1 | Do you have technical control capabilities to enforce tenant data retention policies? | Customer holds complete control over addition and deletion of data. |
| | BCR-11.2 | Do you have a documented procedure for responding to requests for tenant data from governments or third parties? | Hexnode has a process in place for managing third-party requests for customer data. |

| | | | |
|--|----------|---|--|
| | BCR-11.4 | Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements? | Full back up of the customer data is done every day. Incremental backups are done every 10 minutes without interrupting the Hexnode instance that is being run by the user. |
| | BCR-11.5 | Do you test your backup or redundancy mechanisms at least annually? | Yes, backups are tested every month for recovery. |
| Change Control & Configuration Management <i>New Development / Acquisition</i> | CCC-01.1 | Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities? | Hexnode integration team is responsible for the acquisition process. The process follows well defined industry-best methodologies and helps define a standardized approach throughout the lifecycle. |
| | CCC-01.2 | Is documentation available that | Every acquisition and development processes |

| | | | |
|---|----------|---|---|
| | | describes the installation, configuration, and use of products/services/features? | are documented and are made available to authorized personnel. |
| Change Control & Configuration Management <i>Outsourced Development</i> | CCC-02.1 | Do you have controls in place to ensure that standards of quality are being met for all software development? | Hexnode Secure Development Lifecycle includes well-defined practices in accordance with industry standards and regulations. All prospective features are thoroughly reviewed for security and GDPR-based privacy concerns before going into development. Manual and automated reviews along with weekly developer meets to ensure code-compliance with security policies. |
| | CCC-02.2 | Do you have controls in place to detect source code security defects for any outsourced software | All the software development is done in-house. |

| | | | |
|--|----------|--|--|
| | | development activities? | |
| Change Control & Configuration Management <i>Quality Testing</i> | CCC-03.1 | Do you provide your tenants with documentation that describes your quality assurance process? | Hexnode has rigorous processes in place for QA testing which involves both manual and automated testing after development, before release and after bug fixes and vulnerability detection. All QA tests are well documented and are considered confidential due to the sensitive nature of the data housed within. |
| | CCC-03.2 | Is documentation describing known issues with certain products/services available? | The development and technical support team keeps track of known issues. The issues along with its fixes are documented within the release notes. |
| | CCC-03.3 | Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for | Hexnode has automatic and manual procedures in place to implement preventive, detective and remediation policies. |

| | | | |
|--|----------|--|--|
| | | product and service offerings? | <p>Detected vulnerabilities or bugs are classified based on potential severity.</p> <p>A system is in place that creates work tickets to prioritize and queue bugs/vulnerabilities for due action.</p> |
| | CCC-03.4 | Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions? | Prior to every release, Hexnode QA team reviews the final code to assure all debugging and test code elements are removed from released software versions. |
| Change Control & Configuration Management <i>Unauthorized Software Installations</i> | CCC-04.1 | Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems? | <p>Hexnode runs its own MDM console on every corporate device connected to its system to restrict un-authorized installation of third-party software and applications.</p> <p>A centrally managed threat defense policy is</p> |

| | | | |
|--|----------|--|---|
| | | | enforced on all systems exposed to vulnerabilities. |
| Change Control & Configuration Management <i>Production Changes</i> | CCC-05.1 | Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it? | Hexnode maintains detailed documentation that define changes made to its product. These documents are deemed confidential and are not made available to the customer. |
| Data Security & Information Lifecycle Management <i>Classification</i> | DSI-01.1 | 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)? | Instances assigned based on customers' data location requirements can be identified via metadata. |

| | | | |
|--|----------|--|--|
| | DSI-01.2 | Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)? | An asset inventory is used to manage all production assets. |
| | DSI-01.3 | Do you have a capability to use system geographic location as an authentication factor? | There are no direct geographic policies in place, but the customer can restrict end-user policies based on geographic location or Geofences, from the Hexnode portal. |
| | DSI-01.4 | Can you provide the physical location/geography of storage of a tenant's data upon request? | Hexnode hosts its cloud-based service, and all related data, on AWS data centers, which are localized based on tenant location. Hexnode can provide data when requested. |
| | DSI-01.5 | Can you provide the physical location/geography of storage of a | Hexnode hosts its cloud-based service, and all related data, on AWS data centers, which are |

| | | | |
|--|----------|---|---|
| | | tenant's data in advance? | chosen based on tenant location. Hexnode can provide data when requested. |
| | DSI-01.6 | Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)? | We have a data classification policy in place. Data is classified into Public, Internal, Client Confidential, Company Confidential. |
| | DSI-01.7 | Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation? | Hexnode hosts its cloud-based service, and all related data, on AWS data centers which are chosen based on tenant location. |
| Data Security & Information Lifecycle Management <i>Data Inventory / Flows</i> | DSI-02.1 | Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure | Yes, Hexnode maintains comprehensive documentation on the data flows within the Hexnode infrastructure system. |

| | | | |
|---|----------|--|---|
| | | network and systems? | |
| | DSI-02.2 | Can you ensure that data does not migrate beyond a defined geographical residency? | Yes |
| Data Security & Information Lifecycle Management <i>E-commerce Transactions</i> | DSI-03.1 | 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)? | Data transfer between client-server/device-console are encrypted based on industry best standards. Hexnode does not provide tenants with any methodologies. |
| | DSI-03.2 | 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 | All in-bound and out-bound data transfer are encrypted based on AWS standards. |

| | | | |
|--|----------|---|--|
| | | data from one environment to another)? | |
| Data Security & Information Lifecycle Management Handling / Labeling / Security Policy | DSI-04.1 | Are policies and procedures established for labeling, handling and the security of data and objects that contain data? | Hexnode has Data Protection Policies in place prioritizing security concerns relating to data and objects that house data. |
| | DSI-04.2 | Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data? | Hexnode has an information classification policy that ensures information is properly classified and labelled in accordance with the legal requirements, value, criticality and confidentiality. |
| Data Security & Information Lifecycle Management <i>Nonproduction Data</i> | DSI-05.1 | Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments? | Hexnode has measures in place to isolate data from one another. Lack of network links between different environments of the system ensure data is localized to its dedicated environment. |

