Eceptionist SaaS - Security, Privacy and Architecture

Date: January 1, 2022

Eceptionist's Corporate Trust Commitment

Eceptionist is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across the Eceptionist SaaS ("SaaS"), including protection of Customer Data as defined in the **Eceptionist SaaS Agreement.**

Services Covered

This documentation describes the architecture of the security and privacy-related audits and certifications received for, and the administrative, technical, and physical controls applicable to the SaaS services ("Covered Services"):

Architecture and Data Segregation

The Covered Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific unique identifiers and allows the use of customer and user role based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production.

Control of Processing

Eceptionist has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by Eceptionist and its sub-processors. In particular, Eceptionist and its affiliates have entered into written agreements with their sub-processors containing privacy, data protection, and data security obligations that provide a level of protection appropriate to their processing activities. Compliance with such obligations as well as the technical and organizational data security measures implemented by Eceptionist and its sub-processors are subject to regular audits.

Third-Party Functionality

When customers use the Covered Services to transmit or receive mobile messages, such as SMS messages, the content of those messages and related information about those messages are received by: (a) aggregators – entities that act as intermediaries in transmitting mobile messages, and (b) carriers – entities that provide wireless messaging services to subscribers via wireless telecommunication networks. These aggregators and carriers may access, store, and transmit message content and related information to provide these functions.

Audits and Certifications

The Covered Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis. Eceptionist uses infrastructure provided by third parties to host Customer Data submitted to certain services. Specifically, Eceptionist uses infrastructure provided by Microsoft Corporation ("Azure") to host Customer Data submitted to SaaS. Information about security and privacy-related audits and certifications received by Azure, including ISO 27001 certification and SOC reports, is available from the **Azure Security website**, and the **Azure Compliance website**.

Security Controls

The Covered Services include a variety of security controls. These controls include:

- Unique user identifiers allow customers to assign unique credentials for their users and assign and manage associated permissions and entitlements.
- Controls ensure initial passwords must be reset on first use.
- Two-factor authentication at account creation and resetting password either by email or SMS text message.
- Controls limit password re-use.
- Password parameters necessitate sufficient length and complexity requirements.
- Customers have the option to define additional security settings such as account lockout
- Customer's administrators have the option to manage their application users, and assign or define roles, or apply permissions and rights, within their implementation of the Covered Services.
- Where SFTP uploads are available within the Covered Services, Customers use their own external SFTP accounts to upload customer content to the Covered Services. If a customer desires that Eceptionist provide an inbound SFTP account to the customer, the customer sets its own password for that account. Customers may also request Login IP for an Eceptionist-provisioned SFTP account by contacting their support representative. Inbound SFTP accounts are otherwise not subject to the security controls, procedures, or policies in this document.

Some Covered Services use Azure, as described above. Further information about security provided by Azure is available from the **Azure Security website**.

Security Policies and Procedures are operated in accordance with the following policies and procedures to enhance security:

- User passwords are stored using a salted hash format and are not transmitted unencrypted.
- Social account OAuth tokens used within SaaS are encrypted with a minimum of 128-bit AES encryption.
- User access log entries are maintained, containing date, time, URL executed or identity ID operated on, operation performed (accessed, created, edited, deleted, etc.) and source IP address.
- If there is suspicion of inappropriate access to the Covered Services, Eceptionist can provide customers log entry records to assist in forensic analysis. This service will be provided to customers on a time and materials basis.
- User access logs are stored in a secure centralized host to prevent tampering.
- User access logs are kept for a minimum of 90 days.
- Eceptionist personnel will not set or recover a defined password for a user.

Intrusion Detection

Eceptionist, or an authorized independent third party, will monitor the Covered Services for unauthorized intrusions using network-based intrusion detection mechanisms. Eceptionist may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plugins, enabled MIME types, etc.) for security purposes, including to prevent fraudulent authentications, and to ensure that the Covered Services function properly.

Security Logs

All Eceptionist systems used in the provision of the Covered Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis.

Incident Management

Eceptionist maintains security incident management policies and procedures. Eceptionist notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by Eceptionist or its agents of which Eceptionist becomes aware to the extent permitted by law.

User Authentication

Access to the Covered Services requires a valid user ID and password combination, which are encrypted via TLS 1.2 and greater while in transmission, as well as machine specific information for identity validation as described under "Security Controls," above. Following a successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

Cookie Policy

The Eceptionist system generates a cookie when a user has successfully logged in, embeds the cookie in the user browser and uses the information stored in cookie to identify the user. The cookie only contains a unique session identifier assigned to the user. The Cookie does not contain any user's privacy information. The Eceptionist system requires users to allow cookies to be embedded into their browsers to be able to access and use the system properly.

Physical Security

Production data centers used to provide the Covered Services have access control systems. These systems permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by guards, two-factor access screening, and escort-controlled access, and are also supported by on-site backup generators in the event of a power failure.

Reliability and Backup

All infrastructure components are configured in a high availability mode or in a redundant fashion. All Customer Data submitted to the Covered Service is backed up on a daily basis and copies are stored in an encrypted manner both locally and offsite for 30 days

Disaster Recovery

The Covered Services' production systems are protected by disaster recovery plans which provide for backup of critical data and services. A comprehensive system of recovery processes exists to bring business-critical systems back online within the briefest possible period of time. Recovery processes for database security, systems administration, and network configuration and data provide a roadmap for personnel to make processes available after an outage.

Viruses

The Covered Services have controls in place that are designed to prevent the introduction of viruses to these Services' respective platforms. Uploaded attachments are not executable in SaaS and therefore will not damage or compromise the SaaS services by virtue of containing a virus.

Data Encryption

The Covered Services use, or enable customers to use, industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Covered Services including through Transport Layer Security (TLS) 1.2 leveraging at least 2048-bit RSA server certificates and 128 bit symmetric encryption keys at a minimum.

Return of Customer Data

During the contract term, customers may export a copy of any Customer Data that is made available for export through the Covered Services. Within 30 days of termination of the applicable Covered Service, customers may access their account to export or download Customer Data submitted to SaaS; and/or engage Eceptionist professional services to recover any raw data processed SaaS that has not already been deleted.

Deletion of Customer Data

After termination of the SaaS services, following the 30-day period for return of Customer Data, Customer Data submitted to such services is retained in inactive status for up to 90 days, after which it is securely overwritten or deleted.

This process is subject to applicable legal requirements. Without limiting the ability for customers to request return of their Customer Data submitted to the Covered Services, Eceptionist reserves the right to reduce the number of days it retains such data after contract termination. Eceptionist will update this Eceptionist SaaS Security, Privacy and Architecture Documentation in the event of such a change.

Analytics

Eceptionist may track and analyze the usage of the Covered Services for purposes of security and helping Eceptionist improve both the Covered Services and the user experience in using the Covered Services. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve product functionality.

Eceptionist may share anonymous usage data with Eceptionist's service providers for the purpose of helping Eceptionist in such tracking, analysis and improvements. Additionally, Eceptionist may share such anonymous usage data on an aggregate basis in the normal course of operating our business; for example, we may share information publicly to show trends about the general use of our services.