HxGN SFx

Security Policy

Overview

The purpose of this Security Policy document is to outline the various security features and policies of HxGN SFx, as well as the security obligations required of the Users in respect of their access to and use of HxGN SFx Cloud Services ("Services"). Capitalized terms used but not defined in this Security Policy ("Policy") have the meanings given to them in the Cloud Services Agreement.

Security Summary

- Two Factor authentication is used for all HxGN SFx administrative staff with access to back end systems of Services. Access to such systems is not provided to Users.
- Single Factor authentication is used by default for the Customer's Users.
- Regular security audits and assessments are carried out, including PEN testing of HxGN SFx Services.
- Security event monitoring is utilized to provide 24/7 visibility of activity.
- Communications between Customers and the Platform is encrypted over secure protocols using approved digital certificates.
- HxGN SFx will not accept or manage Customer-provided encryption keys in any part of the Platform.
- Regular infrastructure software updates (e.g. operating systems, databases, security software, etc.) are deployed automatically and through the provision of planned maintenance.
- HxGN SFx servers utilize industry leading anti-virus scanning solutions which are updated daily.
- HxGN SFx administrative staff on HxGN SFx cloud infrastructure are prohibited from access to internet browsing services and e-mail clients.
- Customer access is monitored and controlled via the Platform.
- Physical data center security is maintained by our public cloud third party service providers (e.g. Microsoft).
- Although HxGN SFx leverage third party service providers in respect of the public cloud platform, only authorized employees and third-party service providers have direct access to the Customer Data within the Platform.
- For security purposes, HxGN SFx does not provide anyone outside of the Hexagon and its Affiliates' business teams and authorized third-party service providers and auditors, with specific information regarding the types of security equipment, security software vendors, versions, protocols, etc. (e.g. details of Firewall equipment, Anti-Virus and Anti-Malware vendors & versions, etc.) utilized in securing Services.

HxGN SFx Services & Interface Security

- Where appropriate, HxGN SFx to ensure that user data inputs to HxGN SFx Services are of appropriate data type and format.
- Prior to onboarding to HxGN SFx, Customers are required to review and agree to a Hexagon-approved cloud services agreement and acceptable use policy.

Identity & Access Management

- Access to information systems monitoring and audit tools is restricted to authorized personnel.

- Customer's Users are authorized and granted access by the Customer administrator and this process is recorded.
- Source code libraries used for the provisioning of HxGN SFx are limited to authorized personnel. Where feasible, source code libraries maintain separate project workspaces for independent projects. HxGN SFx staff and contractors used in the provision of HxGN SFx are granted access only to those work spaces which they need access to perform their duties. Source code libraries enforce control over changes to source code by requiring a review from designated reviewers prior to submission. An audit log is maintained detailing modification to all source code libraries.
- Access by third-party personnel to the Customer tenant is granted based upon business requirements and only with appropriate management authorization.
- Where feasible, role-based access controls are used to allocate logical access to a specific job function or area of responsibility, rather than to an individual.
- Password policies for HxGN SFx Platform are managed through authentication provider policy that specifies minimum requirements for password length and complexity.
- Customers and its Users are responsible for keeping passwords from being disclosed to unauthorized parties and for choosing passwords with sufficient entropy as to be effectively non-guessable.

Encryption & Key Management

- Hexagon and its Affiliates have identifiable owners of encryption keys and certificates, and certificate management tools.
- HxGN SFx restricts access to Customer Data. HxGN SFx encrypts Customer Data transmitted to and from the Platform over public networks.
- HxGN SFx uses commercially available best practices for encryption standards.

Audit & Compliance

- HxGN SFx customers are responsible for their compliance with applicable laws and regulations relating to their use of the Platform and Services.
- To maintain the security and confidentiality of the entire Platform, HxGN SFx does not allow customers to conduct individual security audits and/or security testing.
- In respect of applicable data protection laws, direct access to the Platform networks, infrastructure, systems and/or physical premises or those belonging to third party service providers, will not be provided to the Customer or auditors on behalf of Customer.

Business Continuity Management

- The data centers facilities used to deliver HxGN SFx follow industry certification standards. These facilities are monitored and controlled 24/7 by trained staff.
- The architecture of the Platform and its infrastructure is designed with redundancy where appropriate and to minimize single points of failure.
- As part of Services, HxGN SFx backs up infrastructure and Customer Data daily and validates the restoration of data periodically for recovery purposes.
- HxGN SFx uses equipment belonging to third party service providers placed in facilities which have been engineered to be protective from theft and environmental risks such as fire, smoke, water, dust, vibration, earthquake, and electrical interference.
- Access to system documentation is restricted to the respective HxGN SFx personnel based on their job roles.
- System documentation is reviewed regularly to reflect any changes to production systems, contractual and business requirements.

Change Control & Configuration Management

- HxGN SFx has a Change and Release management process to control implementation of major changes including:

- The identification and documentation of the planned change -
  - Identification of business goals, priorities and scenarios during product planning
  - Specification of feature/component design
  - Operational readiness review based on a pre-defined criteria/check-list to assess overall risk/impact
  - Testing, authorization and change management based on entry/exit criteria for DEV (development), QA (Integration Testing), Pre-Prod (Pre-production) and PROD (production) environments as appropriate.
  - Changes are tested in various test environments and approved prior to deployment into production.

Data and Data Center Security & Information Lifecycle Management

- HxGN SFx is a multi-tenant environment and separates customer data based on customer organization. Strict testing is performed to ensure data is not visible outside of the customer organization.
- HxGN SFx applies the segregation of duty principle for non-production and production environments.
- Access to data centers used in the provision of HxGN SFx is restricted by job function so that only essential personnel receive authorization to manage the Services. Physical access authorization utilizes multiple authentication and security processes including: badge and smartcard, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication for physical access to the data center environment.

Security by Design

- The HxGN SFx team practices security by design principles, focused at coding standardized, repeatable, automated architectures so that security and audit standards remain consistent across multiple environments. We adhere to the following practices:
  - Controlled, standardized build process
  - Controlled, standardized update process
  - Automated infrastructure and code security testing as part of CI/CD pipeline
  - Enforced configurations in production
  - Mature monitoring tools with data subject to intelligent, well-trained human assessment
  - Little to no direct human intervention in the production environment

Infrastructure & Virtualization Security

- The Operating Systems used on HxGN SFx server estates are built to only run services that are required by the business operation of these systems. Anti-malware and Anti-virus software is deployed as standard and logging is enabled as standard build procedure.
- No wireless network environments exist within the data center network environment used for the provision of the Services.

Human Resources & Security Awareness

- Employees directly engaged in the management of critical Platform functions are required to successfully complete a background check as part of the hiring process. Background checks may include, but are not limited to, review of information relating to a candidate's education, employment, and criminal history.
- All contractor staff directly engaged in the provision of HxGN SFx are required to take any training determined to be appropriate to the services being provided and the role they perform.