| | | | |
|---|----------|--|--|
| Data Security & Information Lifecycle Management <i>Ownership / Stewardship</i> | DSI-06.1 | Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated? | Yes, Data handling and supervision authorities are clearly defined and communicated through documentations. Access to customer data or information is limited to authorized personnel and with the permission of the customer. |
| Data Security & Information Lifecycle Management <i>Secure Disposal</i> | DSI-07.1 | Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant? | Hexnode administers secure methods for deletion of customer data from the portal, along with any data in the backup, when requested by the customer or at the end of the service agreement. |
| | DSI-07.2 | Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant | In reference to DSI-07.1 the data will be completely removed on the request of the customer or on the termination of service agreement. |

| | | | |
|---|----------|--|---|
| | | data once a customer has exited your environment or has vacated a resource? | |
| Datacenter Security <i>Asset Management</i> | DCS-01.1 | Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? | Yes, Hexnode maintains a complete inventory of all its assets in accordance with the Asset Management policy. Assets are categorized based on their owners, who are kept accountable for proper asset management. |
| | DCS-01.2 | Do you maintain a complete inventory of all of your critical supplier relationships? | Hexnode maintains inventory of all supplier relationships, critical or otherwise. |
| Datacenter Security <i>Controlled Access Points</i> | DCS-02.1 | Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication | Complete information regarding physical and other forms of security are documented in the Hexnode Security Assessment document which can be accessed on request. |

| | | | |
|---|----------|--|--|
| | | mechanisms, reception desks, and security patrols) implemented? | |
| Datacenter Security <i>Equipment Identification</i> | DCS-03.1 | Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? | Hexnode hosts its data centers with AWS. AWS manages equipment identification in alignment with ISO 27001 standard. |
| Datacenter Security <i>Offsite Authorization</i> | DCS-04.1 | 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)? | Data centers are assigned to customers based on where they are located. Hexnode makes every attempt to keep data in the initially assigned locations and does not move data between physical location without customer permission, unless required to comply with the law or government bodies. In accordance with our business continuity and disaster recovery plans |

| | | | |
|--|----------|---|--|
| | | | and backup and restore policy, data could be moved to ensure the continuity of our operations and security of customer confidential data. These policies will be made available to customers upon request. |
| Datacenter Security <i>Offsite Equipment</i> | DCS-05.1 | Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment? | <p>Policies and procedures regarding asset management and repurposing of equipment are in alignment with AWS standards. AWS follows ISO 27001 standards for device repurposing and decommissioning.</p> <p>Refer to ISO 27001 standards; Annex A, domain 8 for additional details.</p> |
| Datacenter Security <i>Policy</i> | DCS-06.1 | Can you provide evidence that policies, standards, | Complete information regarding physical and other forms of security |

| | | | |
|----------------------------|----------|--|--|
| | | and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas? | are documented in the Hexnode Security Assessment document which can be accessed on request. |
| | DCS-06.2 | Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures? | Hexnode holds annual training sessions conducted by industry professionals. Minutes of the training sessions are made and Hexnode's documented policies, standards and procedures are stored internally and made available to all employees and relevant third parties. Prior to their employment, they are made to sign an NDA which details their responsibility with regards to maintaining information security. |
| Datacenter Security | DCS-07.1 | Do you allow tenants to specify | Data centers are assigned to customers |

| | | | |
|---|----------|--|--|
| <i>Secure Area Authorization</i> | | 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)? | based on where they are located. Hexnode makes every attempt to keep data in the initially assigned locations and do not move data between physical location without customer consent, unless required to comply with the law or government bodies. |
| Datacenter Security <i>Unauthorized Persons Entry</i> | DCS-08.1 | 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? | <p>Complete information regarding physical and other forms of security are documented in the Hexnode Security Assessment document which can be accessed on request.</p> <p>AWS is our cloud service provider and information regarding access and other security aspects of data center can be viewed here: https://aws.amazon.com/security/</p> |

| | | | |
|---|----------|---|---|
| | | | |
| Datacenter Security <i>User Access</i> | DCS-09.1 | Do you restrict physical access to information assets and functions by users and support personnel? | AWS is our cloud service provider and information regarding access and other security aspects of data center can be viewed here: https://aws.amazon.com/security/ |
| Encryption & Key Management <i>Entitlement</i> | EKM-01.1 | Do you have key management policies binding keys to identifiable owners? | All keys are managed and catalogued based on identifiable owners. The keys will be managed during its entire lifecycle via AWS Key Management System and in accordance with our cryptography policy. |
| Encryption & Key Management <i>Key Generation</i> | EKM-02.1 | Do you have a capability to allow creation of unique encryption keys per tenant? | |
| | EKM-02.2 | Do you have a capability to manage encryption keys on behalf of tenants? | |

| | | | |
|---|--------------|--|--|
| | EKM -02.3 | Do you maintain key management procedures? | |
| | EKM -02.4 | Do you have documented ownership for each stage of the lifecycle of encryption keys? | |
| | EKM -02.5 | Do you utilize any third party/open source/proprietary frameworks to manage encryption keys? | |
| Encryption & Key Management <i>Encryption</i> | EKM -03.1 | Do you encrypt tenant data at rest (on disk/storage) within your environment? | Hexnode utilizes AWS standards for data encryption. For more details on AWS security and encryption standards, visit: |
| | EKM -03.2 | Do you leverage encryption to protect data and virtual machine images during transport across and between networks and | https://aws.amazon.com/security/ When servers are hosted as on-premises, the tenant can choose the encryption of their choice. |

| | | | |
|---|----------|--|--|
| | | hypervisor instances? | All data stored in Hexnode internal servers will be encrypted using 256 AES encryption. |
| | EKM-03.3 | 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)? | |
| | EKM-03.4 | Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines? | These are defined within our cryptography policy. |
| Encryption & Key Management <i>Storage and Access</i> | EKM-04.1 | Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms? | Hexnode utilizes industry standard platform and data appropriate encryptions that are reviewed every year. |

| | | | |
|---|----------|--|---|
| | EKM-04.2 | Are your encryption keys maintained by the cloud consumer or a trusted key management provider? | All encryption keys are created and managed through AWS Key Management System (KMS). Refer: https://aws.amazon.com/kms/ |
| | EKM-04.3 | Do you store encryption keys in the cloud? | |
| | EKM-04.4 | Do you have separate key management and key usage duties? | |
| Governance and Risk Management <i>Baseline Requirements</i> | GRM-01.1 | Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)? | Hexnode maintains comprehensive documents on data flow and security aspects of components constituting the Hexnode infrastructure. |
| | GRM-01.2 | Do you have the capability to continuously monitor and report the compliance of your infrastructure | Systems are in place to report and monitor compliance with the security baselines that are documented by Hexnode which aligns |

