HCL Software – Information Security Practices

Protecting Customer Data

www.hcltechsw.com

POLICIES, STANDARDS, CERTIFICATIONS, AND AUDITS OF CONTROLS.

HCL Software implements a robust Information Security Management System (ISMS) which provides Policies and Procedures that regulate the use of information, including its processing, receipt, transmission, storage, distribution, access and deletion ("Policies and Procedures"), are documented and implemented, and address how confidential information is managed, and protected. The Policies and Procedures are approved by senior management, reviewed and updated to remain compliant with the law and current industry practices.

Security Training

- **Annual Security Training is mandatory for all employees**
- **Security Training covers all aspects of Information Security as per the policies in our ISMS**

Risk Management

HCL Software implements an industry standard Risk Management Program with continuous risk monitoring which includes communication with stake holders at regular intervals. It utilizes a Risk Management methodology to identify assets with value to the business, to understand possible threats and how threats can impact the assets value resulting in business risks.

- **Risk Management Policy, Procedure and Guidelines**
- **Annual Risk Assessments**
- **Central repository for Risks**
- **Management oversight and approval**
- **Monthly Risk Management Review of Risks and Risk Treatment Plans**
- **Security Team review of Security Risk Mitigations**

Compliance

Audits are conducted yearly

HCL SW data centers which may house Customer data received through support or services interactions are ISO27K certified for security controls.

ISO Certification

HCL SW maintains ISO27K certification and an ISO20243 certification. All certs are available here.

SECURITY BY DESIGN

Secure Code Development

All HCL Software Development Teams are required to follow our Software Development Lifecycle (SDLC) and our Secure Engineering Framework (SEF).

- **Static, Dynamic and Interactive Scanning** – Analyzes source code in order to locate vulnerabilities and bad coding practices.
- **Open Source Scanning** – Scans the Product to create a list of open-source code in the product and identifies vulnerabilities.
- **Internal & 3rd Party Penetration Testing** – Authorized simulated cyberattack, performed to evaluate the security of the system/product.
- **Developer Training** – Education on the SW Development Lifecycle (SDLC) & the Secure Engineering Framework (SEF) are mandatory annual requirements.
- **Risk Assessment & Threat Modelling** – Predictive Threat index (PTI) determines what secure engineering activities need to be included, develop Threat Models to minimize security exposure and risk
- **Rigorous Ship Criteria** – Security status at time of ship (outstanding vulnerabilities, any unresolved issues) documented and approved by stakeholders
- **Comprehensive Documentation** – Document all product security functionality throughout the SDLC

Secure Code Release

Prior to release of any product to our Customers, Static, Dynamic and Interactive scanning is performed. Penetration testing is performed annually on each product. Any identified vulnerabilities are tracked via our defect tracking system and remediated in a timely manner per HCL SW remediation timelines.

DATA PROTECTION OVERVIEW

Access to Customer Data
HCL Software may obtain Customer data through a support case.

What Type of Data Does HCL SW Support Collect?
HCL SW Support collects 3 types of data:

Customer Contact Information: To communicate with you, our customer, HCL Software Support maintains a record of Company and Contact details that include, but is not limited to, Company Name, Company address, Contact Name, email address, and telephone number.

Case data including Customer Contact data: The communication data would be any information that the you enter in the support portal itself during the lifetime of the case (for example, description of their problem, communication back and forth with HCL support team to troubleshoot the issue).

Diagnostic data: To effectively respond to your support queries, information between you and HCL Support needs to be shared. You may upload data, like log and configuration files, for Support to use in troubleshooting reported problems.

The 3 different types of data are divided into two groups. Each group has slightly different handling in the communications.

Case data including Customer Contact data: HCL Support keeps Customer Support related information in our Ticket Management System, which is hosted by an accredited external company on servers in Canada. The communication is done via HTTPS and uses the support TLS protocols. This backend database is encrypted.

Diagnostic data: The data is sent via SFTP or HTTPS using supported TLS protocols.

Where is My Data Located and How is it Stored?
Case data including Customer Contact data: HCL keeps Customer Support related information in our Ticket Management System, which is hosted by an accredited external company on servers in Canada.

