Epilogue Systems

Information Security Statement

Last Update: April 5, 2023

Epilogue Systems, Inc (“Epilogue”) and its leadership take the security of Epilogue’s information, infrastructure and applications seriously. The company demonstrates its commitment to IT security through the implementation of policies, controls and procedures.. This document provides a summary overview of the IT security controls employed by Epilogue and is intended to be shared with current and potential clients.

Table of Contents

Information Security Program

Epilogue implements an information security program that aligns with the NIST Cybersecurity Framework. This framework, authored by the National Institute of Standards and Technology, provides a functional model for reducing cyber risks. Epilogue's policy framework is based on ISO 27001, covering acceptable use, access controls, business continuity, communications, data classification and handling, encryption, incident response, compliance, change management, operations, HR security, risk management, supplier relationships and systems acquisition and development.

Data Center & Device Security

The Opus Platform uses Amazon Web Services (AWS) as a cloud service provider for web infrastructure and firewall protection. As with any hosting provider, AWS shares responsibility with Epilogue for the overall security of cloud operations. AWS provides "security of the cloud" while Epilogue provides "security in the cloud." AWS publishes substantial documentation on their security practices. AWS participates in multiple compliance programs such as ISO 27001 and SOC 2.

Epilogue operates as a fully remote employee company with no internal corporate network. All business applications required for business operations and related file storage are cloud-based with appropriate user access controls implemented including multi-factor authentication. All company or personal laptops and desktops used to perform business functions require McAfee Small Business Security suite and hard drive encryption. Mobile devices require a security pin.

Data Protection

Your data is stored and processed in an AWS datacenter in the United States. Your data will never be disclosed to any commercial or government entity, unless Amazon or Epilogue is legally required to do so, to comply with a legally valid and binding order, such as a subpoena or a court order, or as is otherwise required by applicable law.

Your data is treated as confidential incorporating the principle of least privilege and logical segregation, isolating and separating data from other clients. Only security screened individuals or service accounts with absolutely required permissions to maintain the application have access to client data. Data that is not necessary to conduct business will not be retained in any format (e.g., paper or electronic). If such data is shared with any external service provider, Epilogue will ensure that:

- A written agreement is executed and retained which defines the provider's responsibility related to the security of this information;
- Any new service provider will be thoroughly vetted by management, Epilogue IT personnel and others as appropriate before engagement to ensure that the provider can meet information security requirements.

Data Privacy

Epilogue considers your personal data and your privacy to be of the utmost importance. Our privacy policy explains what personal data we collect and how we process them. Please reference our online Privacy Statement for further information.

Please note that this privacy statement will be regularly updated to reflect any changes in the way we handle your personal data or if there are any changes in the applicable laws. The privacy policy will also tell you how we protect personal data relating to you that we collect, process and protect in accordance with applicable data protection laws, and the rights available to you in relation to the processing of personal data.

Monitoring & Detection Capabilities

The Opus Platform and related network traffic is monitored via detailed logging and log analysis. Epilogue utilizes real-time Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) capabilities from AWS GuardDuty and Orca Security Cloud to proactively identify threats, risks, and remediation actions. Any abnormal activity is escalated via automated alerting to Epilogue for deeper investigation and response.

Disaster Recovery

AWS data centers are highly available in their design. Network, power and other critical resources are redundant to mitigate the risk of data center wide outages. In the event of a hardware failure, the impacted Opus Platform's virtual machine will be migrated to a new machine with minimal downtime. In the event of data corruption or other catastrophe, your data will be restored to the most recent valid backup with minimal data loss. Virtual machine images and data backups are replicated to a second AWS datacenter within the same region daily and are retained for 7 days. In the event of a complete data center-wide outage, our services can be restored to an alternate AWS datacenter. Back-up and restore capabilities are summarized below:

- Data is backed up across multiple availability zones using automated AWS backup procedures.
- Epilogue tests restore procedures on a regular basis with all systems monitored continuously for availability.
- Containers are managed by an AWS managed service, deployed virtually and can be recycled within minutes.
- All backup data is stored in a second independent location with no shared access or credentials.

Security Maintenance

Epilogue will ensure that all system security is proactively maintained including but not limited to:

- Detection software will be updated and run at regular intervals to ensure that all confidential data is secured.
- Data encryption software will be implemented and updated.
- Vendor patches will be installed on a timely basis.
- Access will be granted to systems only on a "business-need-to-know" basis with access reviewed continuously.
- If external vendors need remote access to service our third-party software, access will be granted only for the time needed to do the necessary task(s) and then immediately disabled.

Human Resources Security

Newly hired personnel and contractors undergo pre-employment background checks. Security and privacy communications are distributed to Epilogue employees monthly. Processes are in place to review user IDs to verify inactive or terminated individuals are removed from Epilogue systems.

Opus - Password Rules

The minimum length of passwords is 8 characters. Minimum password complexity requirements include:

- At least one number
- At least one uppercase letter

Opus - Encryption-in-Transit

Data communications between the end user and the Epilogue AWS data center are made via secure web service calls (https) using the Simple Open Access Protocol (SOAP) and Representational State Transfer (REST). The transmission of the messages is made using Transport Layer Security (TLS) encryption. TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to Secure Socket Layer (SSL).

Opus - Encryption-at-Rest

The Opus Platform uses AWS encrypted databases and file storage. AWS uses the industry standard AES-256 encryption algorithm to encrypt data. This provides an additional layer of data protection by securing data within its source location.

Single Sign-On (SSO)

SSO is available for ADFS, OKTA, Google Directory and OneLogin via the SAML 2.0 protocol.

Opus Platform - Information Security Best Practices

Best-practices are followed to ensure the confidentiality, integrity and accuracy of data.

Error Handling & Logging

- Error pages capture and control application and framework errors
- Stack traces and unhandled exceptions are prevented
- Privileges changes and authentication failures are logged with AWS CloudTrail and alerted via Alert Logic
- Relational database principles followed, such as the use of strong types and foreign key constraints

Data Protection

- Transport Layer Security (TLS) used for web application and web service transmissions
- SSL certificates are issued from a reputable certificate authority (CA)
- Storage of sensitive data is limited and encrypted at rest

Configuration & Operations

- Rigorous change management process for software development life cycle and IT infrastructure
- Design patterns are utilized
- Design and code reviews are performed
- Security checks are integrated into the QA testing process
- An incident management plan is in place
- Monthly communications with product and design teams on cyber threats and best practices

Authentication

- Credentials are not stored directly within application code
- Database credentials are securely stored and protected
- Generic responses are provided for authentication failures

Session Management

- A best-practice framework for web session management is employed
- Transactions and distributed transactions help manage data
- Industry standard object-to-relational mapping (ORM) frameworks are used
- Queues provide for guaranteed delivery of information Input and Output Handling
- Parameterized SQL queries are used to prevent SQL injection
- Defenses are in place to prevent cross-site scripting

User Access control

- Access control checks consistent across web application
- Least-privileged model for web application
- Accounts segregated by customer
- Single Sign-On (SSO) is available