

<b>HCLTech</b>	Technical and Organizational Measures (TOMs) for Vendor Security Requirements	Version 3.0
	Risk and Compliance	March 2025

**HCLTech**  
**TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs) FOR VENDOR SECURITY REQUIREMENTS**

**Contents**

Objective:..... 2

This document describes:..... 2

Applicability..... 2

General Security Requirements ..... 2

1. Human Resource Security ..... 4

2. Asset Management..... 5

3. Identity and Access Control ..... 5

4. Cryptography..... 7

5. Physical and Environmental Security ..... 7

6. Operations Security ..... 9

7. Network Security.....10

8. Software Development..... 11

9. Vulnerability Management ..... 11

10. Incident management.....12

11. Cloud Security Measures.....12

12. Business Continuity Management.....13

13. Data Retention and Disposal .....13

14. Data Masking and Anonymization.....14

15. Data Minimization .....15

16. Data Catalogue, Classification, Attribute Lineage and Quality .....15

17. Risk Management and Governance.....15

18. Sub-Contracting Measures .....16

19. Right to Audit .....16

HCLTech Restricted

DO NOT CIRCULATE OR MODIFY WITHOUT PRIOR APPROVAL OF HCLTech RISK & COMPLIANCE

<b>HCLTech</b>	Technical and Organizational Measures (TOMs) for Vendor Security Requirements	Version 3.0
	Risk and Compliance	March 2025

### Objective

This Technical and Organizational Measures (TOMs) for Vendor Security Requirements document is incorporated by reference into the Master Agreement and/or Purchase Order Terms and any other HCLTech Agreements that the parties may have entered for the procurement and provision of Services from the Vendor to HCLTech (hereinafter referred to as 'Contractual Terms').

### This document describes

HCLTech's security expectations and requirements for vendors to safeguard HCLTech and/or its Affiliates as defined in Contractual Terms (hereinafter 'HCLTech') data, systems, and supply chain vendor's legal and regulatory compliance obligations that the vendors shall adhere to when providing goods or services to HCLTech or its clients.

### Applicability

This applies to all the vendors, contractors, and third parties that may have access to HCLTech data, IT infrastructure or systems and/or process or collect data on behalf of HCLTech, and/or provide services to HCLTech.

### General Security Requirements

1. HCLTech being a Global IT Service provider may provide services to its clients from various industries and countries. It is mandatory for the vendors associated with HCLTech to comply with all applicable local, national, and international regulations, which vary across industries and geographies (example, but not limited to EU-DORA, German-LKSG, SOX, PCI-DSS, Cyber Essentials, HIPPA, GDPR, FCPA, IRFS, FATCA, BASEL III, etc.) and also comply to new laws and regulations (e.g. upcoming India DPDP Act).
2. If the vendor is processing Personal Data for and on behalf of HCLTech, a separate Data Processing Agreement or Data Processing and Vendor Security Agreement (DPVSA) shall also be applicable, and the vendor agrees to abide by those terms. If the vendor is processing, storing or accessing Protected Health Information (PHI) on behalf of HCLTech, the Vendor must sign and comply with the terms of the Business Associate Agreement (BAA) under The Health Insurance Portability and Accountability Act (HIPAA).
3. Vendors shall have documented and approved (by vendor's senior management) information security policies. The Security policies shall be reviewed and updated at least on an annual basis.
4. The information security policies shall be published, and communicated to the vendor's personnel, contractors, agents and relevant third parties.
5. The information security policies shall be aligned with recognized information security standards such as ISO 27001/27002, NIST CSF, HITRUST CSF, GDPR, or other applicable industry-specific regulations.
6. Vendor shall notify HCLTech immediately without any undue delay upon discovering of a security breach or incident or personal data breach which may affect the services or HCLTech's reputation, via e-mail to [Infosecincidents@hcltech.com](mailto:Infosecincidents@hcltech.com) and to vendor's primary business contact within HCLTech or at the least within 24hrs. To maintain confidentiality of HCLTech's Information, vendors shall collaborate with HCLTech for any further communication or investigation.
7. Vendor shall return or securely destroy all data, remove any access to HCLTech's data or any other assets issued in case of contract termination or end of the contract or end of data retention

**HCLTech Restricted**

**DO NOT CIRCULATE OR MODIFY WITHOUT PRIOR APPROVAL OF HCLTech RISK & COMPLIANCE**

<b>HCLTech</b>	Technical and Organizational Measures (TOMs) for Vendor Security Requirements	Version 3.0
	Risk and Compliance	March 2025

period whichever is earlier.