Diagnostic data: HCL Support diagnostic data is housed in what we call the Customer Data Repository. The data is encrypted once on the HCL servers. The database encryption algorithm is AES (Advanced Encryption Standard 360bit) This is hosted in Bangalore, India. The data may be decrypted and downloaded to our HCL Support standard data analysis environments using HTTPS and using supported TLS protocols. These environments are hosted in our secure internal data centers across US, India, and Italy, or leverage secure zones on AWS and are used by our worldwide support engineers.

HCL Support diagnostic data is deleted within 30 days of case closure. You can manage your case data through the HCL Support portal, for example, you can view your open and closed cases. You can also manage your Support profile through the portal UI. Your Support Admin can manage contacts on the account, for example, add or remove or change permissions on the contacts associated with your account.   If additional changes or updates are needed on the account, a case can be submitted by your account admin.

How Long is my Data Stored on HCL Systems and Can I Ask for it to be Removed or Deleted?

Case data including Customer Contact data: HCL keeps personal information Customer Support related information active for 2 years. After 2 years, the contact person information is anonymized and the data is archived for up to 3 additional years. Anonymized case data may be kept longer to help with product improvement.

Where Are HCL Software Support Personnel Located?

HCL SW Support is a worldwide organization with sites and people working out of various locations, including, but not limited to, North and South America, Europe, India, Australia, China and Japan.

Does HCL Software Share Your Information Outside of Support?

Support may share your information in the following ways:

Within HCL Software:

- **By working with Development and Product Management, Support may use your reported problem details to understand how the product is being used and to improve the product.**
- By working with colleagues who help administer or support internal systems, Support may internally share your account name in order to address an administrative issue such as an entitlement or registration problem
- We may work with other colleagues who will help resolve your concerns

With Third Parties:

- **By working with you and a third-party, Support may, for the purpose of troubleshooting a problem which involves software for such third-party (for example, a third-party database vendor)**
  - **Help instruct you on the appropriate method for directly sharing data with such third-party**
  - **Obtain your consent to share your company name with such third-party in order to help such third-party review any historical information which could benefit problem determination**

Physical Security

HCL Software maintains and administers the following physical access controls:

- All facilities require badge access for employees and contractors. Visitor access must be logged in a physical access log. Visitors are escorted through restricted areas in the facility.
- All data centers where Customer data is processed or stored are further protected by security guards and monitoring cameras (e.g., CCTVs) 24/7.

Employee Security

HCL SW Employees and contractors are subject to background checks prior to being offered employment or given access to HCL SW facilities and systems.

Authorized User Names, Passwords and Authentication

HCL Software monitors access rights to ensure access adheres to stringent privilege principle in line with the employee’s job responsibilities.
In HCL Software, passwords are administered in the following manner:

- Passwords are not shared
- Password policy is to reset every 45 days
- Repeated (failed) access attempts are limited to 5 attempts with a 30 minute minimum lockout duration
- Initial password change is required

Passwords must have minimum length of 8 characters including alpha numeric and special characters. We use 15 characters for root and administrators.

Enterprise Role-Based Access

Logical access procedures define the request, approval, access provisioning and de-provisioning processes. The logical access procedures restrict user access (local or remote) based on user job function for applications and databases (role/profile based appropriate access) for applications, databases and systems to ensure segregation of duties and are reviewed, administered, and documented based on on-boarding, resource re-assignment or separation. User access reviews are performed to ensure access is appropriate throughout the year.

All HCL Software system administrators are authenticated using multi-factor authentication, Tacacs, VPN, AD for system access through privileged access management.

In addition, the use of privileged access management is recorded for audit and forensic analysis.

NETWORK SECURITY MANAGEMENT

Network Controls

HCL Software utilizes firewalls and DMZ for access control between our production and development networks and the internet.

Firewall access is granted to selected network administrators. Login based on individual ID and authentication is controlled by AAA, Tacacs, AD, and LDAP groups. By default, the firewall is implemented to deny all access.

Periodic network vulnerability scans are performed, and any critical vulnerabilities identified are promptly remediated. In addition, penetration tests are also performed by security professionals, both HCL Software employees and independent third parties.

