SECURITY AND PRIVACY WHITE PAPER

Habitat Soundscaping

Part 3725-86758-001

Version 01

May 2020

Introduction
This white paper addresses security and privacy related information regarding Habitat Soundscaping.

It also describes the security features and access controls in Poly's processing of personally identifiable information or personal data ("personal data") and customer data in connection with the provisioning and delivery of the Habitat Soundscaping service, and the location and transfers of personal and other customer data. Poly will use such data in a manner consistent with the Poly Privacy Policy, and this white paper which may be updated from time to time. 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.

Habitat Soundscaping is an audio/visual communication system which enhances the workplace environment by making both a visual and auditory connection with the natural environment. The service consists of computing elements located on-premises in the customer environment and in the cloud, powered by Amazon Web Services (AWS).

NOTE: The Habitat Soundscaping solution is not sold directly by Poly and can only be purchased through one of our Partners. Partners are responsible for the provisioning and delivery of the service and have access to the Habitat cloud application and any customer data stored in the cloud. Please refer to your agreement with the Partner you purchased the service from for information on their security practices.

Security at Poly
Security is always a critical consideration for a cloud-based service such as Habitat Soundscaping. 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.

Product security at Poly is managed through the Poly Security Office (PSO), which oversees secure software development standards and guidelines. 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.

Secure Software Development Life Cycle
Poly follows a secure software development life cycle (S-SDLC) with an emphasis on security throughout the product development processes. Every phase of the development process ensures security by establishing security requirements alongside functional requirements as part of initial design. Architecture reviews, code reviews, internal penetration testing, and attack surface analysis are performed to verify the implementation.

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 services nonessential to standard operation.

Additional testing, in the form of standards-based Static Application Security Testing (SAST) and patch management is a cornerstone of our S-SDLC.

Change Management
A formal change management process is followed by all teams at Poly to minimize any impact on the services provided to the customers. All changes implemented for the Habitat Soundscaping service go through vigorous quality assurance testing where all functional and security requirements are verified. Once Quality Assurance approves the changes, the changes are pushed to a staging environment for UAT (User Acceptance Testing). Only after final approval from stakeholders, changes are implemented in production.

While emergency changes are processed on a much faster timeline, risk is evaluated, and approvals are obtained from stakeholders prior to applying any changes in production.

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.

Secure Deployment

The Habitat Soundscaping solution includes audio hardware located on-premise in the customer environment and a cloud hosted application powered by AWS. The Habitat Soundscaping audio solution consists of a physical server, also known as the system controller, a switch, zone controller, speakers and distraction sensors. The solution may also include visual components such as a waterfall, digital window or digital skylight.

The system controller is the gateway between the Habitat Soundscaping audio components and the cloud application. It is a network-connected rack-mounted appliance running software to enable the soundscape experience. This server is provided by the Partner from which Habitat Soundscaping was purchased from. The Partner is responsible for the secure installation of that server. There is no remote access to the server and the customer must work with the Partner to action any updates needed.

The system controller is configured as a DHCP client and requires a connection to a network with external, outbound access available on TCP port 443 (https), UDP port 123 (NTP), and if a video solution is used, TCP port 80 (http); no inbound connections are required from the internet to the system controller. The system controller's connection to the Habitat Soundscaping cloud application is secured via a server-side TLS certificate and, once on-site provisioning is complete, authenticated via a client-side TLS certificate generated for the system controller specific installation. No other components in the Habitat Soundscaping system require external access.

User Authentication

Authentication for the Habitat Soundscaping Cloud application is via local accounts. These local accounts use a user's email address as the user ID. Poly is responsible for adding users and setting passwords at which time they can sign in. If a user forgets their password they will need to reach out to Poly to initiate changing it. All local passwords are stored hashed using bcrypt with 12 salt rounds. These accounts are for system administrators, as end users are not logging into this service. Poly administrators and the Partner from which you purchased the service from authenticate to the Habitat Soundscaping cloud application via the same method as customers.

Disaster Recovery and Business Continuity

The Habitat Soundscaping solution is architected to provide high reliability, resiliency and security. The entire service is hosted on multiple geographically distributed AWS data centers in the United States. Normal low impact outage due to loss of power or connectivity is already handled by the cloud hosting provider—AWS.

During a major crisis or disaster, service will be moved to a different region until the affected

region is restored.

Poly has a Business Continuity and Disaster Recovery Plan reviewed and approved by management to ensure that we are appropriately prepared to respond to an unexpected disaster event. Poly tests disaster recovery processes and procedures on an annual basis. We use the results of this testing process to evaluate our preparedness for disasters, and to validate the completeness and accuracy of our policies and procedures.