8. Use long and complex passwords (Minimum of 8 characters, recommended is minimum 12 characters), shall include at least one uppercase letter, one lowercase letter, one number, and one special character.
9. All vendors shall use Two-Factor or Multi-Factor Authentication (2FA or MFA) for authentication for all applications and systems used for delivering services to HCLTech.
10. Limit access to systems and data to only those individuals who need it. Enforce the principle of least privilege, ensuring that limited access rights are given to your personnel (minimum access necessary to perform their tasks).
11. Remove access promptly for individuals who no longer require it or leave your organization.
12. All network communications between the vendor's systems and the HCLTech systems must use secure protocols.
13. Do not store (including backups) HCLTech data onto vendor systems, third-party applications (including cloud) or network unless it is explicitly required and clearly specified in the contract.
14. HCLTech data shall NOT be used to train any kind of large language model (LLM) or artificial intelligence (AI) capabilities by the vendor.
15. Encrypt sensitive data at rest and in transit using industry-standard protocols.
16. Maintain antivirus and anti-malware protection across all systems and regularly update software and firmware to patch vulnerabilities.
17. Vendor shall conduct regular penetration testing and vulnerability scans in its own environment.
18. Vendor shall enable logging and monitoring on all operating systems, databases, applications, and security and network devices that are involved in providing services to HCLTech. Logs shall be kept for a minimum of 12 months or as long as legally required, whichever is longer.
19. Protect facilities, hardware, and systems from unauthorized physical access.
20. Perform adequate background checks, onboarding, offboarding for personnel (employees, contractors, and third-party).
21. Ensure that your employees and contractors complete regular security awareness training conducted by you and HCLTech (where needed)
22. Vendor shall participate in periodic audits and assessments as requested by the HCLTech.
23. Vendor shall have an ongoing risk governance program (to manage the risks; identify and assess the impact of risk; risk reduction or mitigation strategies are identified and implemented) to effectively manage risks in the constantly changing threat landscape.
24. Vendor should review the effectiveness of the implemented security controls and conduct internal security audits at planned intervals.
25. Vendor may be subject to local, regional, regulatory, and statutory requirements that affect compliance with certain of the HCLTech standards set forth in this document. In the event of a conflict between the requirement in this document and any regulatory or statutory requirement

**HCLTech Restricted**

**DO NOT CIRCULATE OR MODIFY WITHOUT PRIOR APPROVAL OF HCLTech RISK & COMPLIANCE**

<b>HCLTech</b>	Technical and Organizational Measures (TOMs) for Vendor Security Requirements	Version 3.0
	Risk and Compliance	March 2025

applicable to Vendor, the applicable local, national, or regional regulatory or statutory requirement shall prevail. If such a conflict exists, the Vendor shall inform HCLTech of the underlying regulatory requirements, which affect compliance and propose mitigating controls to provide an equivalent level of information security, business continuity, or privacy.

**Refer to the section Annexure 1: Detailed requirements for comprehensive understanding the Vendor Security Requirements**

[Annexure 1: Detailed requirements:](#)

**1. Human Resource Security**

Vendor shall ensure:

**Background Verification**

- a. Vendors shall have documented and approved policies and procedures for background checks, onboarding, off boarding. The policies shall be reviewed and updated at least on an annual basis.
- b. Adequate background checks (including but not limited to identity verification, criminal Records check, employment history, educational qualification check, address verification, and other checks as applicable, such as drug testing or professional license verification) shall be performed in compliance with applicable local, state, and federal laws and in consideration of the individual's privacy rights. These checks shall be performed for all employees and contractors.

**Training and Awareness**

- a. Appropriate and mandatory trainings of HCLTech (including role-based trainings) shall be conducted at the time of joining and at least annually thereafter for all vendor's personnel and contractors.
- b. The training shall cover key domains (but not limited to) ethics & compliance, information, and cyber security, data privacy and the contents shall be regularly updated considering business requirements, regulatory changes, risks and security incidents.
- c. All vendor's personnel and contractors shall read, Asset Management understand and sign the Terms of Employment and Information Security Policy.
- d. All vendor's personnel and contractors shall be made aware of the disciplinary process, so that they are aware of consequences in case they violate any policy or the terms of employment, or intentionally commit/participate in any kind of activities leading to a security breach or non-compliance.

<b>HCLTech</b>	Technical and Organizational Measures (TOMs) for Vendor Security Requirements	Version 3.0
	Risk and Compliance	March 2025

## 2. Asset Management

Vendor shall ensure:

### Asset Inventory

- a. Vendor shall maintain an asset inventory of all media and equipment (including the cloud environment) where HCLTech's Data is stored. Access to such media and equipment shall be restricted to authorized personnel of the Vendor.
- b. Vendor shall not use any software or hardware that is at/near its End of Life (EOL) or any unlicensed software or product to provide services to HCLTech. Regular monitoring and audits shall be conducted to eliminate the usage of EOS (End of Support) /EOL (End of Life) systems or any non-licensed software.
- c. Each asset shall have an identified owner who shall be responsible for ensuring appropriate controls to safeguard the asset including their physical security.
- d. Regular audits shall be conducted to ensure asset details are appropriately captured in the inventory and it is getting regularly updated.

