HCLTech
VENDOR SECURITY REQUIREMENTS

Contents

Introduction

This document describes HCLTech's information security, business continuity, privacy practices, standards, and its program for assessing the information security and business continuity practices of its vendors and partners.

This Vendor Security Requirements Document is intended to inform Vendor of the information security, business continuity and privacy practices (as applicable) that HCLTech expects of its Vendor and to which Vendor will be held responsible. It is to be used in the provision of services to HCLTech only. Vendor should implement these requirements in accordance with industry best practices and their corporate security policies (ex: evaluating them in a non-operational environment if prudent) in consultation with a HCLTech representative. In no event will HCLTech be liable for vendor's inability to access information or for any damage vendor suffers, including, but not limited to, destruction of data or damage to vendor's equipment, whether such damage is direct, incidental, or consequential, and whether caused by mistake, omission, interruption, deletion of files or messages, errors, defects, delays in operation or transmission, failure of equipment or performance, negligence or otherwise. To the extent any inconsistencies exist between this Vendor Security Requirements Document and the negotiated terms in the written agreement between the Vendor and HCLTech, the language in such written agreement shall prevail.

Vendor who provides services that may be subject to local, national, regional regulatory and statutory requirements that affect compliance with certain of the HCLTech Standards set forth in this Vendor Security Requirements Document. In the event of a conflict between the requirements in the Vendor Security Requirements Document and any regulatory or statutory requirement applicable to a 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.

Overview of Vendor Security Requirements

HCLTech has a responsibility to protect its restricted and confidential information from unauthorized access or disclosure. For this, HCLTech implements internal information security, business continuity and privacy standards to ensure that such restricted and confidential information is protected and that the services provided by HCLTech are continuously available. To ensure HCLTech's compliance with internal standards and regulatory requirements relating to information security and business continuity, HCLTech requires that its Vendors adhere to HCLTech Standards. In turn, to the extent a Vendor delegates or subcontracts to a Vendor any portion of Vendor's obligations under its agreement with HCLTech, or engages a Vendor to provide services directly or indirectly to HCLTech, the Vendor shall require such Vendor to implement and administer an information protection program and plan that complies with HCLTech Standards. HCLTech is committed to working with its Vendor to help Vendor meet compliance requirements relating to HCLTech Standards. This document sets forth an overview of the HCLTech Standards with which Vendors are expected to comply and with which compliance may be evaluated through the Vendor Risk Assessment Program. The extent of the applicability of such HCLTech Standards to a particular Vendor will vary depending on the type of service and products provided by such Vendor to HCLTech.

Identity and Access Control

Vendor shall ensure:

- A documented access control policy is in place, and it's reviewed at least annually.
- User roles with their entitlements and access rights are defined and documented.
- Access to IT (Information Technology) infrastructure components are granted based on least privilege principle and are managed through robust identity management tools such as enterprise Active Directory solution or similar.
- Individual's access to systems, network resources and other IT resources is formally approved and controlled through unique User IDs and individual passwords.
- Policy and associated system configurations make certain that:
    - Users are required to change their password upon initial sign-on
    - Passwords meet the requirement set by the policy based on industry standard, including but not limited to length, expiry, complexity, password history, failed attempts, account lockout duration, password age, and change on first logon etc.
    - Generic and shared IDs are not used unless a formal justification is in place and is approved by senior management along with a mechanism to track the usage of such IDs and it is possible to trace the actions performed using those IDs to an individual.
    - Secure mechanisms are used to deliver user passwords
    - Validate user identities before initiating password resets
- Privileged access to resources is restricted to defined user roles and access to such roles are approved by authorized personnel.
- Privilege user accounts are configured to use multifactor authentication.
- Periodic access rights reviews are carried out and any identified exceptions are addressed promptly. Privileges that are no longer required are revoked immediately.
- Systems that do not support active directory authentication or are required to be built standalone are configured to enforce strong authentication which is no less than the configuration defined in central password and access control policies.
- Standard processes for user onboarding and deboarding are in place including keeping records of relevant approvals.
- Reconciliation of all user IDs (Including but not limited to, domain, applications, network devices, IT systems, middleware, databases etc.) is performed quarterly or as per industry standard and corrective actions to mitigate any identified exceptions are taken promptly.
- All systems, applications, network devices and IT infrastructure components are configured to use secure log-on procedures via approved identity and access management mechanism.

