Criminal Justice Information Security (CJIS) Guide for ShareBase in the Hyland Cloud

Introduction

The Criminal Justice Information Security (CJIS) Policy is a publically accessible document that contains the minimum security requirements needed to allow access to Federal Bureau of Investigation (FBI) CJIS information. The CJIS Security Policy details the required controls to protect Criminal Justice information through its entire lifecycle, from creation to destruction. It is the responsibility of law enforcement agencies and CJIS Systems Agencies to ensure CJIS compliance of applications and vendors.

ShareBase by Hyland is an enterprise cloud-based file sharing solution. The ShareBase application and supporting infrastructure are maintained within the Hyland Cloud and the application is provided as a cloud service. The purpose of the "Criminal Justice Information Security (CJIS) Guide for ShareBase in the Hyland Cloud" is to assist a ShareBase site administrator in identifying which compliance requirements in the CJIS IS Policy that might apply to a ShareBase solution within the Hyland Cloud.

Executive Summary

ShareBase is an enterprise file-sharing product by Hyland. When using the product, a customer retains ownership and control of their solution and information. The Hyland Cloud's ISO-aligned policies and procedures support ShareBase as a secure hosted cloud service.

"Criminal Justice Information Security (CJIS) Guide for ShareBase in the Hyland Cloud" provides information relative to the Hyland Cloud platform that can be helpful to a ShareBase site Administrator when determining if a ShareBase solution complies with applicable CJIS Security Policy requirements.

CJIS Security Policy and Implementation

There are 13 areas incorporated in the CJIS Security Policy that a ShareBase site administrator should evaluate to ensure a ShareBase solution complies with CJIS requirements. The following information is specific to the Hyland Cloud as it relates to these 13 security policy areas.

1. Information Exchange Agreements

The Hyland Cloud maintains a Vendor Management Program to ensure the protection of assets that are accessible to vendors. The program establishes procedures for an extensive review of potential vendors; an evaluation mechanism of risk associated with a vendor; a contract review process for strict compliance to requirements; and confirmation that services provided meet contractual commitments.

A prospective Hyland Cloud vendor undergoes an extensive due diligence review, which includes an assessment of legal, financial and ethical risk. Hyland Cloud management recognizes the criticality of validating that a vendor maintains the information security terms and conditions of an agreement. To ensure ongoing adherence, vendor services, reports and records are monitored, reviewed and audited regularly.

The Vendor Management Program ensures that vendor contracts comply with Hyland Cloud requirements, which include compliance with federal, state and industry standards. Vendor agreements must include an agreed-upon level of information security and service delivery.

2. Security Awareness Training

The Hyland Cloud policies and procedures ensure that employees understand their responsibilities concerning information security within the Hyland Cloud.

When hired, all Hyland Cloud personnel must participate in an orientation covering the Hyland Cloud Information Security policies and procedures. Further training is required for all Hyland Cloud personnel on an annual basis. Employees must acknowledge, in writing or electronically, that they have participated in the required training and that they have read, understand and will abide by the Hyland Cloud Information Security policies and procedures.

Hyland Cloud personnel are required to participate in annual Security Awareness Training and Education (SATE). The Hyland Cloud Information Security policies and procedures, industry standards and applicable laws and regulations are included in the training.

The Hyland Cloud SATE program is administered and monitored using Hyland's internal system. Security policies are audited and reviewed annually by the Hyland Cloud leadership team.

3. Incident Report

The Hyland Cloud Information Security Incident Management policy provides a structured and effective approach to the management of an information security incident. Included in the Hyland Cloud policies are defined procedures for identification, collection, acquisition and preservation of information.

Procedures are in place for escalation and notification in the event of a qualified security incident. Qualified personnel promptly complete investigative steps in the event of a security incident. For other types of incidents, the applicable response steps are completed.

Hyland Cloud personnel follow a standardized response sequence when responding to a security incident. The Hyland Cloud Security Incident Response phases include:

- Incident Trigger
  - When an incident occurs, it is logged and an initial notification is sent to the appropriate Hyland Cloud team members
- Evaluation
  - Each incident is analyzed and information is gathered to formalize a response plan specific to the event
- Escalation
  - The scope and form of the specific response required is determined and coordination with any additionally needed resources is completed
- Response
  - Assigned responsibilities are performed to resolve and manage the incident.