| | | | |
|--|----------|--|--|
| | | against your information security baselines? | with AWS standards, which in turn are based on ISO 27001 standards. |
| | GRM-01.3 | Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards? | Not applicable as Hexnode is a SaaS product and uses AWS as its cloud service provider. |
| Governance and Risk Management <i>Risk Assessments</i> | GRM-02.1 | 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)? | Hexnode conducts regular risk assessment tests and reviews existing risk management policies. Risk assessment tests and risk management policies are well documented and made available to authorized personnel. |
| | GRM-02.2 | Do you conduct risk assessments associated with data governance | Yes, risk assessments are done annually. |

| | | | |
|--|----------|--|---|
| | | requirements at least once a year? | |
| Governance and Risk Management <i>Management Oversight</i> | GRM-03.1 | 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? | All personnel handling managerial roles are well versed with security policies and responsible for upholding the company's stand on security. All employees attend annual security meets to ensure complete awareness of security policies, procedure, and standards. |
| Governance and Risk Management <i>Management Program</i> | GRM-04.1 | Do you provide tenants with documentation describing your Information Security Management Program (ISMP)? | Hexnode provides interested customers with detailed documentation highlighting all its security functions. |
| | GRM-04.2 | Do you review your Information Security Management | Security documentations are reviewed regularly to ensure continued compliance. |

| | | | |
|--|----------|--|--|
| | | Program (ISMP) at least once a year? | |
| Governance and Risk Management <i>Management Support / Involvement</i> | GRM-05.1 | Do you ensure your providers adhere to your information security and privacy policies? | All providers are contractually obliged with Hexnode to maintain security and privacy policies. |
| Governance and Risk Management <i>Policy</i> | GRM-06.1 | Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)? | Hexnode's security and privacy visions are in alignment with the best of industry standards. |
| | GRM-06.2 | Do you have agreements to ensure your providers adhere to your information security and privacy policies? | All providers are contractually obliged with Hexnode to maintain security and privacy policies. |
| | GRM-06.3 | Can you provide evidence of due diligence mapping of your controls, architecture, and processes to | Hexnode maintains a complete security documentation which is reviewed and updated periodically. Interested |

| | | | |
|--|----------|---|--|
| | | regulations and/or standards? | customers can request for the document. |
| | GRM-06.4 | Do you disclose which controls, standards, certifications, and/or regulations you comply with? | These are disclosed within the documents. |
| Governance and Risk Management <i>Policy Enforcement</i> | GRM-07.1 | Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures? | Annual employee security meets are held to spread awareness over violation of security policies and procedures. Disciplinary actions resulting from violations are documented as policies and are made clear during employee training. |
| | GRM-07.2 | Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures? | |
| Governance and Risk Management <i>Business / Policy Change Impacts</i> | GRM-08.1 | Do risk assessment results include updates to security policies, procedures, standards, and | Yes, Hexnode conducts regular risk assessment tests and reviews existing risk management policies. |

| | | | |
|--|----------|---|--|
| | | controls to ensure they remain relevant and effective? | |
| Governance and Risk Management <i>Policy Reviews</i> | GRM-09.1 | Do you notify your tenants when you make material changes to your information security and/or privacy policies? | Our privacy and security policies are updated regularly and are made readily available on the company website. |
| | GRM-09.2 | Do you perform, at minimum, annual reviews to your privacy and security policies? | Privacy and security policies are reviewed and updated at least annually. |
| Governance and Risk Management <i>Assessments</i> | GRM-10.1 | 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? | Hexnode conducts risk analysis tests to ensure industry compliances that aligns with GDPR, HIPAA and other standards. Periodic internal and third-party audits are utilized to ensure full compliance. Hexnode conducts regular risk assessment tests and reviews |

| | | | |
|---|----------|--|---|
| | | | existing risk management policies. Risk assessment tests and risk management policies are well documented and made available to authorized personnel. |
| | GRM-10.2 | 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)? | Comprehensive risk management reports are formed and cataloged based on risk categories. |
| Governance and Risk Management Program | GRM-11.1 | Do you have a documented, organization-wide program in place to manage risk? | Documentation of the risk management program would be available to customers upon request. |
| | GRM-11.2 | Do you make available documentation of your organization-wide risk management program? | |
| Human Resources Asset Returns | HRS-01.1 | Are systems in place to monitor for privacy breaches and notify tenants | Yes, Hexnode has a system in place to monitor for privacy breaches and to |

| | | | |
|--|----------|--|--|
| | | expeditiously if a privacy event may have impacted their data? | automatically notify the customers. Customers can review their privacy policy from the Hexnode Privacy Policy page. |
| | HRS-01.2 | Is your Privacy Policy aligned with industry standards? | They are aligned with the industry standards. |
| Human Resources <i>Background Screening</i> | HRS-02.1 | Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification? | All employee candidates are subject to background checks and verification in accordance with the local law and company policy. The degree of background assessment varies with the authority that the employee will exercise. |
| Human Resources <i>Employment Agreements</i> | HRS-03.1 | Do you specifically train your employees regarding their specific role and the information security controls they must fulfill? | Hexnode provides employee training for all its new employees which include information about their role in the company and security controls they must fulfill. Internal wikis are maintained which house detailed documentations on roles |
| | HRS-03.2 | Do you document employee | |

| | | | |
|--|----------|---|---|
| | | acknowledgment of training they have completed? | and security aspects of the company. Yearly security conferences along with frequent employee training sessions and meets ensure that the employees stay updated on company policies. |
| | HRS-03.3 | Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information? | |
| | HRS-03.4 | Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems? | |
| | HRS-03.5 | Are personnel trained and provided with awareness programs at least once a year? | |

| | | | |
|--|----------|---|--|
| Human Resources <i>Employment Termination</i> | HRS-04.1 | Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? | Hexnode follows pre-approved and documented contractual policies to govern change in employment and/or termination. |
| | HRS-04.2 | Do the above procedures and guidelines account for timely revocation of access and return of assets? | Access privileges are directly based on employee roles and change based on change in roles. All access is revoked, and corporate assets retracted upon employee termination. |
| Human Resources <i>Portable / Mobile Devices</i> | HRS-05.1 | 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 | All devices in the corporate ecosystem are administered and managed by Hexnode's MDM software. MDM ensures device and data security over portable and non-portable devices. |