Network/Communication Security Policy/Encryption

Access list is implemented in order to control the network traffic and reduce network attacks. Subnetting is taking into consideration to provide access on the need to know basis.

Customer data is encrypted while in transit over any public network or wireless network via S2s VPN tunnel with supported encryption level. HCL Software uses secure protocol to transmit and receive flat files (SSH / SFTP / SCP).

HLC SW utilizes an information protection and control solution that is designed and administered to minimize the accidental, negligent and malicious misuse of data through email and other communications aimed outside of HCCL SW firewalls (e.g., a data loss prevention (DLP) solution).

Remote Access Administration

The following remote access settings are applicable:

- Unauthorized remote connections from devices (e.g., modems) are restricted with Tacacs+ and ACCLs
- The data flow in the remote connection is encrypted and multi-factor authentication is enabled
- Remote connection settings limit the ability of remote users to access both initiating network and remote network simultaneously (no split tunneling).
- Remote device connections are based on conditional access rules to ensure only HCL managed devices are able to connect to user approved internal networks

Firewalls

All connections to HCL SW networks, including internet and partner connections are protected with a pair of firewalls using industry best practices fo configuration. All firewalls are monitored and scanned continuously via IDS/IPS.

Intrusion Detection and Protection

HCL SW uses continuous, active and passive intrusion detection and protection techniques. Firewall is enabled with all active licenses. These tools check for updates at least daily. Log files are maintained (for a maximum of 6 months) months from the date created, protected from alteration and checked continuously for signs of unauthorized access. HCL SW monitors all activity on the network and all activity inside their servers for suspicious activities.

Wireless Policy

HCL SW networks are secured to industry standards, including but not limited to, the use of WPA2 enterprise secure configuration of wireless access points; and continuous detection of unauthorized network devices.
Users are authenticated via LDAP/AD and Radius group

In addition, the use of privileged access management is recorded for audit and forensic analysis.

SECURITY INCIDENTS

HCL SW rehearses and maintains a confidential Cybersecurity Incident Management & Response Plan designed utilizing industry best practices to detect, analysis, isolate, eradicate, recover and communicate cybersecurity incidents.

COMPLIANCE WITH DATA PRIVACY LAWS

HCLs privacy statement is available on our website

BUSINESS CONTINUITY AND PANDEMIC PLANNING

Business Continuity & Disaster Recovery Planning

A. Backup Procedures
Backup procedures are applied to critical development systems. Backup is done at the storage level and industry standards are followed. .
Each Data Center has its own backup infrastructure.

B. Interruptions and Outages
Outages are communicated. Communication includes the following:

- Nature of impact
- Locations / Departments / Process impacted
- Extent of impact
- Location and contact information of the IT helpdesk
- Location and contact information of recovery coordinator responsible for recovery activities

Penetration Testing

Product Security

HCL takes the security of our products seriously. In addition to traditional penetration testing exercises, we work with development teams, build engineers, and release management to ensure security activities are implemented throughout the SDLC and software assurance is embraced as an organization.

During the development stage, automated tests are run to deliver instantaneous feedback to the developer. When code is merged, peer review assures multiple eyes are reviewing the code for security issues. In the Test environment, static code analysis and software composition tools are run to detect common vulnerabilities as well as components using libraries with known vulnerabilities. When the release candidate passes these tests, it is subject to dynamic scanning to test for runtime vulnerabilities. Finally, manual comprehensive penetration testing is conducted internally before each major release, or at least annually. In addition to internal penetration testing, it is an HCL Software policy that all applications undergo a third-party penetration test on at least an annual basis.

All discovered vulnerabilities are subject to a Service Level Objective, which is a time frame in which remediation is mandated according to the criticality rating.

Infrastructure Security

Automated scans are conducted on our network infrastructure on a monthly basis. This includes internal infrastructure, development environments, and production environments. Assets within scope include, but are not limited to, servers of all kinds (application servers, database servers, DNS servers, mail servers, etc.), network devices, laptops, and desktops.

