HCL Software

STATEMENT OF APPLICABILITY

ISO 27001:2022 INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS)
HCL SOFTWARE PRODUCTS

Version: 4.0, December 2024
Classification : HCL Public
Approved by : Associate Director of Compliance, HCL Software

Clause Number	Control Description	Implemented?	Implemented Internally or Externally?	Implemented Controls	Comment / Justification for Exclusion
A.5	**ORGANIZATIONAL CONTROLS**				
A.5.1	**Policies for Information Security** Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Yes	Internal HCL	HCL Software Information Security Management System	HCL Software security programs is established through formal documented requirements that include HCL Software Security Policies, HCL Privacy Statement, HCL Corporate policies and Code of Business Ethics and Conduct and ensured its reviewed on a defined basis.
A.5.2	**Information Security roles and responsibilities** Information security roles and responsibilities shall be defined and allocated according to the organization needs.	Yes	Internal HCL	HCL Software follows Instruction that requires roles and responsibilities and Separation of Duties across multiple policies	HCL Software has roles and responsibilities defined, delegations of duty and restrictions on access throughout its policies.
A.5.3	**Segregation of duties** Conflicting duties and conflicting areas of responsibility shall be segregated.	Yes	Internal HCL	HCL Software operate permissions systems, least needs access throughout its policies to ensure separation of duties	HCL Software follows Instruction that requires Separation of Duties by ensuring that no one individual has two or more responsibilities or accesses that would allow them to misuse or divert company assets. Product teams are responsible for ensuring adequate Separation of Duties exists within its organization.
A.5.4	**Management Responsibilities** Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization..	Yes	Internal HCL	HCL Software Information Security Management System, Human Resource Practices and Code of Business Ethics and Conduct	All HCL Software managers ensure that their employees adhere to HCL Software Security requirements for the data and IT resources within their area of responsibility. Managers are also responsible to deny requests for unnecessary access to resources and to remove access to resources when they are no longer needed by employees.
A.5.5	**Contact with authorities** The organization shall establish and maintain contact with relevant authorities.	Yes	Internal HCL	HCL Software Information Security Management System and its Incident Management policy	Contact with authorities is managed by the HCL Tech Crisis Management team.
A.5.6	**Contact with special interest groups** The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Yes	Internal HCL	Various Policies & Products relate to areas of special interest	HCL SW Security & Compliance team maintain contact with special interest groups through a variety of means including by subscribing to newsletters HCL Products and Platform Specific teams are responsible for maintaining contact with special interests that maybe relevant to their specific product/platform/domain, as needed.
A.5.7	**Threat Intelligence** Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Yes	Internal HCL	Security Monitoring and Logging Policy	HCL Software utilizes Threat Intelligence and Advisory Reports which provide detailed information about current and potential future cyberattacks and a deeper understanding of threats by gathering, analyzing, and contextualizing data.
A.5.8	**Information Security in Project Management** Information security shall be integrated into project management.	Yes	Internal HCL	HCL Software Secure Engineering Practices governed by our Development and Maintenance policies and Release Management Practices HCL Software ISMS - System Acquisition, Development and Maintenance policy	All information security requirements are included at the time of acquisition, development and maintenance of systems and products. Secure Engineering Practices provides guidelines on Project Planning for Security Practice Area. All released product must comply with specific enhanced security requirements prior to release.
A.5.9	**Inventory of Information and other Associated Assets** An inventory of information and other associated assets, including owners, shall be developed and maintained.	Yes	Internal HCL	HCL Software ISMS - Asset Management policy, tooling to support management of the inventory	HCL Software ISMS - Asset Management policy requires identifying and maintaining and Asset Inventory. Each asset maintained in the inventory shall have an identified owner with applicable details pertaining to data classification.
A.5.10	**Acceptable use of Information and other Associated Assets** Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	Yes	Internal HCL	HCL Software ISMS - Asset Management policy, Code of Business Ethics and Conduct	HCL Software maintains acceptable use criteria within HCL Software ISMS - Asset Management policy. Additionally, it's Code of Business Ethics and Conduct defines the HCL code of conduct and addresses the issues of, but is not limited to, (1) rules for fair and appropriate dealings with our customers, competitors, the general public and fellow HCL staff; (2) acquisition and handling of information about others or owned by others and receiving information that may be confidential or has restrictions on its use; (3) rules regarding protection of customer-owned data, i.e., that all customer-owned data should be protected (4) rules for secure processing, storage, transmission, declassification and destruction also considering Information Classification and labelling
A.5.11	**Return of Assets** Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Yes	Internal HCL	HCL Human Resource practices HR Separation practice	HCL HR has processes and procedures which address return of assets from terminated employees.