| | | | |
|--|----------|---|--|
| | | higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)? | |
| Human Resources <i>Non-Disclosure Agreements</i> | HRS-06.1 | 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? | All employees and personnel, who are in anyway associated with accessing confidential data, are contractually bound under NDA. These agreements are reviewed quarterly or earlier. |
| Human Resources <i>Roles / Responsibilities</i> | HRS-07.1 | Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? | Hexnode defines its administrative roles, restrictions and tenant roles in its Terms of Service . |
| Human Resources | HRS-08.1 | Do you provide documentation | Hexnode has defined and documented |

| | | | |
|---|----------|---|---|
| <i>Acceptable Use</i> | | regarding how you may access tenant data and metadata? | conditions of access and use of tenant data in its Terms of Service , Privacy Policy and EULA |
| | HRS-08.2 | Do you collect or create metadata about tenant data usage through inspection technologies (e.g., search engines, etc.)? | |
| | HRS-08.3 | Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies? | |
| Human Resources <i>Training / Awareness</i> | HRS-09.1 | 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, | Hexnode hosts annual security meets and knowledge sharing sessions which include employee awareness programs for cloud-related access and data management issues. |

| | | | |
|--|----------|--|---|
| | | and conflicts of interest) for all persons with access to tenant data? | |
| | HRS-09.2 | Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity? | |
| Human Resources <i>User Responsibility</i> | HRS-10.1 | Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements? | All Hexnode employees have access to internal documents that define employee responsibilities and security compliances in the organization. |
| | HRS-10.2 | Are users made aware of their responsibilities for maintaining a safe and secure working environment? | All employees follow industry standard security practices for maintaining a secure working environment. Tenant can review user |

| | | | |
|--|----------|---|---|
| | | | security policies from the Hexnode security document that is provided when requested. |
| | HRS-10.3 | Are users made aware of their responsibilities for leaving unattended equipment in a secure manner? | |
| Human Resources <i>Workspace</i> | HRS-11.1 | Do your data management policies and procedures address tenant and service level conflicts of interests? | Our data management policies consider all customer service level requirements. |
| | HRS-11.2 | Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data? | We have a strict access control policy in place to ensure only authorized personnel have access to tenant data. Employees who disregard the guidelines set within the policy will be subjected to disciplinary actions. |
| | HRS-11.3 | Does the virtual machine management infrastructure include a tamper audit or software integrity function to | Not applicable since virtual infrastructure is not used. |

| | | | |
|--|----------|--|--|
| | | detect changes to the build/configuration of the virtual machine? | |
| Identity & Access Management <i>Audit Tools Access</i> | IAM-01.1 | Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)? | Access to Hexnode management systems is limited to a small team of authorized personnel. Every key access is logged and monitored, for security. |
| | IAM-01.2 | Do you monitor and log privileged access (e.g., administrator level) to information security management systems? | All access to security management systems are logged and monitored through a centralized server. |
| Identity & Access Management <i>User Access Policy</i> | IAM-02.1 | Do you have controls in place ensuring timely removal of systems access that is no | Upon termination, the user will be removed from the company's directory server. All of the user's access will be automatically revoked. |

| | | | |
|---|----------|--|--|
| | | longer required for business purposes? | Details regarding the allocation and removal of access rights is detailed within our access control policy. |
| | IAM-02.2 | 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? | |
| Identity & Access Management <i>Diagnostic / Configuration Ports Access</i> | IAM-03.1 | Do you use dedicated secure networks to provide management access to your cloud service infrastructure? | Yes, multi factor authentication and various secure logon protocols are used. Access will only be granted with regards to our access control policy. |
| Identity & Access Management <i>Policies and Procedures</i> | IAM-04.1 | Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access? | Infrastructure and network access are cataloged based on authority. Apart from Hexnode's MDM platform, Hexnode also uses industry standard sensitive data access protocols which include storing the information of all personnel who access the network or IT infrastructure. |
| | IAM-04.2 | Do you manage and store the user identity of all personnel who have network access, | |

| | | | |
|--|----------|---|--|
| | | including their level of access? | |
| Identity & Access Management <i>Segregation of Duties</i> | IAM-05.1 | Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering? | Duties are segregated Hexnode role management system. |
| Identity & Access Management <i>Source Code Access Restriction</i> | IAM-06.1 | 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? | Access to sensitive data including software source code is restricted based on the authority of personnel. Management controls are in place to restrict un-authorized access. |
| | IAM-06.2 | Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to | Hexnode maintains a strict access control policy to ensure access is restricted to just the authorized personnel. |

| | | | |
|--|----------|---|---|
| | | authorized personnel only? | |
| Identity & Access Management <i>Third Party Access</i> | IAM-07.1 | Do you provide multi-failure disaster recovery capability? | All internal product infrastructures are protected based on risk analysis reports and contingency plans derived from internal audits. |
| | IAM-07.2 | Do you monitor service continuity with upstream providers in the event of provider failure? | Hexnode continuously monitors its cloud network infrastructure hosted in AWS. |
| | IAM-07.3 | Do you have more than one provider for each service you depend on? | At present, Hexnode relies on the services of just one cloud provider that is AWS. |
| | IAM-07.4 | Do you provide access to operational redundancy and continuity summaries, including the services you depend on? | No, Hexnode considers its operational details and associated services to be confidential. |

| | | | |
|---|----------|---|--|
| | IAM-07.5 | Do you provide the tenant the ability to declare a disaster? | A disaster can only be declared by authorized personnel and not the customer. |
| | IAM-07.6 | Do you provide a tenant-triggered failover option? | No, failover cannot be triggered by customers. |
| | IAM-07.7 | Do you share your business continuity and redundancy plans with your tenants? | Hexnode considers this information to be internal. |
| Identity & Access Management User Access Restriction / Authorization | IAM-08.1 | Do you document how you grant and approve access to tenant data? | Hexnode only authorizes access to tenant data with tenant approval, unless required by the law. Hexnode has well-defined documentation on handling tenant data in accordance with Hexnode Privacy Policy . |
| | IAM-08.2 | Do you have a method of aligning provider and tenant data classification methodologies for access control purposes? | |

| | | | |
|---|----------|---|--|
| Identity & Access Management <i>User Access Authorization</i> | IAM-09.1 | <p>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?</p> | <p>Tenant data will only be accessed with prior permission from the tenant, unless required by the law. No other entity, business body or individual has access to tenant data or internal systems, except authorized Hexnode personnel.</p> |
| | IAM-09.2 | <p>Do you provide upon request user access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical</p> | <p>Access to information or Hexnode internal systems will be granted, based on the nature of the request and level of authority of the requester.</p> |