- Access to critical IT infrastructure, systems, network devices and applications such as remote access and access to critical servers, network devices etc. is protected using multifactor authentication mechanism.
- Solutions to prevent unauthorized changes to critical system files are implemented.
- Use of administrative credentials is restricted to limited circumstances such as troubleshooting purposes and users perform their day-to-day operations with least privileged credentials.
- Segregation of duties is maintained while creating/amending user IDs and allocating privileges.
- Vendor-supplied default credentials are changed before systems, applications, network devices or other IT infrastructure devices are put in production.
- All non-console administrative access is encrypted using industry approved encryption algorithms and insecure protocols such as telnet/ftp are prohibited for non-console administrative access.
- Third party vendor access to network and systems is strictly controlled and should be based on the need to know and formal approval basis.
- Systems and applications are configured for idle session time out to prevent unauthorized access.

Asset Management

Vendor shall ensure:

- Asset labelling, information classification policy and supporting procedures/guidelines are maintained. All assets are labelled as per labelling instructions and information is classified and protected as per the classification levels.
- Asset inventories are maintained, capturing all required details such as asset owner details, contact information, location etc.
- Asset management procedures and configuration controls to manage the availability of critical assets and the configurations of critical network and information systems are established and maintained
- Records of Information Technology assets (Hardware, OS, applications & database etc.) are maintained and periodic reviews are performed to keep the list accurate and up to date.
- Policies and procedures for controlling mobile devices (Including BYOD) used to store, transmit or process business information are in place. Ensure adequate level of protection

is in place before allowing mobile devices to have access to business information and resources.

- Acceptable usage policy and asset management guidelines for handling assets are maintained and communicated to all applicable employees and contractors.
- Processes are in place to confirm allocated assets to an employee/contractor is returned without undue delay to the corresponding asset management team upon termination/separation of employment, contract, or agreement.
- Use of removable mass storage devices is prohibited by default and any exceptions are recorded and formally approved with proper business justification.
- Documented procedures are in place for safeguarding information assets, identification of assets due for disposal and for secure disposal of such assets.
- Use of unlicensed/ unapproved software is prohibited, and processes are in place to identify any violations and take necessary actions to address such violations.

IT Operations

Vendor shall ensure:

- Procedures for the operation of critical networks and information systems by personnel which include but is not limited to the following are established and maintained:
  - Formal approval to access the IT assets/technology.
  - Robust authentication mechanism for use of all technologies such as VPN, Windows logon etc.
  - Review of privilege entitlements
  - Network locations are identified for critical technologies based on business continuity requirements
  - Processes to ensure only company approved software are used
  - Data retention requirements are identified, documented, and complied with
  - Standard operating procedures (SOP's) and configuration standards are defined for all systems, applications, tools, and technologies.
- Change management processes are established 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. The change management plan includes the rollback of changes if the proposed changes have a negative impact. Records of all change are maintained.
- File Integrity monitoring checks are in place for systems and network components handling sensitive and confidential information.