A.5.12	**Classifications of Information** Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.	Yes	Internal HCL	HCL Software ISMS - Asset Management policy, HCL Data Classification Policy	Information shall be classified in terms of our Information and Data Classification policies.
A.5.13	**Labelling of Information** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes	Internal HCL	HCL Software ISMS - Asset Management policy	Information shall be labelled based on classification in terms of our Information and Data Classification policies.
A.5.14	**Information Transfer** Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	Yes	Internal HCL	HCL Software ISMS - Human Resources, Cryptography, Supplier Management, HCL Code of Business Ethics and Conduct, and HCL corporate email standards	HCL Software employees shall neither receive from nor disclose to any other party any Confidential Information (as per our Code of Business Ethics and Conduct) without following procedures. All data in transit is encrypted for protections. HCL Software supplier agreements include security controls on data transfer. Information is never shared without a Non Disclosure agreement in place. Based on information classification, private/confidential information is not disclosed to unauthorized individuals during electronic transmission.
A.5.15	**Access Control** Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	Yes	Internal HCL	HCL Software ISMS - Access Controls policy	HCL Software Access Control policy requires access controls have elements of need to know basis, least privilege and management support included in Identification, Authorization, System and security administrative authority, Access authorization, and Application security administrative authority requirements.
A.5.16	**Identity Management** The full life cycle of identities shall be managed.	Yes	Internal HCL	HCL Software ISMS - Access Controls policy	User registration and de-registration standards are defined in HCL Software Access Control policy. The controls include Information Owner approvals, specific requirements and time frames.
A.5.17	**Authentication Information** Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	Yes	Internal HCL	HCL Software ISMS - Access Controls policy	HCL Software ISMS - Access Controls policy contains details for management of secret authentication details including the mechanisms for protecting password information and a process for creating strong passwords. HCL Software requires mechanisms for protecting password information when in use or being renewed as defined in HCL Software Access Control policy.
A.5.18	**Access Rights** Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	Yes	Internal HCL	HCL Software ISMS - Access Controls policy, HCL Human Resource practices, HR Separation practice	Requirements and management of privileged access controls are defined in HCL Software Access Control policy. Regular reviews by management of user access consists of Employee verification, Continued business need, Privileged access review as defined in the HCL Software Access Control policy. HCL Software Access Control policy includes policy for revoking userids and for employment termination, verification and continued business need.
A.5.19	**Information Security in Supplier Relationships** Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Yes	Internal HCL	HCL Software ISMS - Supplier Management	Security requirements for the Supplier's are managed as part of any supplier agreement. HCL will expect as a minimum to match all security requirements and standards as defined by the HCL Software ISMS
A.5.20	**Addressing Information Security within Supplier Agreements** Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	Yes	Internal HCL	HCL Software ISMS - Supplier Management	Security requirements for the Supplier's are managed as part of any supplier agreement. HCL will expect as a minimum to match all security requirements and standards as defined by the HCL Software ISMS
A.5.21	**Managing Information Security in the Information and Communication Technology (ICT) Supply-Chain** Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Yes	Internal HCL	HCL Software ISMS - Supplier Management	Security requirements for the Supplier's are managed as part of any supplier agreement. HCL will expect as a minimum to match all security requirements and standards as defined by the HCL Software ISMS
A.5.22	**Monitoring, Review and Change Management of Supplier Services** The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Yes	Internal HCL	HCL Software ISMS - Supplier Management	Performance Monitoring for Supplier's are managed as part of any supplier agreement. HCL will expect as a minimum to perform to a standards as defined by the HCL Software ISMS Security requirements for the Supplier's are managed as part of any supplier agreement. HCL will expect as a minimum to match all security requirements and standards as defined by the HCL Software ISMS
A.5.23	**Information Security for use of Cloud Services** Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	Yes	Internal HCL	Cloud Infrastructure Security Standard	HCL Software ensures applicable parameters are defined in Cloud services agreement. Also ensures Integration of Cloud Security Posture Management and Cloud Workload Protection Tools (CSPM/CWPP) standard tools to monitor and protect any cloud environment in real time.