| | | | |
|---|----------|---|---|
| | | and virtual) applications, infrastructure systems and network components? | |
| Identity & Access Management <i>User Access Reviews</i> | IAM-10.1 | Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)? | Yes, a periodic process is in place for reviewing access privileges. Apart from the above-mentioned periodic process, access is revoked after completion of contract period or any explicit reasons that call for the same. |
| | IAM-10.2 | If users are found to have inappropriate entitlements, are all remediation and certification actions recorded? | All remediation activities are recorded and documented as reports for internal |
| | IAM-10.3 | Will you share user entitlement remediation and certification reports with your tenants, if inappropriate | At Hexnode, tenant data is labeled as having the highest level of confidentiality. Any inappropriate access, once identified, are |

| | | | |
|--|----------|---|---|
| | | access may have been allowed to tenant data? | swiftly remediated for and recorded in our risk remediation and disaster management reports. Notifications are automatically sent to related tenant(s) on conformation of unauthorized access. |
| Identity & Access Management <i>User Access Revocation</i> | IAM-11.1 | Is timely deprovisioning, 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? | Third party application, software or business bodies, do not have access to tenant data, unless requested by the tenant or required by the law. Access privileges are directly based on employee roles and change based on change in roles. All access is revoked, and corporate assets retracted upon employee termination. |
| | IAM-11.2 | Is any change in user access status intended to include termination of | |

| | | | |
|---|----------|---|--|
| | | employment, contract or agreement, change of employment or transfer within the organization? | |
| Identity & Access Management <i>User ID Credentials</i> | IAM-12.1 | Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service? | Yes. |
| | IAM-12.2 | Do you use open standards to delegate authentication capabilities to your tenants? | <p>Single Sign-On is available for users of Hexnode portal. They can sign in using their Google, Microsoft and Okta credentials.</p> <p>SAML authentication is currently under development.</p> <p>Hexnode harbors a strong identity management system to ensure tenants are properly authenticated before they access</p> |
| | IAM-12.3 | Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/auth orizing users? | |
| | IAM-12.4 | Do you have a Policy Enforcement Point capability | |

| | | | |
|--|----------|--|---|
| | | (e.g., XACML) to enforce regional legal and policy constraints on user access? | Hexnode's resources. Customers can manage administrative control over the MDM console. End user privileges are defined by the administrators and assigned by the customer. |
| | IAM-12.5 | 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? | https://www.hexnode.com/mobile-device-management/help/configuring-custom-technician-roles-using-hexnode-mdm/ |
| | IAM-12.6 | Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access? | IAM features and integration with third-party identity assurance services are currently in development. |
| | IAM-12.7 | Do you allow tenants to use third-party identity assurance services? | |

| | | | |
|--|-----------|--|---|
| | IAM-12.8 | Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement? | |
| | IAM-12.9 | Do you allow tenants/customers to define password and account lockout policies for their accounts? | |
| | IAM-12.10 | Do you support the ability to force password changes upon first logon? | |
| | IAM-12.11 | 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)? | Hexnode has “Forgot Password” self-service mechanism in place to help customers retrace their login credential using their own email. |

| | | | |
|---|----------|--|--|
| | | | |
| Identity & Access Management <i>Utility Programs Access</i> | IAM-13.1 | Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored? | All attack management policies are in accordance with AWS security policies. For more information visit: https://aws.amazon.com/security/ |
| | IAM-13.2 | Do you have the capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)? | Not Applicable since virtual infrastructure is not used. |
| | IAM-13.3 | Are attacks that target the virtual infrastructure prevented with technical controls? | Not Applicable as virtual infrastructure is not used. |
| Infrastructure & Virtualization Security <i>Audit Logging / Intrusion Detection</i> | IVS-01.1 | Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, | Hexnode utilizes an IDS tool along with a feedback system for timely detection and responsive remediation to intrusions. |

| | | | |
|--|----------|---|--|
| | | investigation by root cause analysis, and response to incidents? | All logs are stored and made available in a centralized system which can only be accessed by authorized personnel. |
| | IVS-01.2 | Is physical and logical user access to audit logs restricted to authorized personnel? | |
| | IVS-01.3 | Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done? | |
| | IVS-01.4 | Are audit logs centrally stored and retained? | |
| | IVS-01.5 | Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)? | |

| | | | |
|---|----------|---|---|
| Infrastructure & Virtualization Security <i>Change Detection</i> | IVS-02.1 | Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)? | Not applicable as virtual infrastructure is not used. |
| | IVS-02.2 | 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)? | |
| Infrastructure & Virtualization Security <i>Clock Synchronization</i> | IVS-03.1 | Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? | Hexnode uses a standard time service to synchronize time reference throughout the system. |
| Infrastructure & | IVS-04.1 | Do you provide documentation | Excess memory, network bandwidth, storage etc. |

| | | | |
|---|----------|--|---|
| Virtualization Security <i>Capacity / Resource Planning</i> | | regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios? | are properly managed and monitored based on industry best practices. System oversubscriptions are documented but are available for internal reference only. |
| | IVS-04.2 | Do you restrict use of the memory oversubscription capabilities present in the hypervisor? | |
| | IVS-04.3 | Do your system capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants? | Hexnode's infrastructure was engineered to scale in a matter of minutes. |
| | IVS-04.4 | Is system performance monitored and tuned in order to continuously meet | Hexnode's infrastructure systems are regularly monitored and reviewed to ensure maximum efficiency of working |

| | | | |
|---|----------|--|--|
| | | regulatory, contractual, and business requirements for all the systems used to provide services to the tenants? | and maintain the highest level of security. |
| Infrastructure & Virtualization Security <i>Management - Vulnerability Management</i> | IVS-05.1 | Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)? | Not applicable as virtual infrastructure is not used. |
| Infrastructure & Virtualization Security <i>Network Security</i> | IVS-06.1 | For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution? | Hexnode does not provide an IaaS offering at present. |
| | IVS-06.2 | Do you regularly update network architecture | Hexnode maintains, regularly updated, documentation on the |