- Recovery
  - Steps to restore the impacted system(s) are performed
- De-escalation
  - Normal processes are reinstated
- Post-incident Review
  - Secondary actions occur and a review is completed to improve procedures for future incident response

The goal of the Hyland Cloud incident response is to prevent data loss and to protect information.

4. Auditing & Accountability

Hyland Cloud policies for information security are embodied in the Hyland Global Cloud Services (GCS) Information Security (IS) Policy Suite. Information Security, as defined in the Hyland GCS IS Policy Suite, is protecting and preserving the confidentiality, integrity, availability and security of information.

To ensure controls are in place to safeguard hosted customer data, the Hyland Cloud policies and procedures align with IEC/ISO 27001:2013, including Annex A controls. In addition, the Hyland Cloud aligns with guidelines found in NIST (National Institute of Standards and Technology) Special Publications including controls from standards such as SP 800-53, SP 800-171, SP 800-88, where applicable.

To verify adherence to the controls detailed in the Hyland GCSGCS IS Policy Suite, the Hyland Cloud is SOC 2 audited on an annual basis. The Hyland Cloud SOC 2 audit is performed by a qualified external agency that extensively reviews policies, measures the Hyland Cloud against those policies, and makes a determination against those policies concerning Hyland's procedures and preparedness. To further support adherence to the documented GCS IS Policy Suite, the Hyland Governance, Risk and Compliance (GRC) team completes internal audits on a quarterly basis.

Global Cloud Services uses tools within the Hyland Cloud platform that aggregate and centralize security events as they are generated. The events are collected directly from their source. Hyland Global Cloud Services uses dashboard capabilities to gain insight into performance metrics and to complete health checks for a hosted customer's solution. The data is monitored for conditions concerning both security and availability. Alerts are generated that triggers investigatory activity by appropriate GCS resources. Staff is available 24/7/365 to respond to alerts from these systems. Logs are hashed for integrity verification. Access to the system log location is set up with strict limited access. Deletion and modification to the logs from within the tool is prohibited. These logs are kept in non-repudiation format and kept for one year. Access to the central log repository is limited to a small team, based on job role.

The Hyland Cloud is housed in collocated data centers that are ISO 27001 certified and SOC 1 or SOC 2 audited on an annual basis. Visitors are not permitted into the data center unless they are approved using the documented Hyland Cloud change management procedure and then proper authorization provided to the data center.

On an annual basis, an independent third party completes penetration testing of the Hyland Cloud network infrastructure within each Hyland Cloud data center. Hyland reviews the results of the third-party tests, and any identified risks are remediated. Hyland then creates a response document.

On an annual basis, ShareBase functionality is subjected to an application penetration test, performed by an independent third party, in order to assess its security. This is done in addition to the continuous penetration testing done by internal security testers. The Hyland security team reviews the results of the third-party tests and identified risks are prioritized for remediation. The identified risks are remediated and a Hyland response document is created.

5. Access Control

Hyland Cloud has strict, well-documented access control policies that govern all systems, networks and applications. They are controlled by a unique user ID and authentication using a comprehensive password schema. This includes a requirement that all vendor supplied default passwords must be changed before installation.

The Hyland Cloud is structured to ensure users are allocated appropriate rights based on their role and job responsibilities. The Hyland Cloud supporting staff is comprised of teams separated based on the functional areas required to operate a hosting environment and provide related services. This organization allows account owners to apply consistent standards, including the principles of least privilege and separation of duties.

Each Hyland employee that is granted administrative access to the Hyland Cloud is provided with unique credentials to a virtual desktop environment. Use of this account requires a username, password, and electronic token (multi-factor authentication). The electronic token is rotated every 60 seconds.

Global Cloud Services manages all data stored within ShareBase as though it contains personally identifiable information (PII). The Hyland Cloud data handling policies provide for a secure method of transfer for customer data; tracking of the data within Hyland; and specific restrictions on use, storage, and retention of such data. All Hyland Cloud personnel must acknowledge and abide by it.