A.5.24	**Information Security Incident Management Planning and Preparation** The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Yes	Internal HCL	HCL Software ISMS - Information Security Incident Management	HCL Software has a dedicated Incident Response team that focuses on various scenarios. HCL Software's Incident Response team includes a group that has a data incident response process which supports all of HCL Software operations 24x7x365 worldwide.
A.5.25	**Assessment and Decision on Information Security Events** The organization shall assess information security events and decide if they are to be categorized as information security incidents.	Yes	Internal HCL	HCL Software ISMS - Information Security Incident Management	HCL Software has a dedicated Incident Response team that focuses on various scenarios. HCL Software's Incident Response team includes a group that has a data incident response process which supports all of HCL Software operations 24x7x365 worldwide.
A.5.26	**Response to Information Security Incidents** Information security incidents shall be responded to in accordance with the documented procedures.	Yes	Internal HCL	HCL Software ISMS - Information Security Incident Management	HCL Software has a dedicated Incident Response team that focuses on various scenarios. HCL Software's Incident Response team includes a group that has a data incident response process which supports all of HCL Software operations 24x7x365 worldwide.
A.5.27	**Learning from Information Security Incidents** Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	Yes	Internal HCL	HCL Software ISMS - Information Security Incident Management	HCL Software perform incident analysis to learn from information security incidents and drive continued improvement
A.5.28	**Collection of Evidence** The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Yes	Internal HCL	HCL Software ISMS - Information Security Incident Management	HCL Software has a dedicated Incident Response team that focuses on various scenarios and including the collection of evidence. HCL Software's Incident Response team includes a group that has a data incident response process which supports all of HCL Software operations 24x7x365 worldwide.
A.5.29	**Information Security during Disruption** The organization shall plan how to maintain information security at an appropriate level during disruption.	Yes	Internal HCL	HCL Software ISMS - Information Security Aspects of Business Continuity	HCL Software have a formal approach to planning for information security continuity through its comprehensive Business Continuity Management and Planning Program.
A.5.30	**ICT readiness for Business Continuity** ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Yes	Internal HCL	HCL Software ISMS - Information Security Aspects of Business Continuity	HCL Software ICT readiness has been planned, implemented, maintained and tested based on business continuity objectives and recovery requirements.
A.5.31	**Legal, Statutory, Regulatory and Contractual Requirements** Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	Yes	Internal HCL	Corporate Instructions: HCL legal & Regulatory HCL Software ISMS - Cryptography.	Corporate instructions mandate management of these processes via the Regulatory team. Legal provides all guidance on legal and contractual requirements. A cryptography policy is on the use, protection and lifetime of cryptographic keys has be developed and implemented through their whole lifecycle.
A.5.32	**Intellectual Property Rights** The organization shall implement appropriate procedures to protect intellectual property rights.	Yes	Internal HCL	HCL Software - Release Management, Certificate of Originality	Corporate Instructions on Intellectual Property include Rights to Intellectual Property, Invention protection, Receipt and Disclosure of confidential information, Patents and Inventions, Product and services reviews, copying of published materials, examination of non-HCL software.
A.5.33	**Protection of Records** Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Yes	Internal HCL	HCL Software Information Security Management System (tools), HCL Software ISMS - Access Controls, HCL Human Resource Practices and Code of Business Ethics and Conduct	Tooling used in support of the HCL Software ISMS is access controlled and designed to protect all records / data. All employees contracts include details regarding Confidential Information, Intellectual Property, and Other Matter
A.5.34	**Privacy and Protection of Personally Identifiable Information (PII)** The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Yes	Internal HCL	HCL Corporate - Privacy Statement	HCL Software Privacy and protection of personally identifiable controls are defined in our Privacy Statement supported by our classification and control of information
A.5.35	**Independent Review of Information Security** The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	Yes	Internal HCL	HCL Software ISMS - Internal Audit and Compliance	HCL Software Internal Audit program and external independent auditors perform independent reviews of information security implementation and compliance.