### Asset labelling

- a. Vendor shall classify and label HCLTech assets and data basis on-Confidentiality, Integrity, and Availability (CIA), so that it is clearly identifiable, and access controlled at all times.
- b. Vendor shall maintain an acceptable use policy with restrictions on printing HCLTech's Data or information. In case printing is unavoidable due to business needs, procedures shall exist for appropriate disposal of HCLTech related printed materials.
- c. No personnel of vendors shall store or access any HCLTech related data outside of the vendor's facilities on portable devices like laptops, mobile phones, tabs etc. unless explicitly approved by HCLTech in writing.
- d. If HCLTech has provided any hardware or software to the vendor, the vendor shall maintain proper asset inventory, capturing the details of asset user, contact information, location etc.
- e. For vendor's own information systems (hardware, software, intellectual property etc.), vendor shall maintain an asset classification and labelling policy and supporting procedures/guidelines. All the vendor assets shall be inventoried and labelled accordingly.
- f. Acceptable usage policy and asset management guidelines for handling assets are maintained and communicated to all applicable employees and contractors.
- g. Processes shall be in place to confirm allocated assets to an employee/contractor. Processes shall be implemented to timely collect the allocated devices from employees and contractors on or before the last day of employment in case of termination/separation of employment, contract, or agreement.

## 3. Identity and Access Control

Vendor shall ensure:

- a. Vendor shall maintain an appropriate access control policy that is designed to restrict access to HCLTech Data (including cloud environment and SaaS applications) and only to authorized personnel, agents, and contractors.
- b. Vendor shall maintain user account creation and deletion procedures for granting and revoking access (including creation and allocation of privileged user accounts) to all assets, HCLTech Data, and all internal applications while delivering goods or services as per the contract. For privilege access or user accounts with elevated access levels, appropriate approval authority and accountability shall be established.

**HCLTech Restricted**

**DO NOT CIRCULATE OR MODIFY WITHOUT PRIOR APPROVAL OF HCLTech RISK & COMPLIANCE**

<b>HCLTech</b>	Technical and Organizational Measures (TOMs) for Vendor Security Requirements	Version 3.0
	Risk and Compliance	March 2025

- c. Unique user ID shall be created for each user having access to the information systems. Generic IDs creation based on the operation/functional requirement shall be avoided and if required due to business need, HCLTech's approval shall be obtained prior to creation of such ID. Usage and changes done using such ID shall be appropriately logged and tracked.
- d. Vendor shall ensure all the default or OEM supplied credentials are modified before using any asset or application for HCLTech.
- e. For systems and applications having HCLTech sensitive or confidential data, the vendor shall perform quarterly access right reviews for users and for other systems and applications access rights review shall be performed at least once annually.
- f. Vendor applications must have the capability to configure roles and the entitlements for each role in addition to the out of the box roles and entitlements
- g. Vendor applications must have the capability to connect to HCLTech applications to read the employee profile and grant and revoke role(s) and the entitlements dynamically to an employee.
- h. In cases where dynamic role and entitlement is not possible, vendor applications must have the capability to define functional admin roles who can grant and revoke roles and entitlements to users.
- i. Vendor applications must have the capability to connect HCLTech's or any third-party identity and access management tool and consume the role and entitlement configured in such identity and access management tool and provision the access to the users as per configuration in the identity and access management tool.
- j. Vendor applications must have the capability to generate reports on lists of users, their roles and entitlement and share the same with HCLTech when required or provide a capability for HCLTEC users to generate such reports. The access to generate such reports must be restricted to limited roles.

#### Least Privilege Access

- a. Vendor shall restrict access to its systems (including cloud environment and SaaS applications) to only those individuals who require such access to perform their duties using the principle of least privilege access through robust identity management tools such as enterprise Active Directory solution or similar.
- b. Use of administrative credentials shall be restricted to limited circumstances (such as troubleshooting purposes) and users perform their day-to-day operations with least privileged credentials.
- c. Vendor shall implement segregation of duties between its environments so that no individual person has access to perform tasks that create a security conflict of interest (e.g., programming/administrator, developer/operations)

#### Authentication

- a. Vendor personnel, agents and contractors shall use multi-factor authentication (including privilege users) and encrypted sessions for access to vendor systems and the cloud environment.
- b. Vendor shall maintain and enforce a password policy that is aligned with leading Industry Standards (e.g., NIST Cyber Security Framework, PCI DSS (Payment Card Industry Data Security Standard), Centre for Internet Security, etc.)
- c. Passwords must always be encrypted when stored and during transit.
- d. In case the Vendor Services require external connections to HCLTech's environment, it shall be done only as per HCLTech approved solution/design

**HCLTech Restricted**

**DO NOT CIRCULATE OR MODIFY WITHOUT PRIOR APPROVAL OF HCLTech RISK & COMPLIANCE**

<b>HCLTech</b>	Technical and Organizational Measures (TOMs) for Vendor Security Requirements	Version 3.0
	Risk and Compliance	March 2025

- e. Vendor shall use current Industry best practices to:
  - a. To identify and authenticate personnel, agents and contractors who attempt to access information systems and assets.
  - b. Monitor for repeated access attempts to information systems and assets.
  - c. Deactivate passwords that have been corrupted or disclosed.
  - d. Define account lockout thresholds.
  - e. Implement solutions to prevent unauthorized changes to critical system files.
  - f. Generate reports capturing the user ID, role assigned, activities performed, time stamp, etc. for various systems.
- f. Vendor shall have policies and system configured to ensure:
  - a. Passwords meet the requirements set by the policy based on industry standards, including but not limited to length, expiry, complexity, password history, failed attempts, account lockout duration, password age, and change on first logon etc.
    - i. Eliminate usage of generic and shared IDs.
    - ii. Secure mechanisms to deliver user passwords.
    - iii. Validate user identities before initiating password resets.
    - iv. Generation and retention of logs for privileged account activities for future audit purposes.