- Processes are in place to monitor the available capacity of systems and applications to identify resource requirement for the IT environment.
- Backup policy and supporting procedures are clearly documented. Data backups are taken periodically using a secure and reliable mechanism. Backup restoration processes are documented, and restoration of data is tested at defined frequency and corresponding evidence is maintained. A copy of critical data backup files is kept in secure offsite location(s).
- Information in backup media or storage appliance is encrypted using strong encryption algorithm.
- Logs for failed backups (if any) are monitored by backup admin and corresponding corrective action is performed and documented.
- Hardening baselines for all its IT infrastructure components are defined and documented. The Operating Systems, databases, applications, and network devices etc. are configured as per respective hardening baselines before introducing them to the production environment.
- Systems and network components are configured to use authorized Network Time Protocol (NTP) source for time synchronization.
- Processes are in place for proactive and preventive maintenance of all critical systems, applications, network devices and end user machines at regular interval.
- Firewall and router rule set reviews are conducted on a quarterly basis or as per industry standard and any unnecessary or unauthorized rule sets are removed immediately.
- Controls are in place to maintain the integrity of information and software.
- Controls are in place for redundancy in IT Infrastructure such as redundancy of LAN, WAN, servers, workstation, and IT Infrastructure etc. to ensure continuity of operations.
- Controls to facilitate secure internet browsing for end users e.g., through web proxy, web content filter etc., are in place.

Human Resource Security

Vendor shall ensure:

- Policy and procedures for background checks are established and maintained.
- Appropriate background checks are performed on personnel (employees, contractors, and third-party users) before they are onboarded and to the extent legally permitted for their duties and responsibilities.

- A program for training and awareness is implemented to make sure all personnel have sufficient and up-to-date information security knowledge.
- All personnel undergo information security and data privacy training at the time of joining and at least annually thereafter.
- Security and personal data protection knowledge of all personnel is tested.
- Training and awareness program is reviewed and updated periodically, taking into account changes in business requirements, legislation, and based on past incidents.
- An appropriate process for managing changes in personnel or changes in their roles and responsibilities and to educate new personnel on the policies and procedures is in place.
- Following changes in personnel, access rights, badges, equipment, et cetera are revoked if no longer necessary or permitted.
- A disciplinary process for employees who violate security policies is established and maintained either standalone or as part of a broader process that covers security breaches caused due to violations by personnel.
- Personnel are held accountable for violating security policies, for example via employment contracts, third party contracts, etc.

Information Security & Governance

Vendor shall ensure:

- Vendor has an established security standard framework for information and cyber security governance which covers the following components:
    - Information and Cyber Security policies and procedures which are reviewed (at least annually), approved and communicated
    - An information security strategy
    - Governance and risk management processes which address information and cyber security risks
    - Legal and regulatory requirements regarding Information and Cyber Security
- Appropriate roles and responsibilities for Information and Cyber Security are defined and implemented.
- A Chief Information Security Officer (or equivalent) is appointed who is sufficiently senior and has responsibility for Vendor's information security program.
- A committee or equivalent body (e.g., information security steering committee) is established which coordinates information security activities across the vendor and is chaired by a suitably senior member of staff and meets on a regular basis.

- Information security objectives and associated activities to ensure commitment towards Information security management systems (ISMS) are identified and documented and an Information security management system is established which is aligned to meet the information security objectives of the organization.
- Processes and/or tools are in place to identify events that cause interruptions to organizations key business purpose.
- Critical systems are protected against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
- Vendor is certified with the latest Payment Card Industry Data Security Standard if it stores/processes/transmits Payment Card Data on behalf of HCLTech or HCLTech's customer.
- A formal risk management framework approved by Sr. Management is in place for:
  - Identifying both internal and external threats
  - Sensitivity of information / data in scope
  - Assessing potential business impacts
  - Assessing Threats, vulnerabilities, and corresponding risks
- All risks and threats identified as part of the risk assessment are prioritized and action taken accordingly to mitigate the risks in a timely manner.
- Notify HCLTech immediately if they are unable to remediate or reduce any material risk that could have an impact on the service being provided.
- The Vendor obtain and maintain cyber liability insurance covering claims related to violation of any applicable privacy rule(s), privacy and data protection laws, or regulation concerning the privacy of HCLTech Information and claims, and if applicable based on obligations pursuant to the Data Processing Vendor Security Agreement (DPVSA) available on hyperlink, with coverage of not less than one million US Dollars (USD 1,000,000) per occurrence.