A.5.36	**Compliance with Policies, Rules and Standards for Information Security** Compliance with the organization's information security policy, topic- specific policies, rules and standards shall be regularly reviewed.	Yes	Internal HCL	HCL Software ISMS - Internal Audit and Compliance and all ISMS Operational Security activities	HCL Software Management is responsible for ensuring compliance with the policies and procedures and reviewing the compliance within their products. Security operational monitoring is conducted on an ongoing basis
A.5.37	**Documented Operating Procedures** Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Yes	Internal HCL	HCL Software ISMS - Operational Security	HCL Software security practices are established through formal documented requirements for operational security activities
A.6	**PEOPLE CONTROLS**				
A.6.1	**Screening** Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Yes	Internal HCL	HCL Human Resource practices	HCL performs background checks on all new employees through HCL Recruitment practices
A.6.2	**Terms and Conditions of Employment** The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	Yes	Internal HCL	HCL Software Information Security Management System, Human Resource Practices and Code of Business Ethics and Conduct	Employees are required to enter into confidentiality agreements and adhere to the HCL Code of Business Ethics and Conduct
A.6.3	**Information security awareness, education and training** The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	Yes	Internal HCL	Mandatory Information Security Annual Training, Code of Business Ethics and Conduct and various Security Policies	Employees are required to complete information security training annually. Progress is communicated to managers via automated emails/tools/reports and tracked to completion.
A.6.4	**Disciplinary Process** A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Yes	Internal HCL	HCL Software Information Security Management System, Human Resource Practices and Code of Business Ethics and Conduct	Employees must at all times comply with Code of Business Ethics and Conduct related guidelines. Violation of any HCL guideline is cause for discipline including dismissal from the company, as stated in the Code of Business Ethics and Conduct.
A.6.5	**Responsibilities after Termination or Change of Employment** Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	Yes	Internal HCL	HCL Software Information Security Management System, HR Separation practice	All HCL Software managers shall ensure appropriate removal or modification of access for employee termination or change of employment responsibility. Managers are also responsible to remove access to resources when they are no longer needed by employees. Employment Verification must be in place for annual employment verification of individuals assigned a userid on internal HCL Software systems.
A.6.6	**Confidentiality or Non-Disclosure Agreements** Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Yes	Internal HCL	HCL Software ISMS - Supplier Management, HCL Software ISMS - Human Resources, HCL Code of Business Ethics and Conduct and HCL Software ISMS - Cryptography	HCL Software supplier agreements include security controls on data transfer. Information is never shared without a Non Disclosure agreement in place. This approach is supported by our HR and Code of Business Ethics and Conduct policies
A.6.7	**Remote Working** Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Yes	Internal HCL	HCL Software Security and Standards for all Employees includes security measures for teleworking / remote working	HCL Software Security and Standards for all Employees includes security measures for teleworking / remote working
A.6.8	**Information Security Event Reporting** The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Yes	Internal HCL	HCL Software ISMS - Information Security Incident Management and Information Security Training	For security Incidents that may occur, product teams work with HCL Software's Incident Response team and HCL Legal to address incidents involving loss or exposure of PI Data. HCL Software's Incident Response team includes a group that has a data incident response process which supports all of HCL operations 24x7x365 worldwide.
A.7	**PHYSICAL CONTROLS**				
A.7.1	**Physical Security Perimeter** Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Yes	Internal HCL (if HCL hosted) External Party (if 3rd party hosted)	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes perimeter security for HCL data centers. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.7.2	**Physical Entry** Secure areas shall be protected by appropriate entry controls and access points.	Yes	Internal HCL (if HCL hosted) External Party (if 3rd party hosted)	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes entry, Delivery/Loading area control security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.

A.7.3	**Securing Offices, Rooms and Facilities** Physical security for offices, rooms and facilities shall be designed and implemented.	Yes	Internal HCL (if HCL hosted) External Party (if 3rd party hosted)	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes entry control security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.7.4	**Physical Security Monitoring** Premises shall be continuously monitored for unauthorized physical access.	Yes	Internal HCL (if HCL hosted) External Party (if 3rd party hosted)	Physical Access Standard Physical and Environmental Security	HCL Software Facilities are ensured to be suitably alarmed, monitored, and support intruder detection to information processing areas including protection from environmental threats.