| | | | |
|--|----------|---|---|
| | | diagrams that include data flows between security domains/zones? | data flows within the Hexnode infrastructure system. |
| | IVS-06.3 | Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network? | Hexnode maintains minimal communications between security /zones within the network, based on our risk management policy. All communications within the network are filtered using a centrally managed firewall system. |
| | IVS-06.4 | Are all firewall access control lists documented with business justification? | Yes, Hexnode maintains a list of all firewall access control, and are periodically reviewed. |
| Infrastructure & Virtualization Security <i>OS Hardening and Base Controls</i> | IVS-07.1 | Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical | All unnecessary ports, protocols and services are disabled by default. |

| | | | |
|--|----------|--|--|
| | | controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template? | |
| Infrastructure & Virtualization Security <i>Production / Non-Production Environments</i> | IVS-08.1 | For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes? | No, Hexnode does not currently provide a separate test environment for tenants. Separate environment for test and production processes exists but they are not available for tenants. New updates and fixes will be documented in our release notes. |
| | IVS-08.2 | For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments? | Hexnode does not provide an IaaS offering at present. |
| | IVS-08.3 | Do you logically and physically segregate | Development and QA are run on a non- |

| | | | |
|--|----------|--|--|
| | | production and non-production environments? | production environment that utilize separate equipment to ensure physical and logical segregation. |
| Infrastructure & Virtualization Security Segmentation | IVS-09.1 | Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements? | Yes, system and network environments are protected by a centrally managed logical firewall. |
| | IVS-09.2 | Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory, and contractual requirements? | |
| | IVS-09.3 | Are system and network environments protected by a | |

| | | | |
|---|----------|---|--|
| | | firewall or virtual firewall to ensure separation of production and non-production environments? | |
| | IVS-09.4 | Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data? | |
| Infrastructure & Virtualization Security <i>VM Security - Data Protection</i> | IVS-10.1 | Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers? | Not applicable since virtual infrastructure is not used. |
| | IVS-10.2 | Do you use a network segregated from production-level networks when migrating physical servers, | Not applicable since virtual infrastructure is not used. |

| | | | |
|---|----------|--|---|
| | | applications, or data to virtual servers? | |
| Infrastructure & Virtualization Security <i>VMM Security - Hypervisor Hardening</i> | IVS-11.1 | 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)? | Hexnode utilizes the principle of least privilege to minimize sensitive data access to a handful of authorized personnel. All personnel access is logged and monitored. |
| Infrastructure & Virtualization Security | IVS-12.1 | Are policies and procedures established and mechanisms configured and | All corporate devices are connected to a pre-configured Wi-Fi network using certificates allotted to |

| | | | |
|--------------------------|----------|---|---|
| <i>Wireless Security</i> | | implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic? | the user. All corporate networks are encrypted using WPA2 enterprise. Wi-Fi networks are constantly monitored to detect and isolate unauthorized users. |
| | IVS-12.2 | 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)? | |
| | IVS-12.3 | 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? | |
| Infrastructure & Virtualization Security <i>Network Architecture</i> | IVS-13.1 | Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts? | Hexnode maintains network architecture which outlines data flows between different network zones, both internal and external, and also highlights critical environments and data flows that may have legal compliance impacts. |
| | IVS-13.2 | 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 | Hexnode utilizes spam detection tools, IP blacklisting, centralized malware detection systems and firewall rules that deny access by default. Hexnode uses industry standard methods to utilize and manage excess |

| | | | |
|--|----------|--|--|
| | | 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? | bandwidth resulting in DDoS mitigation. DDoS mitigation is also achieved by making use of AWS services. For more information visit: https://aws.amazon.com/security/ |
| Interoperability & Portability APIs | IPY-01.1 | Do you publish a list of all APIs available in the service and indicate which are standard and which are customized? | Customers can access detailed documentation on the Hexnode API from: https://www.hexnode.com/mobile-device-management/api/ |
| Interoperability & Portability Data Request | IPY-02.1 | Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)? | Hexnode provides detailed and cataloged reports on end-user, from its management console. Reports can be exported as CSV and PDF. |
| Interoperability & Portability Policy & Legal | IPY-03.1 | Do you provide policies and procedures (i.e. service level | Customers can access detailed documentation on the Hexnode API from: |

| | | | |
|--|----------|--|---|
| | | agreements) governing the use of APIs for interoperability between your service and third-party applications? | https://www.hexnode.com/mobile-device-management/api/ |
| | IPY-03.2 | Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service? | <p>Customers have complete control over their data and data migration policies. Customer data management is in accordance with the Privacy Policy and compliant with GDPR standards.</p> <p>Customers can read the service level agreement from Hexnode's website https://www.hexnode.com/saas-terms/</p> |
| Interoperability & Portability <i>Standardized Network Protocols</i> | IPY-04.1 | Can data import, data export, and service management be conducted over secure (e.g., non-clear text and | All data import, export and communication are encrypted with industry best standards for maximum TLS. |

| | | | |
|--|----------|---|---|
| | | authenticated), industry accepted standardized network protocols? | |
| | IPY-04.2 | Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved? | <p>There is documented information on the use of Hexnode's APIs. This is available on Hexnode's website as well as the Hexnode Help Center.</p> <p>https://www.hexnode.com/mobile-device-management/hexnode-mdm-api/</p> <p>https://www.hexnode.com/mobile-device-management/api/#</p> |
| Interoperability & Portability <i>Virtualization</i> | IPY-05.1 | Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability? | Not applicable since virtual infrastructure is not used. |

| | | | |
|---|----------|--|--|
| | IPY-05.2 | Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review? | Not applicable since virtual infrastructure is not used. |
| Mobile Security <i>Anti-Malware</i> | MOS-01.1 | Do you provide anti-malware training specific to mobile devices as part of your information security awareness training? | Hexnode host's an annual security meet where employees are made aware of security concerns and industry best security practices. Security of mobile devices are discussed, and related software are made available for the employee. |
| Mobile Security <i>Application Stores</i> | MOS-02.1 | Do you document and make available lists of approved application stores for mobile devices accessing or storing company data | Hexnode uses its own Mobile Device Management (MDM) console to secure all corporate and BYOD devices in the enterprise. In its BYOD |