Network Security

Vendor shall ensure:

- The vendor network is designed using "defence in depth" principles to ensure information and cyber security breaches are minimized by ensuring appropriate controls such as network segmentations are in place.
- External connections to the network are documented, routed through a firewall, verified, and approved prior to the connections being established.

- Design and implementation of the network is reviewed at least annually.
- All wireless access to the network is subject to authentication, authorization, segmentation, and encryption protocols. Mechanisms are in place to detect and respond to presence of rogue wireless access points/unauthorized connection to wireless network.
- Communications between network devices and workstations used for management of such devices are secure.
- Non-console administrator access is over an industry approved encrypted channel.
- Strong architectural design with effective identity management and operating system configuration are used.
- Services, applications, and ports that are not in use are disabled.
- Appropriate measures are in place for intrusion detection and/or prevention for critical network segments.
- Guest accounts are disabled or removed, and all default and vendor supplied passwords are changed before network devices are commissioned in the production environment.
- Network is configured to meet all applicable legal and regulatory requirements
- Implement controls to prevent/minimize unauthorized individuals from gaining access to the Vendor Network.
- Any remote access to vendor network must be approved and must be over an encrypted Virtual Private Network (VPN) connection configured with Multifactor authentication.

Cryptography

Vendor shall ensure:

- Policy and supporting procedures for cryptographic controls required to comply with all applicable legal, regulatory, and business requirements are established.
- Use of only secure and industry approved encryption algorithms and key strengths which assure adequate protection of data is permitted.
- Passwords are always encrypted when stored and during transit.
- Key Management procedures for secure key generation, ownership, distribution, archival, storage, and revocation to protect keys throughout the life cycle are established and maintained.
- Cryptographic solutions based on industry best practices to enable secure encryption and in line with applicable laws and regulations are implemented to make sure confidential information is protected and access to sensitive data is restricted e.g., encryption of data during transit and while at rest.

Data Security

Vendor shall ensure:

- Systems, applications, and networks components that process, store, and transmit HCLTech or HCLTech Customer's data are protected against data leakage using a combination of tools such as centrally administered data leakage prevention tool, log and file integrity monitoring and auditing tool etc. to prevent unauthorized disclosure of confidential Information. All events triggered by the data leakage prevention system are reviewed by the central Security Operations Centre (SOC) team.
- Full disk encryption is configured for workstations and servers.
- Documented data classification policy is in place and data is classified based on its criticality and sensitivity. Security controls corresponding to sensitivity of data are identified and implemented.

Information Communication

Vendor shall ensure:

- Controls e.g., Web Content filtering software are in place to prevent access to websites hosting malicious content. Security controls are in place to prevent misuse of email system and ensure all email communications are over an encrypted channel.
- Anti-phishing and Anti-Spam filters along with other configurations such as Spoof protection etc. to prevent email bound threats are enabled on the email gateway.
- Access to all systems and applications is over a secure and authenticated mechanism, and client server communication of applications and web portals is over an encrypted channel.

Software Development

Vendor shall ensure:

- An established Software and Systems development framework is in place.
- Systems and applications are developed in line with Secure Software Development best practices (e.g., OWASP). Software code is protected from unauthorized modification and is securely stored and subject to Quality Assurance.
- Applications are thoroughly tested for security and functionality related issues before deploying them in the production environment.
- Production and non-production environments are segregated appropriately.
- Live data is not used in test environment unless prior approval from the data owners and controls corresponding with the production environment are in place.
- Segregation of duties between production and non-production developments is maintained.

Application security

Vendor shall ensure:

- Application security assessments are performed for all newly developed applications and any existing applications that are going through a significant change to identify any known security vulnerabilities.
- All security vulnerabilities identified with CVSS score greater than 4 are mitigated prior to deployment of application in the production environment.
- Strong authentication mechanisms are used, and periodic access rights reviews are performed.
- Application developers are trained in secure coding techniques and such training is conducted on an annual basis at least.

- Code review processes are in place to identify and correct any code that may lead to security vulnerability.
- Public facing web applications are protected by a robust web application firewall.