A.7.5	**Protecting against External and Environmental Threats** Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Yes	Internal HCL (if HCL hosted) External Party (if 3rd party hosted)	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes external and environmental security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.7.6	**Working in Secure Areas** Security measures for working in secure areas shall be designed and implemented.	Yes	Internal HCL (if HCL hosted) External Party (if 3rd party hosted)	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes policy for working in secure areas for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.7.7	**Clear Desk and Clear Screen Policy** Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	Yes	Internal HCL (if HCL hosted) External Party (if 3rd party hosted)	HCL Software ISMS - Human Resources	HCL Software Human Resource policy describes clean desk and clear screen security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.7.8	**Equipment Siting and Protection** Equipment shall be sited securely and protected.	Yes	Internal HCL (if HCL hosted) External Party (if 3rd party hosted)	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes siting and protection security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.7.9	**Security of Assets Off-Premises** Off-site assets shall be protected.	Yes	Internal HCL (if HCL hosted) External Party (if 3rd party hosted)	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes equipment and asset off-premise security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.7.10	**Storage media** Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Yes	Internal HCL	HCL Software ISMS - Asset Management policy	HCL Software seldom manage/use removable media. However, if we do, Information Owners / Custodians must ensure the management of removable media in accordance with the information classification. Cryptographic techniques must be used to protect data on all removable media. Authorization must be required and documented for media removed from the organization. If no longer required, the contents of any re-usable media that are to be removed from the organization must be made unrecoverable.
A.7.11	**Supporting Utilities** Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	Internal HCL (if HCL hosted) External Party (if 3rd party hosted)	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes supporting utilities security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.7.12	**Cabling Security** Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.	Yes	Internal HCL (if HCL hosted) External Party (if 3rd party hosted)	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes cabling security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.7.13	**Equipment Maintenance** Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	Yes	Internal HCL (if HCL hosted) External Party (if 3rd party hosted)	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes equipment maintenance security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.7.14	**Secure Disposal or Re-use of Equipment** Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Yes	Internal HCL (if HCL hosted) External Party (if 3rd party hosted)	HCL Software ISMS - Physical and Environmental Security, HCL Software ISMS - Asset Management	HCL Software Physical and Environmental Security and HCL Software Asset Management describe disposal and re-use security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.8	**TECHNOLOGICAL CONTROLS**				
A8.1	**User End Point Devices** Information stored on, processed by or accessible via user end point devices shall be protected.	Yes	Internal HCL	HCL Software Security and Standards for all Employees includes security measures for mobile devices. HCL Software ISMS - Human Resources	HCL Software maintains mandatory compliance criteria for workstations and mobile devices within HCL Security Use Standards for Employees. HCL Software Human Resource policy describes clean desk and clear screen (including Unattended equipment) security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.8.2	**Privileged Access Rights** The allocation and use of privileged access rights shall be restricted and managed.	Yes	Internal HCL	HCL Software ISMS - Access Controls policy	Management of privileged access requires management approval and regular reviews as defined in HCL Software Access Control policy.
A.8.3	**Information Access Restriction** Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	Yes	Internal HCL	HCL Software ISMS - Access Controls policy	HCL Software Access control requirements are defined at both system and application levels.
A.8.4	**Access to Source Code** Access to program source code shall be restricted.	Yes	Internal HCL	HCL Software ISMS - Access Controls policy	Processes for modifying software as authorized by HCL Software management are defined in HCL Software Access Control policy.
A.8.5	**Secure Authentication** Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	Yes	Internal HCL	HCL Software ISMS - Access Controls policy	HCL Software Production delivery treats all system, application and data as confidential unless specifically exempted and therefore any log on access must be secure log-on
A.8.6	**Capacity Management** The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Yes	Internal HCL	HCL Software ISMS - Security Readiness Standard, Provisioning and Deprovisioning HCL Software ISMS - Health Check of Environments	HCL Software ISMS - Security Readiness Standard, Provisioning and Deprovisioning provides requirements of capacity planning / projection and HCL Software Health Check policy has capacity management as a health check requirement for monitoring
A.8.7	**Protection against Malware** Protection against malware shall be implemented and supported by appropriate user awareness.	Yes	Internal HCL	HCL Software ISMS - Security Readiness Standard, Provisioning and Deprovisioning	HCL Software approved anti-virus program/solution to detect and block malware being uploaded is a requirement for any device to be security ready
A.8.8	**Management of Technical Vulnerabilities** Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	Yes	Internal HCL	HCL Software ISMS - Vulnerability Scanning HCL Software ISMS - Internal Audit and Compliance and all ISMS Operational Security activities	Initial service activation vulnerability scans and periodic scans shall be performed. Upon identification of potential technical vulnerabilities, corrective action shall be taken to an established time-line. Vulnerability scanning - TCP/IP vulnerability scanning must be conducted. Security advisory patch management to install security advisory patches within the time limits outlined. HCL Software Management is responsible for ensuring technical compliance with the requirements of the ISMS. Security operational monitoring is conducted on an ongoing basis giving insight to technical compliance
A.8.9	**Configuration Management** Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	Yes	Internal HCL	Asset Management Policy Configuration Management Standard OS Hardening & Golden Image	Operating System (OS) Hardening is implemented which includes the process of implementing security measures and patching for operating systems for both Windows and Linux with the objective of protecting sensitive computing systems.