In addition to automated scanning, it is the policy of HCL Software that all networks undergo a manual network penetration test by a third party at least annually.

Encryption

Encryption Policy. Encryption use and applicable encryption standards are documented. The encryption strength of confidential information in transmission is defined.

File/Data Type	Cipher	Encryption Algorithm	Strength
Flat (ASCII) files	Symmetric Block	AES	256 bits, TLS 2.1
Database Table	Symmetric Block	AES	256 bits, TLS 2.1
Backup/Tape	Symmetric Block	AES	256 bits, TLS 2.1
Other	Symmetric Block	AES	256 bits, TLS 2.1

Network Controls

HCL SW utilizes firewalls and DMZ for access control between our networks and the internet.

Firewall access is granted to selected network administrators. Login based on individual ID and authentication is controlled by AAA, Tacacs, AD, and LDAP groups. By default, the firewall is implemented to deny all access.

Periodic network vulnerability scans are performed, and any critical vulnerabilities identified are promptly remediated. In addition, penetration tests are also performed by security professionals, both HCL SW employees and third parties.

Network/Communication Security Policy/Encryption

Access list is implemented in order to control the network traffic and reduce network attacks. Subnetting is taking into consideration to provide access on the need to know basis.

Customer data is encrypted while in transit over any public network or wireless network via S2s VPN tunnel with AES256 encryption. HCL SW uses secure protocol to transmit and receive flat files (SSH / SFTP / SCP).

HLC SW utilizes an information protection and control solution that is designed and administered to minimize the accidental, negligent and malicious misuse of data through email and other communications aimed outside of HCL SW firewalls (e.g., a data loss prevention (DLP) solution).

Remote Access Administration

The following remote access settings are applicable:

- Unauthorized remote connections from devices (e.g., modems) are restricted with Tacacs+ and ACCLs
- The data flow in the remote connection is encrypted (AES 256) and multi-factor authentication
- Remote connection settings limit the ability of remote users to access both initiating network and remote network simultaneously (no split tunneling).

Firewalls

All connections to HCL SW networks, including internet and partner connections are protected with a pair of firewalls using industry best practices for configuration. All firewalls are monitored and scanned continuously via IDS/IPS.

Intrusion Detection and Protection

HCL SW uses continuous, active and passive intrusion detection and protection techniques. Firewall is enabled with all active licenses. These tools check for updates at least daily. Log files are maintained (for a maximum of 6 months) months from the date created, protected from alteration and checked continuously for signs of unauthorized access. HCL SW monitors all activity on the network and all activity inside their servers for suspicious activities.

Wireless Policy

HCL SW networks are secured to industry standards, including but not limited to, the use of WPA2 enterprise secure configuration of wireless access points; and continuous detection of unauthorized network devices.
Users are authenticated via LDAP/AD and Radius group

In addition, the use of privileged access management is recorded for audit and forensic analysis.

Data in Transit

TLS (Transport Layer Security) encryption is required for all Internet connections during login and all data shall be encrypted during transmission.

Data at Rest

Stored client data is encrypted. Key Management conforms to industry best practices. Encryption leverages AES 256 standards.

Encryption Key Management. Cryptographic key management procedures are documented and automated. Products or solutions are deployed to keep the data encryption keys encrypted (e.g., software- based solution, Hardware Security Module (HSM)). This is software-based Encryption, Key Management procedure will be automated.

Encryption Uses. Confidential information transmission over the public internet always utilizes an encrypted channel. Encryption details are documented if transmission is automated. If manual encryption is required, approved and dedicated staff is responsible for encrypting / decrypting the data. Confidential information is encrypted while in transit over any network using secure protocols like HTTPS, SSL, SFTP, etc. VPN transmissions are performed over an encrypted channel.

Security Event Monitoring

HCL Software continuously monitors and analyzes past/real time system information to identify and respond to any potential threats and or vulnerabilities. The Monitoring and event response framework is designed from industry best practice related policy and procedures; virus and malicious code, intrusion prevention and detection, data loss prevention and event and state monitoring. Related logging and system monitoring processes provide an effective control to identify and investigate security events. All systems' infrastructure components, workstations, and applications are monitored for any activity and critical configuration changes. The log permission and retention alteration is restricted to approved security personal.