#### 4. Cryptography

Vendor shall ensure:

- a. Vendor shall maintain policies regarding the use of cryptographic controls that are implemented to protect HCLTech Data.
- b. Key Management procedures for secure key generation, ownership, distribution, archival, storage, and revocation to protect keys throughout the life cycle shall be established and maintained by the service Vendor
- c. Use of only secure and current industry standard encryption algorithms and key strengths that assure adequate protection of data is permitted.

#### 5. Physical and Environmental Security

Vendor shall ensure:

##### Physical Access to Facilities

- a. Policy and associated procedures for physical security measures and environmental controls shall be implemented based on industry standards and regulatory requirements.
- b. Vendor shall limit access to facilities (where systems that are involved in providing the Services to HCLTech are located) to authorized personnel, agents and contractors.
- c. All critical facilities and locations which house the important IT systems, applications, and personnel (e.g., data centres, operational facilities) shall be adequately protected against accidents, attacks, and unauthorized access etc.
- d. Security controls such as electronic access controls, Identity verification, security guards, visitor management and 24x7 CCTV monitoring etc. shall be in place to protect the buildings against unauthorized access.

HCLTech Restricted

DO NOT CIRCULATE OR MODIFY WITHOUT PRIOR APPROVAL OF HCLTech RISK & COMPLIANCE

<b>HCLTech</b>	Technical and Organizational Measures (TOMs) for Vendor Security Requirements	Version 3.0
	Risk and Compliance	March 2025

- e. CCTV recordings shall be retained for a minimum of 60 days for sensitive areas like datacentres, ODC and a minimum of 30 days for other areas or longer as per the applicable legal and regulatory requirements.
- f. Vendor shall maintain visitor logs and not permit visitors to access/visit facilities (where systems that are involved in providing the Services to HCLTech are located) unless explicitly approved by HCLTech on the grounds of business requirements.
- g. Access rights to secure areas shall be regularly reviewed and updated
- h. Effectiveness of physical and environmental controls shall be tested and evaluated at least annually.

**Media Handling and Transfer**

- a. Vendor shall maintain records of incoming and outgoing media/equipment containing HCLTech Data, including the type of media, the authorized sender/recipient, the date and time, the number of media, and the type of data the media contains.
- b. Vendor shall ensure that backups (including remote and cloud service backups) are properly protected via physical security or encryption when stored, as well as when they are moved across the network.
- c. In the event that backup media/equipment of HCLTech and/or HCLTech client data is stored / shipped offsite, vendor must take written approval of HCLTech before moving the media/equipment to any such location

**Protection from Disruptions**

- a. The Vendor shall protect equipment from power failures and other disruptions caused by failures in supporting utilities.
- b. All critical facilities and IT system locations are housed in secure buildings that have been built using fire-proof materials and are equipped with fire alarms, smoke detectors, temperature sensors, fire extinguisher systems etc. to protect against fire, the weather, flooding, and other natural hazards.
- c. Telecommunications and network cabling must be protected from interception, interference, and/or damage.
- d. Periodic maintenance of all critical equipment like Generators/UPS/smoke detectors/fire extinguishers/fire suppression systems, access control systems shall be performed, and appropriate records shall be maintained.

**Secure Disposal or Reuse of Equipment**

- a. Vendor shall verify equipment containing storage media, to confirm that all HCLTech Data has been deleted or securely overwritten using current Industry Standard processes, prior to disposal or re-use.
- b. Mechanisms for secure disposal of data in hard and soft copy format shall be defined and implemented – for example, crosscut shredders shall be used for disposing of paper documents, and use (where appropriate) methodologies such as sanitization, Degaussing, and physical destruction for shredding of electronic media.

**Clear Desk and Clear Screen Policy**

- a. Vendors shall adopt a clear desk policy for papers and removable storage media and a clear screen policy.

<b>HCLTech</b>	Technical and Organizational Measures (TOMs) for Vendor Security Requirements	Version 3.0
	Risk and Compliance	March 2025

## 6. Operations Security

Vendor shall ensure:

- a. Vendor shall maintain appropriate operational, and security operating procedures and such procedures shall be made available to all personnel who require them.
- b. Operating procedures shall be reviewed minimum on an annual basis and updated whenever there shall be any operating or system change. The updated procedure shall be duly approved and released to all the relevant personnel.