A.8.10	**Information Deletion** Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	Yes	Internal HCL	Personal Data Retention and Deletion Standard	HCL Software shall keep personal/sensitive Data in a form that is personally identifiable for no longer than necessary to accomplish the purposes, or other permitted purpose, for which the Personal Data was obtained. Thereafter, it shall either be destroyed, deleted, anonymized, or removed from the information systems in accordance with the company's data retention and deletion policies.
A.8.11	**Data Masking** Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Yes	Internal HCL	Data Privacy Policy	HCL Software shall keep Personal Data in a form that is personally identifiable for no longer than necessary to accomplish the purposes, or other permitted purpose, for which the Personal Data was obtained. Thereafter, it shall either be destroyed, deleted, anonymized, or removed from the information systems in accordance with the company's data retention and deletion policies.
A.8.12	**Data Leakage Prevention** Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Yes	Internal HCL	End Point Protection Standard	DLP tools are installed at the user endpoint (laptop) which is part of OS configuration and includes monitoring activities that are sent to the DART team. The DART team monitor and report incidents and quarantine devices as needed.

A.8.13	**Information Back Up** Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Yes	Internal HCL	HCL Software ISMS - Information Security Aspects of Business Continuity	HCL Software secures daily and weekly backups which are encrypted and stored.
A.8.14	**Redundancy of Information Processing Facilities** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes	Internal HCL	HCL Software ISMS - Information Security Aspects of Business Continuity	HCL Software have a formal approach to planning for information security continuity
A.8.15	**Logging** Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	Yes	Internal HCL	HCL Software ISMS - Security Monitoring and Logging	HCL Software security strategy includes the requirement to establish standard methods of recording various security related activity through event logging. Access to log information is controlled to prevent any tampering or unauthorised access. Administrator and operator logs shall be logged and the policy is to ensure this level of logging is never disabled.
A.8.16	**Monitoring Activities** Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Yes	Internal HCL	Security Monitoring and Logging Policy Logging Management Standard	Policies and standards are in place which describes the Security Monitoring and Logging requirements along with the list of applicable tools and Reports within the context of HCL Software products.
A.8.17	**Clock Synchronization** The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	Yes	Internal HCL	HCL Software ISMS - Security Readiness Standard, Provisioning and Deprovisioning	Clock Synchronisation as a security readiness requirement is mandated for all devices ensuring that activity logging has synchronized timings.
A.8.18	**Use of Privileged Utility Programs** The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	Yes	Internal HCL	HCL Software ISMS - Access Controls policy	HCL Software access for utility programs is defined by the requirements in the Access Control policy.
A.8.19	**Installation of Software on Operational Systems** Procedures and measures shall be implemented to securely manage software installation on operational systems.	Yes	Internal HCL	HCL Software ISMS - System Acquisition, Development and Maintenance, Security Readiness Standard, Provisioning and Deprovisioning, Patch Management, Asset Management and HCL Code of Business Ethics and Conduct.	HCL practices for software deployment, device readiness and patch management assure the controls required for software installation and management on operating systems
A.8.20	**Network Controls** Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	Yes	Internal HCL	HCL Software ISMS - Communication Controls (Networks & Firewalls)	HCL Software data network infrastructure must meet our security requirements to preserve the security of data and data in motion across our offerings. Our Policy provides the guidance for the management and control of networks, network devices or applications that provide Network Services .