Patch Management

Vendor shall ensure:

- Latest security patches are applied to systems, Networks, applications, and databases etc. in a timely manner and based on criticality of the vulnerability addressed by the patch. Patches are obtained from respective OEMs directly for proprietary systems.
- Patches are either digitally signed or verified via the use of a vendor hash for the update package to ensure that the patch can be confirmed as coming from a reliable support community for open-source software.
- All patches are tested before deployment of the patches to production systems and the correct operation of the patched service are verified after any patching activity.
- Appropriate mitigations are in place if a system cannot be patched, effectiveness of such mitigations is assessed periodically, and corresponding evidence maintained

Malware Protection

Vendor shall ensure:

- All IT systems are protected in real time by a malware protection solution which inspects all data for malware to prevent service disruption or security breaches and ensure that appropriate user awareness procedures are implemented. Anti-malware to include detection for (but is not limited to), viruses, spyware, worms, unauthorized mobile code, key logger software, botnets, worms, trojans etc.
- Malware signatures are updated on a regular basis to ensure systems are using the latest definitions.
- Malware protection software is configured to run scheduled as well as on demand scans and to isolate/delete any malicious files or software.
- End users are not provided with rights to disable malware protection.

Vulnerability Management

Vendor shall ensure:

- Established policies, processes, and procedures for vulnerability management are in place.
- Roles and responsibilities for vulnerability management program are documented and appropriate tools such as vulnerability scanning systems and Intrusion Detection Systems are implemented.
- Critical systems, IT assets, and network activity are routinely monitored to detect potential cyber security events such as unauthorized connections, unauthorized software / applications etc.
- There are processes established to receive, analyse, and respond to vulnerabilities disclosed to the organization from internal and external sources.
- Identified vulnerabilities with CVSS score greater than 4 are remediated within defined timelines.
- An independent penetration test at least annually and vulnerability assessments at least on a quarterly basis are performed on vendor's IT infrastructure and applications used to provide services to HCLTech including disaster recovery sites to identify vulnerabilities that could be exploited to breach data/services and to prevent against any security breaches through Cyber Attacks.
- On reasonable request Vendor allows HCLTech to have access to penetration/vulnerability test reports relevant to the services being provided.

- Only approved scanning and diagnostics tools with securely configured management console/ports are permitted.
- Access to Scanning/audit tools are restricted to relevant vendor personnel and their use is monitored.

Logging and monitoring

Vendor shall ensure:

- There is an established and consistent audit and log management framework implemented.
- Critical systems including applications are set to log key events (including
- those of privileged access and user activity) and retain such for a minimum period
- of 1 Year or as per applicable regulatory requirements.
- As a minimum the logs (as appropriate) contain the following events:
  - System start-up and shutdown
  - Start and stop status of critical services and processes
  - Changes in the configuration parameter e.g., changes in system boot configuration
  - Successful logins and Failed login attempts
  - Creation, modification, and deletion of user accounts.
  - System/resources accessed
  - Identification and location of who accessed the resources and from where
  - Date and timestamp
- Audit logs are collected and correlated from multiple sources and sensors and stored securely and are tamper-proof to enable the reconstruction of such events.
- Processes for monitoring log events (preferably real time) are established to detect any unauthorized activities, attack targets, and ensure that logs of key events are reviewed by an independent function (e.g., Security Operations Centre) daily.
- Incident alert thresholds are configured to determine the impact of any events and ensure such events are responded to in a timely manner as per the criticality of the alarm.

Incident management

Vendor shall ensure:

- Documented incident management policy and associated procedures are in place for management of security incidents.
- Responsibilities and practices for ensuring a quick, effective, and orderly response to information security and privacy incidents are defined and established.
- Employees and contractors are educated in what qualifies as a security incident and where and how to report any such potential or confirmed security incidents.
- Employees responsible for analysing and responding to incidents are qualified in the subject matter and are periodically trained on how to effectively respond to incidents.
- Repository of all reported incidents is maintained along with the actions taken to mitigate the impact of the incident and lessons learnt.
- HCLTech is notified immediately after becoming aware of the security incident impacting HCLTech, but no later than 24 hours.