Anti-virus and Malicious Code

Servers, workstations and internet gateway devices are updated periodically with latest antivirus definitions that include zero-day anti-malware protection. Defined procedure highlights all anti-virus updates. Anti-virus tools are configured to run weekly scans, virus detection, real time file write activity and signature files updates. Laptops and remote users are covered under virus protection. Procedures to detect and remove any unauthorized or unsupported (e.g., freeware) applications are documented.

Endpoint security detects malicious behavior and helps prevent files attack. Network environment is optimized to provide industry standard security. Internet firewall gateways are equipped with latest security features like IPS, Anti-Malware, Anti-Virus and zero-day protection against unknown, unidentified threats. Signatures for these products are updated periodically. Traffic passing through firewalls is scanned for difference level of checks based on sensitivity, importance and categorization in real time.

Systems Hardening and Device Security

General
All servers, routers, firewalls and other relevant infrastructure conform to industry best practices. HCL SW removes all unnecessary files, utilities from operating system configurations, restricts access rights to least privilege and implements other best practices for cyber defense. HCL SW patches on a regularly prescribed schedule per industry best practices. In case of a breach of network, patches would be implemented immediately.

Device Security
Active anti-virus and anti-malware scanning is in place for all workstations and servers that will access or store client data. Such security software is updated regularly, and users are not able to disable scans. Malware containment and resolution procedures are defined and include the isolation of infected systems where appropriate. In addition to daily malware definition updates, we do ensure that malware scan engine software remains within latest two (2) available versions.

- DLP is installed on all end points
- Mobile device passcode minimum length and complexity is managed by our MDM solution

Domain Security
We follow industry standard security protection for all domains. The ISMS (Information Security Management System) policies are followed as they relate to Domain Security (AD, MFA, Tacacs, LDAP)

Change Management

We follow a change management process for all changes before moving to the implementation phase.

Product Vulnerability Management.

A PSIRT process and vulnerability disclosure program is in place to receive, manage, and communicate remediation for all verified reported software security vulnerabilities. Vulnerabilities are communicated via security bulletins when they have been remediated or when a work-around is available.

Product security vulnerability reports may come from customers, security researchers, Open Source or third-party disclosures.

A vulnerability is considered to be remediated when a software patch/upgrade or a workaround is made available and a security bulletin is published on the HCL Support Knowledge Base. The security bulletin describes the vulnerability, its potential impact if exploited, the affected versions of the product, and the remediation.

To protect our customers, security bulletins are published only when the remediation has been made available in all affected releases.

Non USG clients may report product vulnerabilities through the HCL SW PSIRT page or directly to PSIRT@hcl.com. Customers may also subscribe to our blog.

Way Forward

Expected Value To Customers
Customer hyper-care – Nurture and strengthen existing customer relationships. Engage in closer, meaningful discussions on product direction. Customer-centric roadmaps – Apart from addressing key customer requirements, HCL is also investing in product modernization and TCO reduction for customers.

Expected Value To Partners
HCL Software has a robust Partner ecosystem to design, deliver and support our offerings. Whether you are a developer, consultant or partner, Partner Connect will provide you with insight on how you can build value in your go to market with HCL Software. Partner Connect - One-stop-shop for software-based offerings to enable growth and scale:
https://www.hcltechsw.com/wps/portal/resources/partner-connect/

Resell and Build With Us | Provide Services around our Products.
Please reach out to Geo Partner heads for more information. You can find your geo head at:
https://www.hcltechsw.com/wps/portal/resources/partner-connect/partner-resources/partner-team

For more information about our product portfolio, visit us at www. hcltechsw.com

About HCL Software

HCL Software is a division of HCL Technologies (HCL) that operates its primary software business. It develops, markets, sells, and supports over 20 product families in the areas of DevOps, Automation, Digital Solutions, Data Management, and Mainframes. HCL Software has offices and labs around the world to serve thousands of customers. Its mission is to drive ultimate customer success with their IT investments through relentless innovation of its products. For more information, please visit www.hcltechsw.com.