| | | | |
|---|-----------|--|--|
| | | and/or company systems? | policy, Hexnode clearly defines the hardware, software and security requirements that |
| Mobile Security <i>Approved Applications</i> | MOS -03.1 | Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device? | qualify a device to be used in the enterprise. Devices that do not meet the requirements are marked non-compliant on the Hexnode dashboard and are isolated. Hexnode maintains a complete inventory of all managed devices along with comprehensive device details, including |
| Mobile Security <i>Approved Software for BYOD</i> | MOS -04.1 | Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices? | OS version, device model and device status. Wi-Fi, corporate email, VPNs and cloud-based storage are pre-configured on every corporate device on deployment. BYOD |
| Mobile Security <i>Awareness and Training</i> | MOS -05.1 | Do you have a documented mobile device policy in your employee training that clearly defines mobile | devices are not allowed access to company storage and production systems. |

| | | | |
|---|-----------|--|---|
| | | devices and the accepted usage and requirements for mobile devices? | <p>Hexnode defines a corporate app store that house's every application required by the end-user and deemed secure by the enterprise.</p> <p>Hexnode also has whitelisting/blacklisting policies in place to ensure only secure applications are installed on every managed device.</p> |
| Mobile Security <i>Cloud Based Services</i> | MOS -06.1 | Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device? | |
| Mobile Security <i>Compatibility</i> | MOS -07.1 | Do you have a documented application validation process for testing device, operating system, and application compatibility issues? | |
| Mobile Security <i>Device Eligibility</i> | MOS -08.1 | Do you have a BYOD policy that defines the device(s) and eligibility requirements | |

| | | | |
|--|-----------|--|---|
| | | allowed for BYOD usage? | |
| Mobile Security <i>Device Inventory</i> | MOS -09.1 | Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)? | |
| Mobile Security <i>Device Management</i> | MOS -10.1 | Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data? | |
| Mobile Security <i>Encryption</i> | MOS -11.1 | Does your mobile device policy require the use of encryption for either the entire device or for data identified as | Hexnode's Mobile Device Management policies defines device level encryptions to be mandatory on all devices. Devices found non-compliant with the |

| | | | |
|---|-----------|---|---|
| | | sensitive enforceable through technology controls for all mobile devices? | policy will be encrypted remotely from the MDM portal. |
| Mobile Security <i>Jailbreaking and Rooting</i> | MOS -12.1 | Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)? | Hexnode deems devices that are jailbroken or rooted to be exposed to security threats and unsecure to be used in the enterprise. Above devices are marked as non-compliant on the Hexnode MDM dashboard and |
| | MOS -12.2 | Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls? | remediated for, by the management team. |
| Mobile Security <i>Legal</i> | MOS -13.1 | Does your BYOD policy clearly define the expectation of privacy, | All BYOD policies defining security and legal compliance are documented and made |

| | | | |
|--|-----------|---|---|
| | | requirements for litigation, e-discovery, and legal holds? | available to the employee through an internal wiki. |
| | MOS -13.2 | Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls? | Hexnode deems devices that are jailbroken or rooted to be exposed to security threats and unsecure to be used in the enterprise. Above devices are marked as non-compliant on the Hexnode MDM dashboard and remediated for, by the management team. |
| Mobile Security <i>Lockout Screen</i> | MOS -14.1 | Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices? | All employee devices are locked, after a pre-defined period of inactivity. The administrator defines the period of inactivity from a centrally managed system. |
| Mobile Security <i>Operating Systems</i> | MOS -15.1 | Do you manage all changes to mobile device operating systems, patch | Changes to the corporate device operating systems and application versions are |

| | | | |
|--|-----------|--|---|
| | | levels, and applications via your company's change management processes? | managed directly from the management console. |
| Mobile Security <i>Passwords</i> | MOS -16.1 | Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices? | Hexnode has defined password policies that define password complexity, length, period of renewal and the history of usage. Password policies are enforced onto every corporate device from the MDM console. |
| | MOS -16.2 | Are your password policies enforced through technical controls (i.e. MDM)? | |
| | MOS -16.3 | Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device? | |
| Mobile Security <i>Policy</i> | MOS -17.1 | Do you have a policy that requires BYOD users to | All BYOD devices are containerized, which effectively separates |

| | | | |
|--|-----------|---|--|
| | | perform backups of specified corporate data? | work data from employee personal data. Restrictions are enforced on the container without effecting employee personal data. |
| | MOS -17.2 | Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores? | Containerization also prevents employee applications or services from interacting with data in the container. |
| | MOS -17.3 | Do you have a policy that requires BYOD users to use anti-malware software (where supported)? | The enterprise can also corporate wipe the BYOD devices, which will remove corporate data stored in the container, leaving personal data intact. |
| Mobile Security <i>Remote Wipe</i> | MOS -18.1 | Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices? | |
| | MOS -18.2 | Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices? | Corporate devices that are non-compliant or no longer in active service can be remotely wiped. |

| | | | |
|---|-----------|---|---|
| Mobile Security <i>Security Patches</i> | MOS -19.1 | Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier? | Latest available OS and system updates are enforced on managed devices. |
| | MOS -19.2 | Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel? | |
| Mobile Security <i>Users</i> | MOS -20.1 | Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device? | BYOD devices are by-default denied access to Hexnode systems and servers. |
| | MOS -20.2 | Does your BYOD policy specify the user roles that are allowed access via a | |

| | | | |
|---|----------|---|---|
| | | BYOD-enabled device? | |
| Security Incident Management, E-Discovery, & Cloud Forensics <i>Contact / Authority Maintenance</i> | SEF-01.1 | Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations? | Hexnode maintains a liaison with regulatory authorities for risk and disaster management. |
| Security Incident Management, E-Discovery, & Cloud Forensics <i>Incident Management</i> | SEF-02.1 | Do you have a documented security incident response plan? | Hexnode has devised a set of procedures to be executed in response to an incident which may, or may not, result in compromise of customer, or other sensitive, information that can cause direct or indirect consequences to the customer or the company. |
| | SEF-02.2 | Do you integrate customized tenant requirements into your security incident response plans? | Hexnode's incident response plans are based on industry best practices and reviewed by experts. |

| | | | |
|--|----------|--|---|
| | | | |
| | SEF-02.3 | Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents? | Terms of Service and SaaS Terms specify roles and responsibilities. |
| | SEF-02.4 | Have you tested your security incident response plans in the last year? | Hexnode incident response plans are reviewed at least annually. |
| Security Incident Management, E-Discovery, & Cloud Forensics <i>Incident Reporting</i> | SEF-03.1 | Does your security information and event management (SIEM) system merge data sources (e.g., app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting? | Hexnode SIEM does merge data sources. |
| | SEF-03.2 | Does your logging and monitoring framework allow isolation of an | Yes, Hexnode's incident management system indexes incident to the customer. |