Compliance

Vendor shall ensure:

- Processes are in place to identify, record, and track all applicable legal, regulatory, and contractual requirements for the organization.
- Periodic assessments are performed to validate compliance with legal, regulatory, and contractual obligations. Records are maintained for such assessments and identified gaps are mitigated without undue delay.
- Policies, procedures, and guidelines are reviewed at least annually and updated as per the legal, regulatory, and contractual requirements.
- Key Performance Indicators for critical functions such as IT, Information Security and Data Privacy etc. are defined, formally documented, periodically assessed, and reported to Sr. management.

Physical and Environmental Security

Vendor shall ensure:

- Policy and associated procedures for physical security measures and environmental controls based on Industry standard implementation of physical and environmental controls are implemented.
- All critical facilities and locations which house the important IT systems, applications, and personnel (e.g., data centres, operational facilities) are physically protected against accidents, attacks, and unauthorized access etc.
- Security controls such as electronic access controls, Identity verification, security guards, visitor management and 24x7 CCTV monitoring etc. are in place to protect the buildings against unauthorized access.
- CCTV recordings are retained for a minimum of 30 days or as per legal and regulatory requirements applicable to the vendor.
- Access to facilities is restricted and only granted for specific and authorized purposes and is subject to regular reviews.
- All visitors are escorted while inside the premises and the entry and exit times are logged and monitored. Visitors are issued Visitor IDs are required to be always worn while inside the premise. ID/Access cards or keys issued to visitors should be collected at the time of their departure from the premises.
- All critical facilities and locations are physically protected against loss of power to prevent any interruption in service. Critical facilities are protected by uninterruptible power supply (UPS) or generators to support operation in case of a prolonged power loss.
- Periodic maintenance of all critical equipment like Generators/UPS/smoke detectors/fire extinguishers/fire suppression systems, access control systems is performed, and records of such maintenance are maintained.
- 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, flood detection sensors, fire extinguisher systems etc. to protect against fire, the weather, flooding, and other natural hazards.
- Mechanisms for secure disposal of data in hard and soft copy format are defined and implemented. Cross cut shredders are used for disposing off paper documents, and use (where appropriate) methodologies such as sanitization, Degaussing and physical destruction for shredding of electronic media.
- A clear desk policy is in place to ensure secure disposal of Post It notes, keeping written notes in a safe place, and ensuring that any removable media isn't just lying around.

- Effectiveness of physical and environmental controls are evaluated at least annually.

Privacy and Data Protection

If the Vendor or its sub-processors processes personal data on behalf of HCLTech or HCLTech's customers, Vendor shall ensure the following:

- Compliance with all applicable data protection laws.
- An established privacy management framework is in place which covers the following components:
  - Privacy policies, statements, notices, and procedures which are reviewed (at least annually), approved and communicated
  - Privacy Governance and risk management processes which address personal data risks
  - Legal and regulatory requirements regarding data privacy
- Up-to-date records of processing activities for all personal data processing activities performed on behalf of HCLTech are maintained.
- Appropriate roles and responsibilities for Data Privacy are defined and implemented.
- A Data Privacy Officer (or equivalent) is appointed who is sufficiently senior and has responsibility for Data Privacy Program.
- A committee or equivalent body which coordinates Data Privacy Compliance activity across the vendor is in place and is chaired by a suitably senior member of staff and meets on a regular basis.
- A specialist Data Privacy function with suitable and defined roles and responsibilities is in place.
- In particular, implement administrative, physical and technical safeguards to protect HCLTech's or its customer's information that are no less rigorous than accepted industry practices (such as ISO/IEC 27001:2013 – Information Security Management Systems – Requirements and ISO-IEC 27002:2013 – Code of Practice for International Security Management, The Control Objectives for Information and related Technology (COBIT) standards [or] other applicable industry standards for information security), and ensure that all such safeguards, including the manner in which the information is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of the Data Processing Vendor Security Agreement(DPVSA), if applicable.
- If the processing involves sensitive personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or

biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences or any other data types considered sensitive personal data with regards to applicable data protection law, the Vendor apply specific restrictions and additional safeguards to protect sensitive personal data e.g., by implementing encryption, pseudonymization techniques etc.