Cryptographic Security

While processing all Habitat Soundscaping data, industry standard HTTPS over TLS1.2 is used for data encryption in transit and AWS database encryption with AES-256 for data at rest. Encryption keys are managed by AWS.

Data Processing

Poly does not access any customer's data except as required to enable the features provided by the service. The Poly Partner, from whom the customer purchased Habitat Soundscaping, will have access to customer data as required to administer and provision services. Please refer to your agreement with the Partner for information on their data processing activities.

If you are an individual user, and the purchase of Habitat Soundscaping has been made by your employer as the customer, all the privacy information relating to personal data in this white paper is subject to your employer's privacy policies as controller of such personal data.

Source From Where PI Collected	Categories of PI Collected	Business Purpose for Collection	Disclosed to the following Service Providers
Tenant IT Administrator details	• Name • Address • Phone number • Email address • Company name • Time zone	• Administering services • Customer communication • Required to create Habitat Soundscaping tenant	AWS
Office Environment Layout	• Floor plans • Photos of office space	• Build Habitat Soundscaping designs for customer • Visualize services in customer environment.	AWS

Purposes of processing
The Habitat Soundscaping solution collects data to enable the service and enhance the workplace environment.

Audio Signal Processing
In a Habitat Soundscaping installation, distraction sensors are installed at the customer site in the ceiling which connect to the zone controller(s). Distraction sensors transmit audio data in real time to the zone controller. All analysis of audio data is done on the zone controller. The zone controller extracts metadata from the audio stream which is then routed to the system controller. Metadata extracted includes:

- Noise Floor: Numeric value indicating general level of audio in the space
- Distraction Indicator: Numeric value indicating the amount of speech detected in the space.

The zone controller has no direct connectivity to the customer network or internet. The only system that has any connection to the customer network is the system controller which is used to consolidate metadata to transmit to the cloud application and receive adaptive response information back. The adaptive response data is a numeric value indicating the volume amount the Habitat Soundscaping system should adjust to. No audio data is ever stored or transmitted from the system controller.

How Customer Data is Stored and Protected
All customer data is stored within the AWS data centers on which the service is deployed. Data is encrypted at rest using AWS database encryption, AES-256. Data resides in the United States. Tenant-specific data are stored in separate DB schemas using Amazon S3 buckets.

Customer data stored on the AWS database is backed up using AWS RDS backups and encrypted at rest using industry-standard AES-256 encryption technology.The same encryption key used for the source database. Normal access controls of authorized users and data security policies are followed for all backup data. No physical backup media is used. Data stored on the system controller is not backed up.

Office floor plans, including heat maps, are accessed using signed URLS by AWS. Signed URLs allow for more control over secure access to specific content and support timed link expiration.

To learn about how encryption is applied, please visit the following link here.

Poly may change the location of the Habitat Soundscaping database server and details of any such change shall be set forth in the latest copy of this white paper available on Poly's website.

For transferring personal data of EU customers to the US, Poly uses an Intragroup Data Transfer Agreement incorporating the EU Standard Contractual Clauses as the transfer mechanism.

The Habitat Soundscaping database and application servers reside in the AWS data center behind a fully patched firewall that is also managed. Access for any services not required by Habitat Soundscaping is blocked.

Server Access and Data Security
Habitat Soundscaping is hosted on AWS. Only authorized staff members with proper access permissions have access to the production servers. For details on AWS cloud security see https://aws.amazon.com/security/.

We use a combination of administrative, physical, and logical security to keep your information safe. Your data may be accessed by Poly as required to support the service and access is limited to only

those within the organization with the need to access data in order to support the service.

Data Deletion and Retention
All information collected from the customer is stored in the database with the tenant information configured as the access control mechanism. Nothing is transmitted outside of Habitat Soundscaping. All data is self-contained in the database in the data center.

Poly may retain customer data for as long as needed to provide the customer with any Poly cloud services for which they have subscribed and for product improvement purposes. When a customer makes a request for deletion to privacy@poly.com, Poly will delete the requested data within 30 days, unless the data is required to be retained to provide the service to customer. Poly may "anonymize" personal data in lieu of deletion. In cases where anonymization occurs, the process is irreversible and includes but is not limited to searching and sanitizing all customer-specific data (e.g., name, site information and IP address) with randomly generated alphanumeric characters.

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
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.

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.

Additional Resources
To learn more about Habitat Soundscaping, contact your Poly representive..

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.