SECURITY AND PRIVACY WHITE PAPER

HP | Poly Security and Privacy Overview

Part 3725-85379-001

Version 05

March 2024

Introduction

HP | Poly helps unleash the power of human collaboration with secure video, voice, and content solutions. This white paper describes HP | Poly privacy and security practices and includes information about how these practices are applied to the design, development, implementation, hosting, and maintenance of systems, infrastructure and the networks that store HP | Poly and customer data. This white paper is supplemental to the HP Privacy Statement. The most current version of this white paper will be available on HP | Poly's website.

Security at HP | Poly

Information security at HP | Poly is managed by the HP Cybersecurity team led by HP | Poly's Chief Information Security Officer (CISO), which oversees both corporate information technology (IT) and product development. Standards and guidelines are developed by the team to drive secure deployment of all corporate IT systems and development of secure products and services.

HP | Poly's Information Security Management System (ISMS) has achieved ISO 27001:2013 certification. ISO/IEC 27001 is the most widely accepted international standard for information security best practices and provides assurance that HP | Poly has established and implemented best-practice information security processes.

HP | Poly's Information Security Management System (ISMS) is comprehensive and covers people, processes and technologies used to provide unified communication and collaboration services and solutions to employees and customers (both hosted and on-premises).

Technical and Organizational Measures (TOMs) are thoughtfully designed and implemented to address risks identified.

Both HP | Poly's internal systems and the products and services that are provided to customers are regularly reviewed to verify compliance of information processing and procedures with the appropriate security policies, standards, and guidelines.

Policies, Procedures, Standards and Guidelines

Policies for information and product security are defined and approved by management, published, and communicated to employees and relevant external parties on a need-to-know basis for the purposes of delivering HP | Poly products and services. The policies are also reviewed at planned intervals and/or when significant changes occur to ensure their continuing suitability, adequacy, and effectiveness. Additionally, all employees receive appropriate awareness education and training and regular updates about security and data privacy policies on at least an annual basis. HP | Poly requires all employees and contractors to practice information security in accordance with all approved policies and procedures.

The HP | Poly Product Security Standards align with NIST Special Publication 800-53, ISO/IEC 27001:2013 and OWASP for application security. Guidelines, standards, and policies are implemented to provide our developers industry approved methods for adhering to the HP | Poly Product Security Standards.

Employee Training and Awareness

All HP | Poly workers receive regular security awareness training on at least an annual basis, including regular updates about security and data privacy policies. Employees who process sensitive data and/or handle sensitive information systems or services are required to participate in additional training and awareness activities.

Physical Security

The physical security of offices, rooms and facilities is designed and applied in accordance with HP | Poly

Security Standards to protect against natural disasters, malicious attacks, or accidents. Security perimeters and work procedures are defined and used to protect areas that contain sensitive or critical information and information processing facilities. Access points that could be used by unauthorized persons are controlled through the requirement of physical badges and proximity cards. Access is additionally monitored by security guard personnel.

Network Security

HP | Poly's internal corporate and development networks are managed and controlled to protect both systems and applications. Security mechanisms, service levels and management requirements of all network services are identified and included in network services agreements, whether those services are provided in-house or outsourced.

Network segregation is also implemented using VLANs, network controls and firewalls to manage and further restrict groups of information systems, services, and users.

Production environments are segregated from dev, QA and staging environments and production data will not normally be used for testing purposes except when required to perform necessary troubleshooting.

Security by Design

HP | Poly implements a layered defense-in-depth approach to protect information in products and systems from unauthorized processing. For example, border controls are implemented with firewall rules to block, or limit known network-based attacks.

Products are subject to similar restrictive standards (e.g., PKI signed software and firmware will block the installation of updates that are not digitally signed by HP | Poly.) Furthermore, 802.1x support is included in infrastructure, voice and video endpoint devices produced by HP | Poly.

System hardening and system integrity checks across the company and within our products are designed to protect against most file-based or malicious configuration threats and reduce the attack surface within HP | Poly products.

Secure Software Development Life Cycle

HP | Poly follows a secure software development life cycle (S-SDLC) with an emphasis on security throughout the product development process. Every phase of the development process ensures security by establishing security requirements alongside functional requirements as part of initial design.

The S-SDLC implemented by also includes a significant emphasis on risk analysis and vulnerability management. To increase the security posture of HP | Poly products, a defense-in-depth model is systematically incorporated through layered defenses.

- The principle of least privilege is always followed.
- Access is disabled or restricted to system accounts and services nonessential to standard operation.
- Standards-based Static Application Security Testing (SAST) and patch management are cornerstones of our S-SDLC.
- Architecture reviews ensure compliance with requirements without conflicts and validate the design quality, scalability, and performance of products.
- Code reviews are implemented to detect issues prior to QA testing and limit the risk of introducing logic or design flaws, and common security misconfigurations which are hard to identify during the later phases of the S-SDLC process.
- Internal penetration testing and attack surface analysis are performed to verify the implementation of security controls in HP | Poly products and may include:
    - Evaluating services on open TCP/UDP ports
    - Automated and scripted testing

  - Web UI testing (searching for XSS, CRSF, RCE, file inclusion and injections)
  - Evaluation of access to and hardening of the underlying operating system in products
  - Manual testing and fuzzing of interfaces
- Regular retention of independent third-party penetration testers for additional validation of our program

Every new product released is subject to full security and penetration testing prior to release to detect any possible new vulnerabilities that might exist. Ongoing product releases are subject to security audits that incorporate dozens of vulnerability scanning tools (some commercially available and some custom) and may involve extensive source code audits and/or manual penetration tests.