### Logging and Monitoring of the Events

- a. Vendor shall enable logging and monitoring on all operating systems, databases, applications, and security and network devices that are involved in providing services to HCLTech.
- b. Logs shall be kept for a minimum of 12 months or as long as legally required, whichever is longer.
- c. Logs shall capture the access ID, the authorization granted or denied, the date and time, the relevant activity, and be regularly reviewed.
- d. All relevant information processing systems shall synchronize time to a single reference time source.
- e. Logging capabilities shall be protected from alteration and unauthorized access.
- f. Vendors shall monitor and analyze the logs for incident monitoring, unusual events/activities, alerts, etc. and take appropriate measures and corrective actions in a timely manner.

### Protection from Malware

- a. Vendor shall maintain anti-malware controls that are designed to protect systems from malicious software, including malicious software that originates from public networks like (but not limited to), viruses, spyware, worms, unauthorized mobile code, key logger software, botnets, Trojans, polymorphic malware, zero-day malware etc.
- b. Malware signatures shall be updated on a regular basis to ensure systems are using the latest definitions.
- c. Events like anti-malware services being terminated or disabled shall be closely monitored and addressed at highest priority.
- d. Malware protection software shall be configured to run scheduled as well as on-demand scans and to isolate/delete any malicious files or software.
- e. End users are not provided with the rights to disable malware protection.

### Change Management

- a. Documented and approved change management policy and processes shall be established by the vendor to ensure changes to IT systems, applications, databases, and network components etc. are logged, reviewed, tested, and formally approved by authorized personnel before the changes are implemented.
- b. The change management plan shall include the rollback of changes if the proposed changes have a negative impact. Records of all changes shall be maintained.
- c. The vendor shall ensure that only approved and secure versions of code, configurations, systems, utilities, and applications shall be deployed in the production environment.

HCLTech Restricted

DO NOT CIRCULATE OR MODIFY WITHOUT PRIOR APPROVAL OF HCLTech RISK & COMPLIANCE

<b>HCLTech</b>	Technical and Organizational Measures (TOMs) for Vendor Security Requirements	Version 3.0
	Risk and Compliance	March 2025

### Encrypted Backup

- a. Vendor shall maintain an encrypted backup and restoration policy that also protects HCLTech's Data from exposure to ransomware attacks, and shall back up HCLTech's Data, software, and system images in accordance with contractual requirements.
- b. Data backups shall be taken periodically using a secure and reliable mechanism. Backup restoration processes shall be documented, and restoration of data is to be tested at a defined frequency and corresponding evidence be maintained.
- c. Information in backup media or storage appliance is encrypted using a strong encryption algorithm.
- d. Logs for failed backups (if any) are monitored by the backup admin and corresponding corrective action is performed and documented.

### Data Security

- a. Vendor shall implement controls to prevent copy, transfer, upload or sharing of HCLTech data to any unauthorized location / media or recipient without express written approval from HCLTech
- b. Full disk encryption is configured for workstations and servers.
- c. Vendor shall ensure no HCLTech information is stored in any unauthorized third-party cloud storage solutions.
- d. Vendor shall document and share with HCLTech, the data locations, for the copies of data that are made and how they are controlled and stored
- e. Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit HCLTech data.

### Patch Management

- a. Vendor shall ensure that the latest security patches shall be applied to systems, Networks, applications, and databases, etc. in a timely manner and based on the criticality of the vulnerability addressed by the patch. Patches shall be obtained from respective OEMs directly for proprietary systems and deployed at the earliest as per the patch management policy of the vendor or as per timelines recommended by the OEM, whichever is earlier.
- b. All patches shall be tested before deployment of the patches to production systems and the correct operation of the patched service is verified after any patching activity.

## 7. Network Security

Vendor shall ensure:

- a. Segregate network systems containing HCLTech Data from network systems supporting internal or other activity.
- b. The vendor shall consider defence in-depth principles for network security to minimize the network security risks. The design and implementation of the networks are reviewed at least annually.
- c. Vendor Inbound and outbound network points shall be protected by current industry leading firewalls and intrusion detection systems (IDS). Firewall and router rule set reviews shall be conducted on a periodic basis.
- d. Communications shall be limited to systems strictly allowed, and if possible, intrusion prevention systems (IPS) shall be used. Ports and protocols shall be limited to those with specific business purposes.
- e. Vendor shall implement access controls on wireless networks, strong encryption and strong authentication (e.g., WPA2) shall be used.

HCLTech Restricted

DO NOT CIRCULATE OR MODIFY WITHOUT PRIOR APPROVAL OF HCLTech RISK & COMPLIANCE

<b>HCLTech</b>	Technical and Organizational Measures (TOMs) for Vendor Security Requirements	Version 3.0
	Risk and Compliance	March 2025

- f. Vendor shall implement Internet filtering procedures and technology to protect end user workstations from malicious websites and unauthorized file transfers outside the network. Only authorized file sharing websites and tools shall be used for business purposes. Access to unauthorized file sharing websites and tools shall be blocked.
- g. Any remote access to vendor network shall be approved and shall be over an encrypted Virtual Private Network (VPN) connection configured with Multifactor authentication.
- h. Controls shall be implemented to prevent access to websites hosting malicious, illegal and harmful content. Security controls are in place to prevent misuse of email systems and ensure all email communications are over an encrypted channel.
- i. Anti-phishing and Anti-Spam filters along with other configurations such as Spoof protection etc. to prevent email bound threats shall be enabled on the email gateway.
- j. Access to all systems and applications shall be done using secure protocols, and authentication mechanisms and encrypted channels.