Within the ShareBase environment, the ShareBase site administrator, who is designated by the end user organization, determines who has access and if any shared access should be permitted by creating and managing ShareBase accounts.

ShareBase site administrators have all the privileges of a user administrator, but can also create new site and user administrators; create and modify password policies; adjust deployment settings; add new products to the deployment (if applicable); and create and modify libraries.

The default for the ShareBase application is to provide individual accounts for the users within the customer organization. The activities of users are tracked in the ShareBase application.

Share by link passwords are secured using the same technology as user passwords, including salted Password-Based Key Derivation Function 2 (PBKDF2). The links support enforcement of

the active password policy, either custom or default, for the deployment. This ensures that a customer's document links are as secure as their user accounts.

If an individual leaves the organization voluntarily or through termination, the ShareBase site administrator can lock that user's account. When removing the user account, the site administrator can also transfer ownership of documents and shared files to another user.

ShareBase data is purged through end user action or when customer authorization is provided to Hyland. Hyland deletes customer data according to methods recommended in the NIST Special Publication 800-88, Guidelines for Media Sanitization for sensitive data. Confirmation is completed to ensure that data has been destroyed and cannot be retrieved by data, disk, file recovery utility or any other commercially available recovery method.

6. Identification & Authentication

The Hyland Cloud adheres to ISO-based polices governing access control. A minimum two-factor authentication is used for Hyland Software technical personnel managing the Hyland Cloud. The multi-factor authentication requires the usage of a token that is rotated every 60 seconds.

Strong password controls are enforced for all employees who are granted administrative access to the Hyland Cloud. Policy elements include complexity, rotation, usage, sharing/distribution, and storage/encryption concerns. Hyland Cloud policy currently requires a minimum length of 12 characters and a password rotation every 6 months. Additionally, passwords cannot be reused within four rotation cycles. If failed logins occur, the account will be locked out after five consecutive failed authentication attempts.

ShareBase site administrators can create and modify password policies within their ShareBase deployment.

7. Configuration Management

The Hyland Cloud platform is purposefully built to support ShareBase as a cloud service. System configuration standards for all components are developed, documented, kept current and applied with consistency. Configuration standards are developed to incorporate industry best practices and to mitigate known security vulnerabilities.

The N+1 architecture design supports a highly available cloud environment. A multitier, or N-tier architecture is used to support presentation, application, processing and data services. For enhanced security in the Hyland Cloud platform, technologies such as firewalls, intrusion detection and prevention, and vulnerability management are used.

To ensure the availability of ShareBase information, three copies of all customer data are maintained. All data is replicated to an active secondary file server within the primary hosting facility. A third data copy is replicated to the secondary/remote hosting facility.

Within the Hyland Cloud, advanced storage technologies are used for disk checking and corrective measures, which allows for data protection of stored information. The replication

technology used replicates data to two independent locations for every bit that is changed. This replication process checks the integrity of the read disk prior to replicating the data. Active scanning technology and separate customer data storage three layers deep within the network to protect information housed within the Hyland Cloud.

A variety of server hardening techniques are implemented including use of ACLs, deploying servers with one primary function, changing vendor supplied defaults, eliminating unnecessary functionality.

ShareBase customers are empowered to manage their ShareBase solutions as they see fit, based on their organizational needs. ShareBase site administrators can create a corporate password policy to meet their specific corporate requirements. Some organization require passwords to follow a corporate standard that may differ from the ShareBase default. For this reason, ShareBase allows customers to configure a password policy that is unique to their deployment.

The ShareBase site administrator, who is designated by the end user organization, determines who has access. A ShareBase site administrator may configure the number of failed attempts that may be made against an account before that account is locked out of the system.

Share by link passwords are secured using the same technology as user passwords (i.e. salted PBKDF2) and they enforce the active password policy (either custom or default) for the deployment. This ensures that a customer's document links are as secure as their user accounts.

8. Media Protection

Media protection within the Hyland Cloud is consistent with ISO-based policies and procedures for information security.