Vulnerability Management
Managing technical vulnerabilities within HP | Poly information systems is constructed on timely information through regular threat intelligence. Prompt evaluation and analysis of the organization's exposure to such vulnerabilities is designed to result in appropriate measures being taken at early stages to address the associated risks.

Rules are in place to restrict the following:
1. Unauthorized users installing or configuring software
2. Installation of unauthorized software by any user

For each vulnerability discovered in a HP | Poly product, a CVSSv3 score is assigned which is associated with the turnaround time allowed for providing fixes.

Security Incident Response
The HP Cybersecurity team promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. You may contact them directly at informationsecurity@hp.com

This practice serves as the reactive (but enforced) arm of the security lifecycle. The Cybersecurity team works proactively with customers, independent security researchers, consultants, industry organizations and other suppliers to identify possible security issues with HP | Poly products and networks. HP | Poly security advisories and bulletins can be found on the HP Customer Support.

Product Documentation
HP | Poly provides security and privacy related information about its products and services in a variety of forms to meet the varying needs and requests of partners and customers.

- Product user, administrator and privacy guides include sections specific to security controls as do product and solution deployment guides, which are all published on the HP | Poly website.
- Public Security and Privacy White Papers are available for most products and services on the HP | Poly website . Additional information may be available. Please contact your HP | Poly representative to inquire.
- For cloud services, a completed Consensus Assessments Initiative Questionnaire (CAIQ) may be available to inform your risk assessments.
- For critical security issues, HP | Poly security advisories and bulletins are published publicly and can be found on the HP Customer Support.

All security and privacy related publications and documentation are thoroughly reviewed and undergo a formal approval process prior to final release. Multiple business units are required to provide feedback including (but not limited to) Engineering, Marketing, Legal, Security Office and the Technical Communications teams. These teams combine to produce detailed technical documentation that is designed to provide useful and direct answers to many of our partners' and customers' security and privacy concerns.

Privacy by Design
HP | Poly implements internal policies and measures based on perceived risks which meet the principles of data protection by design and data protection by default. Such measures consist of minimizing the processing of personal data, anonymizing personal data as soon as possible, transparently documenting the functions and processing of personal data and providing features which enable the data subject to exercise any rights they may have.

When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfill their task, HP | Poly considers the right to data protection with due regard.

Compliance with Data Protection Laws and Regulations
The protection of personal data, as well as compliance with applicable data privacy and protection laws and regulations, is important to HP | Poly and its subsidiaries as well as our customers, partners, employees, contractors, service providers and others. HP Privacy Statement outlines and explains the principles for processing, retaining, deleting and otherwise using the personal data of enterprise customers.

Protection of Customer Personal Data
On an ongoing basis, HP | Poly conducts comprehensive reviews of where and how our products, services, and business processes collect, use, store and dispose of customer personal data. Policies, standards and governance structures are reviewed at regular intervals and updates are made as appropriate.

Subprocessors
HP | Poly uses certain subprocessors to assist in providing our products and services. A subprocessor is a third-party data processor who, on behalf of HP | Poly, processes customer data. Prior to engaging a subprocessor, HP | Poly executes an agreement with the subprocessor that is in accordance with applicable data protection laws.

The subprocessor list here identifies HP | Poly's authorized subprocessors and includes their name, purpose, location and website. For questions, please contact HP's Chief Privacy and Data Protection Officer form.

Prior to engagement, suppliers that may process data on behalf of HP | Poly must undergo a privacy and security assessment. The assessment process is designed to identify deficiencies in privacy practices or security gaps and make recommendations for reduction of risk. Suppliers that cannot meet the security requirements are disqualified.

Cross-Border Data Transfers
Contractual commitments are in place to meet the requirements to legally transfer personal data from the EU to the rest of the world under applicable law. HP | Poly continues to use EU standard model clauses as a basis for such transfers to jurisdictions where there is no 'adequacy' of data protection as recognized by the EU.

HP | Poly Partners and Customers
When HP | Poly processes the personal data of our end customers, HP | Poly generally acts as a "data processor" and our partners and customers are acting as the "controller" as those roles are defined by the GDPR. As we continue to work with our partners and end user customers, our goal is to find new opportunities for our products and services to further aid our partners and customers in meeting their own GDPR compliance obligations.

Contractual Protections
As needed, we are updating contracts with our partners, customers, and suppliers to directly address GDPR requirements. HP | Poly reviews

its key supplier contracts on an ongoing basis and uses all reasonable efforts to ensure GDPR compliance throughout its supply chain.

How HP | Poly can help with Data Privacy Compliance

In connection with the development of our products and solutions, HP | Poly incorporates Privacy by Design elements early in the process with the objective that technical and organizational security measures will limit, by default, the amount and use of personal data to what is specifically required.

Additional Resources

To learn more about HP | Poly, please visit our website.

Disclaimer

This white paper is provided for informational purposes only and does not convey any legal rights to any intellectual property in any HP | Poly product. You may copy and use this paper for your internal reference purposes only. HP | POLY MAKES NO WARRANTIES, EXPRESS OR IMPLIED OR STATUTORY AS TO THE INFORMATION IN THIS WHITE PAPER. THIS WHITE PAPER IS PROVIDED “AS IS” AND MAY BE UPDATED BY HP | POLY FROM TIME TO TIME. To review the most current version of this white paper, please visit our website.