## 8. Software Development

Vendor shall ensure:

- a. Secure system engineering and coding practices shall be established (in line with Secure Software Development best practices like OWASP), documented, and integrated within the system development life cycle (SDLC).
- b. Developers shall attend secure development training periodically.
- c. System and application changes shall undergo testing and meet defined acceptance criteria prior to implementation. Testing shall also include relevant security controls
- d. Production and non-production environments are segregated appropriately. Segregation of duties for production and non-production developments is maintained.
- e. Source code shall undergo automated static source code analysis and vulnerability remediation prior to any usage or data transfer.
- f. Live data shall not be used in a test environment unless prior approval from the HCLTech is obtained. The access to the test data should be given to limited personnel on need-to-know basis.
- g. Vendor shall monitor outsourced system development activities, subject to third-party vendor management controls.

## 9. Vulnerability Management

Vendor shall ensure:

- a. Vendor shall implement a vulnerability management process to identify, report, and remediate vulnerabilities related to the system, application and Open Source containing HCLTech Data (including cloud and SaaS applications), by performing vulnerability scans on a regular basis (at least annually) and during any major system or application updates; implementing vendor patches or fixes; and Developing procedures to address the remediation of identified vulnerabilities.
- b. Vendor shall also perform annual penetration testing for systems and applications that store or allow access to HCLTech Data, including personal data, or when significant changes are made to those systems and applications.

HCLTech Restricted

DO NOT CIRCULATE OR MODIFY WITHOUT PRIOR APPROVAL OF HCLTech RISK & COMPLIANCE

<b>HCLTech</b>	Technical and Organizational Measures (TOMs) for Vendor Security Requirements	Version 3.0
	Risk and Compliance	March 2025

- c. Identified vulnerabilities shall be remediated within defined timelines "critical" within seven (7) days; "high" within Four (4) weeks; and "medium" within Six (6) and "low" within Ten (10) weeks or as per the timelines provided by the OEM, whichever is earlier
- d. Zero-day vulnerability management policy shall be in place to mitigate the zero-day attack.
- e. On request, Vendor shall share with HCLTech the penetration/vulnerability test reports relevant to the services being provided.
- f. Application security assessments shall be performed for all newly developed applications and any existing applications that are going through a significant change to identify any known security vulnerabilities.
- g. All security vulnerabilities identified with CVSS score greater than four shall be mitigated prior to deployment of application in the production environment.
- h. HCLTech or a third party appointed by HCLTech may conduct Vulnerability Assessment (VA) and Penetration Testing (PT) on Vendor's systems/applications/network used to process, access or store HCLTech or HCLTech's customer data as per the mutually agreed scope of such testing and frequency.

## 10. Incident management

Vendor shall ensure:

- a. A documented incident management policy and associated procedures shall be in place for the management of security incidents.
- b. Vendor shall maintain a record of Security Incidents noting the description of the Security Incident, the applicable time periods, the impact, the person reporting and to whom the Security Incident was reported, and the procedures to remediate the incident.
- c. In the event of a Security Incident identified by vendor, HCLTech shall be notified immediately without undue delay or at the least within 24hrs after becoming aware of the security and data breach incident impacting HCLTech. Notification of Security Breaches may be sent via e-mail to [infosecincidents@hcltech.com](mailto:infosecincidents@hcltech.com), and to vendor's primary business contact within HCLTech, best support to mitigate the risk.
- d. The vendor shall track disclosures of HCLTech Data, including what type of data was disclosed, to whom, and the time of the disclosure.
- e. Repository of all reported incidents shall be maintained along with the actions taken to mitigate the impact of the incident and lessons learned.
- f. In the event of a security incident, the vendor shall fully cooperate with HCLTech in any resulting investigation by HCLTech or HCLTech authorized personnel, a regulatory authority and/or any law enforcement agency by providing access and assistance as necessary and appropriate to investigate the incident.

