



SUMMARY OF HP SECURITY MEASURES

To protect Customer data, HP abides by a robust set of information security controls including policies, practices, procedures, and organizational structures to safeguard the confidentiality, integrity, and availability of its own and its customers' information (including Personal Data as defined in HP's Customer and Data Processing Addenda). The following sets forth an overview of HP's technical/organizational security measures throughout the company.

1. Security Policy

HP maintains globally applicable policies, standards, and procedures intended to protect HP and Customer data. The detail of HP's security policies is confidential to protect the integrity of HP's data and systems. However, summaries of our key policies are included below.

2. Information Security Organization

HP has an Information Security Organization responsible for directing and managing the organization's information security strategy and controls. An Information Security Framework/Management System is put in place to ensure compliance with HP's security policies and controls and confirm that the security requirements of its customers are complied with. This Framework is structured in alignment with the NIST Cybersecurity Framework and is reviewed annually.

3. Cybersecurity Risk Management

HP's comprehensive risk management program aims to preserve the confidentiality, integrity, and availability of HP information assets. The program outlines a consistent and effective approach to identifying, assessing, prioritizing, treating, remedying, tracking, and reporting cybersecurity risks.

HP has a defined cybersecurity Risk Appetite (target level of loss exposure that the organization views as acceptable given business objectives and resources) and Risk Tolerance (degree of variance from the organization's risk appetite that the organization is willing to tolerate). Risks are evaluated as a part of the risk management program according to a defined risk management methodology. This approach enables HP to appropriately mitigate information security risks to an acceptable level. The HP cybersecurity risk management program aligns with HP's Enterprise Risk Management process.

4. HR Security

HP Human Resource Security establishes processes to ensure information security at every stage of the employee lifecycle. These include establishing processes for access to facilities, information systems, and other assets. Obtaining written acknowledgment with confidentiality and non-disclosure agreements and background screening procedures. All candidates for employment with HP must complete a background verification check carried out in accordance with relevant laws, regulations, and ethics.

5. Asset Management

HP has a process in place for identifying technical information assets, and through this process, HP identifies all assets under its responsibility and categorizes the critical assets. HP further maintains a set of documented handling procedures for each information classification type, including those assets that contain Personal Data. Handling procedures address storage, transmission, communication, access, logging, retention, destruction, disposal, incident management, and breach notification. HP security policies and standards mandate secure disposal of media.

6. Data Security

HP's Data Security policy outlines the security practices and technical controls that must be implemented to protect the confidentiality, authenticity, and integrity of data. Legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification are a few of the factors that determine how information is classified under HP's Data Security policy. In addition to data handling procedures, the policy outlines data encryption, deletion, collection and processing, retention, backup and data loss prevention.

7. Access Control

The principle of least privilege is used for providing logical access control. User access is provided via a unique user ID and password. HP's password policy has defined complexity, strength, validity, and password-history related controls. Access rights are reviewed periodically and revoked upon personnel departure.

User account creation and deletion procedures, as have been mutually agreed upon, are implemented to grant and revoke access to client systems used during the engagement.

8. Cryptography

HP has defined a set of robust processes for cryptography to ensure the confidentiality, integrity, and availability of information assets. Approved protocols require encryption for certain assets, including those that contain personal data.

9. Physical and Environmental Security

HP facilities are secured using various physical and electronic access controls and surveillance capabilities. Depending on the facility, this could include security guards, electronic access control, and closed-circuit television (CCTV).

All HP personnel are registered and are required to carry appropriate identification badges.

Facilities have required infrastructure support with temperature control and power backups where required, using UPS and/or diesel generators to support critical services.

10. Operations Management

HP has defined a minimum set of hardening requirements for technology infrastructure, including workstations, servers, and network equipment. Workstation/servers images contain pre-hardened operating systems. Hardening requirements vary depending on the type of operating system and applicable controls implemented.

HP has deployed Network Intrusion Detection/Prevention Systems (NIDS/ NIPS) within the network and are monitored and managed 24*7.

11. Communications Security

Communications Security ensures the protection of information within corporate networks. This includes the installation and management of network security components (e.g. firewalls), segregation of networks, as well as web filtering and email handling controls.

12. Systems Security

By policy, the development of systems and supporting software within HP follow a secure development methodology to ensure security throughout the system/software lifecycle. The Software Development Lifecycle defines initiation, development/acquisition, implementation, operations, and disposal requirements. All system components, including modules, libraries, services, and discrete components, are evaluated to determine their impact on the overall system security state.

HP has defined controls for the protection of application service transactions. These controls include validating and verifying user credentials, mandating digital signatures and encryption, implementing secure communication protocols, storing online transaction details on servers within the appropriate network security zone.

Internal vulnerability scans are performed regularly.

13. Third Parties and Subcontractors

HP has processes in place to select sub-contractors that are able to comply with comprehensive contractual security requirements.

For applicable suppliers (suppliers that handle/store/transmit HP data and customer owned HP held data or have access to the HP network), HP Cybersecurity performs a risk assessment to verify the existence of an information security program. An adequate program must include physical, technical, and administrative safeguards. This assessment must be done before the supplier has access to HP information.

14. Information Security Incident Management

HP follows a developed Cyber Incident Management Process that addresses purpose, scope, roles, responsibilities, management commitment, organizational coordination,

implementation procedures, and compliance checking. HP reviews and updates this process on an annual basis.

A Cyber Incident Response Team, which includes HP Cybersecurity personnel trained in incident response and crisis management, is assembled for regular table-top reviews of process and any incident or event.

15. Business Continuity Management

HP maintains a global Continuity of Operations program. This program takes a holistic, company-wide approach for end-to-end continuity through a set of collaborative, standardized, and internally documented planning processes.

HP periodically exercises its business continuity plans to ensure their effectiveness. HP currently tests and updates all plans at least yearly and ensures that people with a role in the business continuity plan are trained.

16. Compliance

Compliance guides the organization's approach to meet the various legal, contractual, and internal expectations required for an effective information security program. HP conducts regular information security reviews to ensure information security protocols are appropriately incorporated into the operations of each HP business group. HP's review process ensures that documents are updated to reflect all current legal obligations, as requirements change over time.

17. Payment Card Industry

Payment Card Industry (PCI) addresses the organization's approach to meet PCI Compliance, as well as the businesses responsibilities and security controls aligned with PCI DSS. Installing and maintaining appropriate network security controls, such as firewalls and other network security technologies ensure HP to meets PCI Compliance requirements.

18. HP Product Security

HP Product Security covers several important security practices that must be applied to secure HP Products, including code signing, product security vulnerabilities governance and management, security bulletins, and reporting product security issues.

19. HP Service Security

HP Service Security covers several important security practices that must be applied to secure HP Services provided to HP customers. Under this policy, the following areas of service security are addressed: HP infrastructure hosted, third party hosted, partner hosted, as well as customer hosted.

Date: February 2024