| | | | |
|---|----------|---|--|
| | | incident to specific tenants? | |
| Security Incident Management, E-Discovery, & Cloud Forensics <i>Incident Response Legal Preparation</i> | SEF-04.1 | Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls? | Hexnode has an incident management system in place that specify and comply with industry standards. |
| | SEF-04.2 | Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques? | |
| | SEF-04.3 | 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? | Yes, Hexnode can provide data from a single customer at any point of time, without freezing other tenant data. |

| | | | |
|---|----------|--|---|
| | SEF-04.4 | Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas? | Hexnode can separate and produce data of a single tenant, if required by the law. |
| Security Incident Management, E-Discovery, & Cloud Forensics <i>Incident Response Metrics</i> | SEF-05.1 | Do you monitor and quantify the types, volumes, and impacts on all information security incidents? | Hexnode continuously monitors and reviews risk assessment policies based on its incident response plan. |
| | SEF-05.2 | Will you share statistical information for security incident data with your tenants upon request? | All information regarding the incident response system is considered confidential. |
| Supply Chain Management, Transparency, and Accountability <i>Data Quality and Integrity</i> | STA-01.1 | Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them? | Not applicable since the development is not outsourced. |

| | | | |
|--|----------|--|--|
| | | | |
| | STA-01.2 | 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? | Customer data can only be accessed by Hexnode employees and on a least privilege principle. |
| Supply Chain Management, Transparency, and Accountability <i>Incident Reporting</i> | STA-02.1 | Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals)? | In the unlikely event of occurrence of a security incident, all affected customers are notified automatically. |
| Supply Chain Management, Transparency, and Accountability <i>Network / Infrastructure Services</i> | STA-03.1 | Do you collect capacity and use data for all relevant components of your cloud service offering? | Hexnode collects capacity and use data for performance analyzes. |

| | | | |
|--|----------|--|---|
| | STA-03.2 | Do you provide tenants with capacity planning and use reports? | Hexnode does not currently share capacity planning and use data. |
| Supply Chain Management, Transparency, and Accountability <i>Provider Internal Assessments</i> | STA-04.1 | Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics? | Hexnode performs audits and reviews for analyzing the effectiveness of current policies, procedures and supporting measures, at least annually. |
| Supply Chain Management, Transparency, and Accountability <i>Third Party Agreements</i> | STA-05.1 | Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted? | Third party vendors are contractually inclined to be compliant with Hexnode security standards and to follow laws in the country where data is being handled. All third-party agreements are reviewed by a legal counsel. |
| | STA-05.2 | Do you select and monitor outsourced providers in compliance with laws in the country where the data originates? | |

| | | | |
|--|----------|--|---|
| | STA-05.3 | Does legal counsel review all third-party agreements? | |
| | STA-05.4 | Do third-party agreements include provision for the security and protection of information and assets? | |
| | STA-05.5 | Do you provide the client with a list and copies of all subprocessing agreements and keep this updated? | |
| Supply Chain Management, Transparency, and Accountability <i>Supply Chain Governance Reviews</i> | STA-06.1 | Do you review the risk management and governed processes of partners to account for risks inherited from other members of that partner's supply chain? | Hexnode monitors risk management and vulnerability reports of partners regularly. |
| Supply Chain Management, Transparency, | STA-07.1 | Are policies and procedures established, and | SLAs are made available on request. Hexnode has clearly defined Terms of |

| | | | |
|--|----------|---|---|
| and Accountability Supply Chain Metrics | | supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)? | Service, which is made publicly available. Hexnode has a formal process to measure and address non-conformance of provisions and/or terms across the entire supply chain. |
| | STA-07.2 | Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)? | |
| | STA-07.3 | Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships? | Hexnode continuously monitors for service level inconsistencies and supplier performance. |
| | STA-07.4 | Do you review all agreements, | Hexnode legal team reviews all agreements, |

| | | | |
|---|----------|--|--|
| | | policies, and processes at least annually? | policies and processes at least annually. |
| Supply Chain Management, Transparency, and Accountability Third Party Assessment | STA-08.1 | Do you assure reasonable information security across your information supply chain by performing an annual review? | Hexnode reviews and audits are conducted at least annually and include all third-party associates linked with Hexnode. |
| | STA-08.2 | Does your annual review include all partners/third-party providers upon which your information supply chain depends? | |
| Supply Chain Management, Transparency, and Accountability <i>Third Party Audits</i> | STA-09.1 | Do you permit tenants to perform independent vulnerability assessments? | Customers can request to run tests on their own cloud instance as long as it doesn't affect other customers and is in accordance with Hexnode policies. Customers can only run tests post confirmation from Hexnode. |

| | | | |
|---|----------|---|---|
| | STA-09.2 | Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks? | All penetration tests and vulnerability scans are done by the security team. |
| Threat and Vulnerability Management <i>Antivirus / Malicious Software</i> | TVM-01.1 | Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems? | Hexnode maintains a centrally managed malware detection and antivirus system. |
| | TVM-01.2 | 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? | |
| Threat and Vulnerability Management | TVM-02.1 | Do you conduct network-layer vulnerability scans | Hexnode's risk management policy mandates regularly |

| | | | |
|----------------------------------|-----------|---|--|
| Vulnerability / Patch Management | | regularly as prescribed by industry best practices? | vulnerability scans. Hexnode has in place an effective feedback system which assists in robust remediation post vulnerability detection. Hexnode considers all information relating to vulnerability scans to be confidential. |
| | TVM -02.2 | Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices? | |
| | TVM -02.3 | Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices? | |
| | TVM -02.4 | Will you make the results of vulnerability scans available to tenants at their request? | |
| | TVM -02.5 | Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, | |

| | | | |
|--|----------|---|--|
| | | applications, and systems? | |
| | TVM-02.6 | Will you provide your risk-based systems patching time frames to your tenants upon request? | |
| Threat and Vulnerability Management <i>Mobile Code</i> | TVM-03.1 | 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? | <p>Prior to development, the team shall be made aware of the security requirements, a policy on secure development will be made known to the team as well. The mobile code shall always be authorized and its code configuration checked before it is installed and used.</p> <p>Our security team will have an adequate number of technical and operational controls in place to ensure unauthorized mobile code is prevented from executing.</p> |
| | TVM-03.2 | Is all unauthorized mobile code prevented from executing? | |