- Access to personal data and associated application and systems is restricted to authorized individuals on a need to know and least privilege basis. The access rights of employees supporting the processing activities are promptly removed upon termination of their employment or upon their separation from HCLTech engagement or when their roles have changed. In addition, periodic access rights reviews are performed to identify and correct unnecessary permissions timely to prevent misuse.
- All persons authorized to process the Personal Data (including any Vendor Affiliates) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality in relation to such Personal Data.
- Taking into account the nature of the Processing, Vendor assists HCLTech by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of HCLTech's obligations, to respond to requests for the exercise of Data Subject rights under the Data Protection Laws.
- If Vendor or any of its Sub-Processors pursuant to the DPVSA receives a Data Subject rights request from a Data Subject under applicable Data Protection Law in respect to HCLTech Personal Data, Vendor notifies HCLTech promptly and no later than two (2) days of receiving such request; and
- Vendor and any of its Sub-Processors pursuant to the DPVSA shall not respond to a Data Subject Request except on the documented instructions of HCLTech unless as required by Data Protection Laws to which the Vendor and/or the Sub-Processor is subject, in that case Vendor shall to the extent permitted by Data Protection Laws inform HCLTech of that legal requirement before the Vendor or its Sub-Processor responds to the request.
- Notify HCLTech at privacy@hcl.com, as soon as possible, but in no event later than 24 hours from becoming aware of a personal data breach involving HCLTech personal data.

Sub-Contracting Measures

Vendor shall ensure:

- The Vendor does not sub-contract any of its services that it is obligated to perform under the agreement without prior written consent of HCLTech.
- If Vendor decides to change a Sub-processor or to add a new Sub-processor, Vendor notifies HCLTech within (90) days in advance and HCLTech has the right to object to the appointment of Sub-Processor on reasonable grounds. The objection shall be notified by HCLTech to the Vendor within (30) days following the Sub-processor Change notice specifying the reason for the objection.
- 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-contractor(s) which imposes the same obligations on the sub-contractor(s) as are imposed on the Vendor under the Agreement.
- Vendor due diligence is performed before onboarding the third-party vendor and periodic risk assessments are carried out post onboarding the vendor.
- Where the sub-contractor(s) fails to fulfil its obligations under such a written agreement, the Vendor remains fully liable to HCLTech for the performance of the sub-contractor's obligations under such agreement.

Cloud Security Measures

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, Vendor shall ensure:

- An established framework is 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 latest version of the Cloud Security Alliance, Cloud Controls Matrix (CCM) or ISO27017.
- Security measures are implemented across all aspects of the service being supplied, such that it safeguards confidentiality, availability, and integrity by minimizing the opportunity of unauthorized individuals (e.g., other cloud customers) from gaining access to HCLTech Information and the services utilized by HCLTech.

Business Continuity Management

Vendor shall ensure:

- A formal Business Continuity Management (BCM) Policy, plan and associated procedures capturing business continuity objectives are established, reviewed, and approved at least annually.
- A BCM testing framework is developed and implemented to validate effectiveness of the business continuity strategies implemented.
- A formal BCM training and awareness program is implemented.
- Business Impact analysis (BIA) & Risk assessments (RA) are performed at least annually or following a significant change.
- A crisis management plan (including pandemic preparedness) is established to ensure appropriate responses to emergency situations by enabling the protection of employees, visitors, the environment, assets, and business operations.
- Periodic testing of the effectiveness of Business Continuity Management System is performed on an annual basis and records are maintained of such testing.

Right to Audit

Vendor shall ensure:

- Vendor allows 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).
- Vendor is 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.
- In the event of a security incident the vendor fully cooperates 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.
- 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>