SECURITY AND PRIVACY WHITE PAPER

Poly Security and Privacy Overview

Part 3725-85379-001

Version 02

April 2020

Introduction
Poly helps unleash the power of human collaboration with secure video, voice and content solutions. This white paper describes 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 Poly and customer data. This white paper is supplemental to the Poly Privacy Policy. The most current version of this white paper will be available on Poly's website.

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

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

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, customers (both hosted and on-premises).

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

Both 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 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. Poly requires all employees and contractors to practice information security in accordance with posted policies and procedures.

The 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 Poly Product Security Standards.

Employee Training and Awareness
All 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 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 entered by unauthorized persons are controlled through the requirement of physical badges and proximity cards. Access is additionally monitored by security guard personnel.

Network Security
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 may not be used for testing purposes.

Security by Design
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 Poly.) Furthermore, 802.1x support is included in infrastructure, voice and video endpoint devices produced by 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 Poly products.

Secure Software Development Life Cycle
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 Poly also includes a significant emphasis on risk analysis and vulnerability management. To increase the security posture of 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 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

Each new version of a product is tested pre-release in accordance with awareness of the testing levels performed upon previous releases.

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 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 Poly product, a CVSSv3 score is assigned which is associated with the turnaround time allowed for providing fixes.

Security Incident Response
The Poly Security Office (PSO) promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. You may contact the PSO directly at informationsecurity@Poly.com

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

Product Documentation
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 Poly website.
- Public Security and Privacy White Papers are available for most products and services on the Poly Privacy website . Additional information may be available. Please contact your 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, Poly security advisories and bulletins are published publicly and can be found on the Poly Security Center.

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
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, 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 Poly and its subsidiaries as well as our customers, partners, employees, contractors, service providers and others. Poly's Privacy Policy 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, Poly conducts comprehensive reviews of where and how our products, services, and business processes collect, use, store and dispose of enterprise customer personal data. Policies, standards and governance structures are reviewed at regular intervals and updates are made as appropriate.

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

The subprocessor list here identifies Poly's authorized subprocessors and includes their name, purpose, location and website. For questions, please contact privacy@poly.com.

Prior to engagement, suppliers that may process data on behalf of 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. 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.

Poly Partners and Customers
When Poly processes the personal data of our end customers, 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. Poly reviews its key supplier contracts on an ongoing basis and

uses all reasonable efforts to ensure GDPR compliance throughout its supply chain.

How Poly can help with Data Privacy Compliance

In connection with the development of our products and solutions, 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.

Other efforts include having either new or supplemental white papers available for our customers that address privacy-related data processing and other information about our products and solutions available at Poly's Privacy website.

Additional Resources

To learn more about 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 Poly product. You may copy and use this paper for your internal reference purposes only. 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 POLY FROM TIME TO TIME. To review the most current version of this white paper, please visit our website.