When a storage device has reached the end of its useful life, the decommissioning process prevents customer data from being exposed to unauthorized individuals.

Media that contains customer data that is no longer needed for business or legal purposes is destroyed in a manner that is consistent with the standards and techniques described within NIST SP 800-88. A record is maintained of all media disposed of in accordance with this policy and the record is retained in accordance with Hyland's retention policy. If a hardware device is unable to be decommissioned using these procedures, the device will be virtually shredded or physically destroyed in accordance with industry-standard practices.

All media files are encrypted at rest and in transit in ShareBase, and access to files is controlled via ShareBase security. Any modification to files is tracked in the software via Activity Log/Administrator Log and the original file is always available.

9. Physical Protection

Physical protection within the Hyland Cloud is consistent with ISO-based policies and procedures for information security. The Internet Service Providers provide internet connectivity, physical security, power, and environmental systems and services for the Hyland

Cloud platform. The Hyland Cloud data centers are ISO 27001 certified and SOC1 or SOC2 audited on an annual basis.

In the Hyland Cloud, all data transfer is encrypted. By default, the Hyland Cloud uses:

- Advanced Encryption Standard, AES-256 bit
- Transport Layer Security, TLS 1.2
- Secure Shell, SSH2 transport encryption
- AES-256 bit Secure Sockets Layer, SSL

Using these tools, data is encrypted both from the workstation to ShareBase infrastructure and vice versa.

When customer data is replicated from the primary data center to the secondary data center, it is encrypted and transmitted over the internet via a Virtual Private Network (VPN) tunnel. Encryption at rest is standard within ShareBase, where a unique encryption key is used for each individual customer deployment.

10. Systems and Communications Protection and Information Integrity

Hyland Cloud policies and procedures include system management measures to ensure the protection and integrity of ShareBase information. Hyland uses commercially available safeguards to protect the Hyland Cloud platform and hosted data from intrusion, attack and virus infection.

Intrusion detection systems monitor network traffic and alert personnel to any suspected compromises within the Hyland Cloud platform. Data transferred between systems is locked down via network segmentation and permissions.

The hosts within the environment employ anti-virus software and the anti-virus signatures are updated daily by an automated signature repository. Anti-malware is installed and updated regularly within the Hyland Cloud platform.

ShareBase does not perform malware analysis or scanning. We encourage our customers to employ anti-virus software on their endpoints.

The Hyland Cloud uses AES - 256 bit TLS 1.2 and SSH2 transport encryption. When using 256 bit SSL, data is encrypted both from the workstation to ShareBase Infrastructure and vice versa. Encryption at rest is standard within ShareBase.

11. Formal Audits

The Hyland Cloud data centers are ISO 27001 certified and SOC 1 or SOC 2 certified annually. The Hyland Cloud environment aligns with the IEC/ISO 27001:2013 including Annex A controls, and is SOC2 audited annually. GCS's Governance, Risk and Compliance team perform quarterly security audits and annual risk assessments.

12. Personnel Security

The Hyland Cloud security program focuses on access controls as a critical security and management consideration.

The Hyland Cloud organization is structured to ensure users are allocated appropriate rights based on their role and job responsibilities. The Hyland Cloud supporting staff is comprised of teams separated based on the functional areas required to operate a hosting environment and provide cloud content services. Within this functional team structure, consistent standards are maintained, including the principles of least privilege and separation of duties.

All Hyland Cloud personnel must read and acknowledge the Hyland Cloud Employee Process Manual. This manual includes a summary of the most critical security and privacy policies and procedures and must be acknowledged before access can be provisioned. Security policies are audited and reviewed annually by the Hyland Cloud leadership team. All Hyland Cloud personnel must sign a non-disclosure agreement before access is allowed.

ShareBase site administrators have control over who within their organization may have a ShareBase account. If someone leaves the customer's organization or is terminated, the ShareBase site administrator can transfer ownership of documents and shared files to another user account, and can lock accounts as needed.

13. Mobile Devices / Wireless Protocols

Mobile devices are not permitted in the administration of the Hyland Cloud. Additionally, wireless technologies are not used for the administration of the Hyland Cloud.