## 11. Cloud Security Measures

Vendor shall ensure:

- a. If the Vendor provides cloud services or makes use of cloud services to deliver part or full set of services to HCLTech or HCLTech's customers, the following

An established framework shall be in place to ensure that use of cloud technology and non-public data stored in the Cloud is approved and subject to appropriate controls equivalent to the

HCLTech Restricted

DO NOT CIRCULATE OR MODIFY WITHOUT PRIOR APPROVAL OF HCLTech RISK & COMPLIANCE

<b>HCLTech</b>	Technical and Organizational Measures (TOMs) for Vendor Security Requirements	Version 3.0
	Risk and Compliance	March 2025

latest version of the Cloud Security Alliance, Cloud Controls Matrix (CCM) or SCO2-Type-2. Some of the best practises are shared below:

- o The geographic location of vendor infrastructure resources shall be made clear to HCLTech, and it shall be as per the contractual/SOW requirements.
- o Data stored in cloud environment or in transit shall be encrypted as per current industry standards.
- o Data Protection – Vendors providing Cloud Service must securely handle HCLTech related data. Compute resources and virtual machine resources by providing logical isolation and secure migration.
- o Authentication – Supplies providing Cloud Service must include methods or options for multi-factor authentication for cloud administrator roles and as required by HCLTech tenant business.
- o Access controls: Refer to the access controls section.
- b. Cloud security measures are embedded as security-by-design infrastructure with layered security that is built directly into the platform and its services.
  - o Defence-in-Depth security strategies
  - o Security application at all layers
  - o Unified segmentation of workloads
  - o Enable traceability and management
  - o Implementation of strong access identity foundation
- c. Leverage best-in-class industry solutions on Cloud workload protection platforms (CWPPs), Cloud access security brokers (CASBs), Cloud Native Application Protection Platforms (CNAPP).

## 12. Business Continuity Management

Vendor shall ensure:

- a. Business Continuity Management (BCM) Policy and associated procedures capturing business continuity objectives shall established, reviewed, and approved at least annually.
- b. Business Impact Analysis (BIA) & Risk Assessment (RA) shall be performed at least annually or following a significant change.
- c. Business Continuity Plan(s) (BCPs) and/or Disaster Recovery Plan(s) (DRPs) shall be reviewed and approved at least annually.
- d. A formal BCM Training and Awareness Program shall be implemented.
- e. Periodic testing, to validate the effectiveness of the business continuity strategies as mentioned in the BCPs and/or DRPs, shall be performed on an annual basis and records are maintained of such testing.
- f. Cyber Resilience and Crisis Management Plan (including pandemic preparedness) shall be established to ensure appropriate responses to emergency situations by enabling the protection of employees, visitors, the environment, assets, and business operations.

## 13. Data Retention and Disposal

Vendor shall ensure:

- a. Vendor shall retain HCLTech data only as per the contractual requirements. Upon termination or expiry of the contract, vendor shall provide the data records as per HCLTech’s requirement and shall

HCLTech Restricted

DO NOT CIRCULATE OR MODIFY WITHOUT PRIOR APPROVAL OF HCLTech RISK & COMPLIANCE

<b>HCLTech</b>	Technical and Organizational Measures (TOMs) for Vendor Security Requirements	Version 3.0
	Risk and Compliance	March 2025

not retain any data records of HCLTech in all instances where HCLTech data is stored.

- b. During the tenure of the contract, the vendor shall retain HCLTech data records for only such period as per the regulatory requirements of the specific record type and the region to which the record belongs or till such period for which there is a legitimate business need to retain the data. HCLTech data owner will define the period of legitimate business need for specific record type (examples of record type: employee payroll data, employee financial records, employee health data, employee dependent's data, customer invoices, vendor payment records etc.)
- c. Vendor's application shall have the capability to configure purge rules and purge HCLTech's records as per the configured purge rules. The purge rules must be in accordance with the applicable regulatory requirements for the respective data and the region to which the data belongs or the retention periods as defined by HCLTech data owner
- d. Vendor shall test the data retention and purge rules in a non-production environment and share the test results with HCLTech for sign-off
- e. Upon sign-off by HCLTech, vendor shall execute the data retention and purge rules in applicable environments as per the applicable frequency to purge HCLTech's records that qualify the purge rules
- f. Vendor shall provide to HCLTech the unique record ids and date range of the purged records as evidence of executing the data retention and purge rules
- g. Vendor shall take a backup of the production data before executing the purge rules in production environment to enable recovery of the records in case of issues
- h. Vendor shall destroy the back-up taken before execution of purge rules post approval from HCLTech
- i. Vendor and their third parties shall provide written confirmation, supporting logs and evidence of destroying all such data
- j. Vendor shall inventory and keep track of all data which are disposed by the Vendor
- k. If the vendor has outsourced the processing of HCLTech's data to a third party approved by HCLTech, vendor shall ensure that the third party complies with the above requirements as well.

#### 14. Data Masking and Anonymization

Vendor shall ensure:

- a. Vendor's application has the capability to mask such data as defined by HCLTech for the specified roles
- b. Vendor shall not copy HCLTech or HCLTech's customer data from production to non-production environments for any testing purposes. In cases where it is required to copy HCLTech or HCLTech's customer data from production to non-production environments for any testing purposes, vendor shall seek the approval of HCLTech before copying data production to non-production environments and part of the process of copying data, the sensitive data as defined by HCLTech will be anonymized prior to copying from production to non-production environments and the vendor shall demonstrate the evidence of anonymization.
- c. The data shall be anonymised in such a way that the original data is not traceable, or the anonymized data is not reversible.
- d. For cases where sensitive data in production shall be copied as-is to non-production environments, prior approval from the data owner in HCLTech shall be obtained