A.8.21	**Security of network services** Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	Yes	Internal HCL	HCL Software ISMS - Communication Controls (Networks & Firewalls)	HCL Software data network infrastructure must meet our security requirements to preserve the security of data and data in motion across our offerings. Our Policy provides the guidance for the management and control of networks, network devices or applications that provide Network Services .
A.8.22	**Segregation of Networks** Groups of information services, users and information systems shall be segregated in the organization's networks.	Yes	Internal HCL	HCL Software ISMS - Communication Controls (Networks & Firewalls)	HCL Software data network infrastructure must meet our security requirements to preserve the security of data and data in motion across our offerings. Our Policy provides the guidance for the management and control of networks, network devices or applications that provide Network Services .
A.8.23	**Web Filtering** Access to external websites shall be managed to reduce exposure to malicious content.	Yes	Internal HCL	Communication Controls (Networks and Firewalls) Policy Web Application Firewall Standard	HCL network traffic are controlled, managed and periodically evaluated to identify vulnerabilities. All firewalls and network components are monitored to ensure no malicious traffic is on the HCL SW network.
A.8.24	**Use of Cryptography** Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Yes	Internal HCL	HCL Software ISMS - Cryptography policy	Encryption is required for data at rest and in transit. A policy on the use, protection and lifetime of cryptographic keys has be developed and implemented through their whole lifecycle.
A.8.25	**Secure Development Life Cycle** Rules for the secure development of software and systems shall be established and applied.	Yes	Internal HCL	HCL Software ISMS - System Acquisition, Development and Maintenance policy	Secure Engineering principles are applied to development practices including formal change controls
A.8.26	**Application security requirements** Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Yes	Internal HCL	HCL Software ISMS - System Acquisition, Development and Maintenance policy and HCL Software ISMS - Cryptography	Requirement to protect information are assessed, protective solutions applied and all information passing over public networks shall be encrypted. Requirement to protect service transactions are assessed, protective solutions applied and all information passing over public networks shall be encrypted
A.8.27	**Secure System Architecture and Engineering Principles** Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	Yes	Internal HCL	HCL Software ISMS - System Acquisition, Development and Maintenance policy	Secure Engineering principles are applied to development practices
A.8.28	**Secure Coding** Secure coding principles shall be applied to software development.	Yes	Internal HCL	HCL Software Secure Engineering Framework (SEF)	The Secure Engineering Framework (SEF) is a set of recommended guidelines, requirements, and best practices to help HCLSoftware build more secure software through secure by design, secure in implementation and secure in deployment.
A.8.29	**Security Testing in Development and Acceptance** Security testing processes shall be defined and implemented in the development life cycle.	Yes	Internal HCL	HCL Software Secure Engineering framework (SEF) HCL Software ISMS - System Acquisition, Development and Maintenance policy	Secure Engineering principles are applied to development practices including system security testing
A.8.30	**Outsourced Development** The organization shall direct, monitor and review the activities related to outsourced system development.	Yes	Internal HCL	HCL Software ISMS - System Acquisition, Development and Maintenance policy	HCL Software does not currently outsource development. If it does in the future, we have a policy and controls to consider before commencing any outsource agreement
A.8.31	**Separation of Development, Test and Production Environments** Development, testing and production environments shall be separated and secured.	Yes	Internal HCL	HCL Software Secure Engineering framework (SEF) HCL Software ISMS - System Acquisition, Development and Maintenance policy	HCL Software practice secure engineering including separation for development and test activities Secure Engineering principles are applied to development practices including development environments
A.8.32	**Change Management** Changes to information processing facilities and information systems shall be subject to change management procedures.	Yes	Internal HCL	HCL Software ISMS System Acquisition, Development and Maintenance policy	Changes to the organization, security policy and any processes / procedure that affect information security shall be controlled. Secure Engineering principles are applied to development practices including change control, verification and validation after operating system changes
A.8.33	**Test Information** Test information shall be appropriately selected, protected and managed.	Yes	Internal HCL	HCL Software ISMS - System Acquisition, Development and Maintenance policy	Secure Engineering principles are applied to development practices including protection of test data
A.8.34	**Protection of Information Systems during Audit Testing** Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	Yes	Internal HCL	HCL Software ISMS - Health Check of Environments and HCL Software ISMS - Internal Audit and Compliance	Health checking across all environments provides and audit of environment status against our health check criteria. Internal Audit provides assurance of compliance to all aspects of our ISMS