SECURITY AND PRIVACY WHITE PAPER

Habitat Soundscaping

Part 3725-86758-001

Version 05

March 2024

Introduction

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

It also describes the security features and access controls in HP | 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. HP | Poly will use such data in a manner consistent with the HP Privacy Statement, and this white paper which may be updated from time to time. 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.

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 HP | 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 HP | Poly

Security is always a critical consideration for all HP | Poly 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 you can be reassured that HP | Poly has established and implemented best-practice information security processes.

Product security at HP | Poly is managed through the HP Cybersecurity team, which oversees secure software development standards and guidelines.

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 with industry approved methods for adhering to the HP | Poly Product Security Standards.

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 processes. Every phase of 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 HP | Poly 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 services nonessential to standard operation.

Standards-based Static Application Security Testing (SAST) and patch management are cornerstones of our S-SDLC.

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.

Security by Design

HP | Poly follows Security by Design principles throughout our product creation and delivery lifecycle which includes considerations for confidentiality, integrity (data and systems) and availability. These extend to all systems that HP | Poly uses – both on-premises and in the cloud as well as to the development, delivery, and support of HP | Poly products, cloud services and managed services.

The foundational principles which serve as the basis of HP | Poly's security practices include:

1. Security is required, not optional
2. Secure by default, Secure by design
3. Defense-in-depth
4. Understand and assess vulnerabilities and threats
5. Security testing and validation
6. Manage, monitor, and maintain security posture
7. End-to-end security: full lifecycle protection

Security Testing

Both static and dynamic vulnerability scanning as well as penetration testing are regularly performed for production releases and against our internal corporate network by both internal and external test teams.

Cloud systems are managed by HP | Poly and are updated as needed. Patches are evaluated and applied in a timely fashion based on perceived risk as indicated by CVSSv3 scores.

Change Management

A formal change management process is followed by all teams at HP | 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.

Data Processing

System logs and call detail records can be collected by or sent to HP | Poly. These may contain names, emails, IP addresses, and locations. Customers who contact HP | Poly for technical support are asked to provide contact information.

If someone is an individual user and the purchase of a HP | Poly service has been made by their employer as the customer, all the privacy information relating to personal data in this white paper is subject to their employer's privacy policies as controller of such personal data.

Purpose of Processing

Information that is processed is used for enhancing the user experience, allowing configuration of settings required for proper delivery of services, and easy access to frequently used data. When configured to use an optional HP | Poly device management solution, the on-premises server or cloud service processes configuration files and their overrides to aid the management of the devices in a given deployment. The server or cloud service may also process device network information, media statistics, and device asset information to aid in device analytics, which enables device performance validation and visibility into customer quality of experience and service performance.

Source of Personal Data	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

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 is 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.

HP | 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 HP | Poly's website.

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

The 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 Soundscaping is blocked.

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.

HP | Poly may retain customer data for as long as needed to provide the customer with any HP | Poly cloud services for which they have subscribed and for product improvement purposes. When a customer makes a request for deletion to HP's Chief Privacy and Data Protection Officer form, HP | Poly will delete the requested data within 30 days, unless the data is required to be retained to provide the service to customer. HP | 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.

Secure Deployment

The Habitat Soundscaping solution includes audio hardware located on-premises in the customer environment and a cloud hosted application powered by AWS. The 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 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 Soundscaping was purchased. The Partner is responsible for the secure installation of the 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 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 Soundscaping system require external access.

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. Customer data may be accessed by HP | 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.

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 is used for data at rest. Encryption keys are managed by AWS.

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. HP | Poly is responsible for adding users and setting passwords. If a user forgets their password, they will need to reach out to HP | Poly to initiate changing it.

All local passwords are stored hashed using bcrypt with salt rounds. These accounts are for system administrators, as end users are not logging into this service. HP | Poly administrators and the Partner from which you purchased the service will authenticate to the Soundscaping cloud application via the same method as customers.

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.

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 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.

HP | 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. HP | Poly tests disaster recovery processes and procedures on an annual basis but are sometimes conducted more frequently when there are changes to our infrastructure that warrant new tests. 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.

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

The HP 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 website.

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.

Additional Resources

To learn more about Habitat Soundscaping, please contact your HP | Poly representative.

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.