HCLTech Restricted

DO NOT CIRCULATE OR MODIFY WITHOUT PRIOR APPROVAL OF HCLTech RISK & COMPLIANCE

<b>HCLTech</b>	Technical and Organizational Measures (TOMs) for Vendor Security Requirements	Version 3.0
	Risk and Compliance	March 2025

## 15. Data Minimization

Vendor shall ensure:

- a. Vendor's application configures only such fields/ data elements as defined HCLTech and all other out of the box fields which is not required by HCLTech will be hidden and no data will be captured for such fields.
- b. Vendor's application will not expose HCLTech data to any other application (be it HCLTech application or any other third-party application) without the approval of HCLTech's data owner
- c. that the data consumed by vendor's application from other HCLTech applications (home-grown, other 3rd party or SaaS) is not shared further with any other HCLTech application (home-grown, other 3rd party or SaaS) without the approval of the HCLTech data owner of the source application.

## 16. Data Catalogue, Classification, Attribute Lineage and Quality

- a. For any HCLTech data stored or residing in vendor environment, applications or systems, the vendor shall co-operate with HCLTech for data discovery, classification and management of data:
  - o To maintain a structured inventory of HCLTech data assets provided to the vendor and
  - o Establish an appropriate integration mechanism to extract the HCLTech data attribute lineage.
  - o Establish a mechanism to extract the HCLTech data to measure the quality of data.
- a. Vendor shall:
  - o Permit data governance solution/tool used by HCLTech's to connect to vendor's environment to extract the metadata (i.e., database name, schema name, table name, view name, etc.), extract data attribute lineage and measure the quality of data
  - o In cases of no access to the solution/tool used by HCLTech, vendor shall provide at least once in 6 months:
    - A catalogue of metadata (where HCLTech data is stored) along with the business glossary.
    - Technical and business data lineage information at a system and data attributes level of its applications (where HCLTech data is stored) including upstream and downstream data sources.
    - Implement data quality rules as per current business standards and provide the data quality scores, data quality rules execution results.
  - o Make system enhancements to improve data quality scores.

## 17. Risk Management and Governance

Vendor shall ensure:

- a. Appropriate risk assessments shall be performed by vendor as part of an ongoing risk governance program that is established with the objective to recognize risk; to assess the impact of risk; and where risk reducing or mitigation strategies are identified and implemented, to effectively manage the risk with recognition that the threat landscape constantly changes.
- b. All risks and threats identified, as part of the risk assessment shall be prioritized, and action taken accordingly to mitigate the risks in a timely manner. The risk assessment shall also evaluate the susceptibility of assets/systems being used for HCLTech toward the advanced attack vectors.
- c. Notify HCLTech immediately if they are unable to remediate or reduce any material risk that could have an impact on the service being provided.

HCLTech Restricted

DO NOT CIRCULATE OR MODIFY WITHOUT PRIOR APPROVAL OF HCLTech RISK & COMPLIANCE

<b>HCLTech</b>	Technical and Organizational Measures (TOMs) for Vendor Security Requirements	Version 3.0
	Risk and Compliance	March 2025

### 18. Sub-Contracting Measures

Vendor shall ensure:

- a. The vendor shall not sub-contract any of its services that it is obligated to perform under the agreement without prior written consent of HCLTech. Vendor shall duly notify HCLTech point of contact defined in the Master Vendor Agreement or any SOW or Ordering/Transactional Document, regarding the engagement of any Subcontractor and shall seek appropriate consent from HCLTech.
- b. If vendor decides to change a sub-processor or to add a new sub-processor(s), vendor notifies HCLTech of the same (90) days in advance and HCLTech has the right to object to the appointment of sub-processor(s) on reasonable grounds.
- c. Where the vendor sub-contracts its obligations with the consent of HCLTech, it shall do so only by way of written agreement with the sub-processor(s), which imposes the same obligations on the sub-processor(s) as are imposed on the vendor under the agreement executed with HCLTech.
- d. Vendor due diligence is performed before on-boarding any third-party vendor or sub-contractor and periodic risk assessments are carried out post on boarding the third-party vendor or sub-contractor.
- e. Vendor shall be able to promptly procure and provide to HCLTech, any relevant information, for HCLTech to verify compliance by Vendor or its sub-contractors.
- f. Where the sub-processor(s), fails to fulfil its obligations under such a written agreement, the vendor remains fully liable to HCLTech for the performance of the sub-processor(s), obligations under such agreement.

### 19. Right to Audit

Vendor shall ensure:

- a. Vendor shall allow HCLTech or HCLTech authorized personnel to undertake an inspection/assessment of the control environment where the services are developed or provided to perform security compliance testing and/or assessments on at least an annual basis (or immediately following an incident).
- b. Vendor shall be responsible for the costs of remediating any security weaknesses identified by HCLTech in Vendor's control environment within a timescale as agreed by both Parties.
- c. Vendor shall not unreasonably withhold, or delay information requested by HCLTech or HCLTech authorized personnel that is necessary to support the investigation.

*<End of Document>*