

Spectades HxGN EAM Cloud

Security Policy

1. Overview and Definitions

The purpose of this Security Policy document is to outline the various security features and certifications of Cloud Services as well as the security obligations required of the Authorized Users in respect of their access to and use of Cloud Services. Defined terms not explicitly defined herein shall be as defined in the Spectades HxGN EAM Cloud Services Agreement.

As Spectades has a back to back delivery agreement with Hexagon, Hexagon is delivering the Spectades HxGN EAM Cloud as in this document referred to.

“Data Center(s)” means the data center(s) procured from Third Party Service Providers from which the Cloud Services are provided as determined by Hexagon.

2. Security Summary

The following list highlights the security features and certifications of Cloud Services:

- The current certifications held by Spectades as contracted with Hexagon can be found at <https://hexagon.com/company/divisions/assetlifecycle-intelligence/technology-compliance-standards>. The certifications held may vary by the applicable Software Product. Customers will be notified in the event Spectades discontinues a security compliance standard for any Software Product in which they have a subscription.
- Two-factor authentication is used for all Hexagon administrative staff with access to back-end systems of Cloud Services. Access to such back-end systems is not provided to Customer or Authorized Users.
- Two-factor Authentication/Multi-factor Authentication is used by default for the Customer’s Authorized Users.
- Regular security audits and assessments are carried out including penetration testing of Software Products running in the Cloud Services.
- Security event monitoring is utilized to provide visibility into risky activity.
- Communications between customers and Cloud Services are encrypted over secure protocols using approved digital certificates.
- Cloud Services uses various encryption mechanisms to protect Customer Data.

- Hexagon cannot and will not accept or manage Customer-provided encryption keys in any part of the Cloud Environment including the Customer Environment.
- Regular infrastructure software updates (e.g. operating systems, databases, security software, etc.) are deployed through the provision of Planned Maintenance.

All Cloud Services servers utilize industry-leading heuristic and signature-based anti-virus (AV) scanning solutions, which are updated daily.

- Authorized User access to internet browsing services and email clients is prohibited.
- File transfer activity is strictly controlled and audited including multi-engine AV scanning on files uploaded to the Customer Environment file system.
- Customer Environments are logically separated utilizing a layered approach of security controls.
- Physical Data Center security is maintained by the applicable public Cloud Third-Party Service Providers (i.e. Microsoft and Amazon).
- Although Cloud Services leverage Third Party Service Providers in respect of the public cloud platform, no employees of such Third-Party Service Providers have direct access to the Cloud Environment or the Customer Data within the Customer Environment.
- For security purposes, Spectades or Hexagon **does not** provide anyone outside of the Cloud Services business team and Spectades or Hexagon authorized third-party 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 the Cloud Services.

3. Security Policy Details

Software Products & Interface Security

- Hexagon applies a Security Development Lifecycle (a software security assurance process used to design, develop, and implement the Software Products) for the Software Products which run in the Cloud Environment.
- Cloud Services defines acceptable standards to ensure that data inputs to Software Products are accurate and within the expected range of values. Where appropriate, data inputs are sanitized or otherwise rendered safe before being inputted into a Software Product system.

- Prior to onboarding to Cloud Services, customers are required to review and agree to the Spectades HxGN EAM Cloud Services Agreement, which includes usage rights (including incorporating an Acceptable Use Policy).

Identity & Access Management

- Access to information systems audit tools are restricted to authorized personnel within Cloud Services.
- Hexagon requires that access to Cloud Services and Customer Data in the Customer Environment, granted on behalf of Customer, is based on Customer's business justification, with the Customer's authorization and limited based on "need-to-know" and "least-privilege" principles.

All Authorized Users are required to be vetted by Customer before access may be provided to any network resource and this process is recorded and controlled by Customer.

- Cloud Services have formal monitoring processes to include frequency of review for Standard Operating Procedures and review oversight processes and procedures. Access by Customer's third-party personnel or subcontractors to the Customer Environment is, subject to being allowed under the agreement with the customer, granted based upon business requirements and only with the Customer's explicit authorization.
 - Access to information assets within the Customer Environment is granted by Customer based upon need to know and least-privilege principles.
 - 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.
- Customer designated Cloud Services application administrators and data owners are responsible for reviewing who has access to Cloud Services applications and data on a periodic basis. Regular access review audits occur to validate appropriate access provisioning, modification and timely de-provisioning has occurred.
- Password policies for the Cloud Services are managed through authentication provider policy that specifies minimum requirements for password length, complexity, and expiry. All passwords must be at least twelve characters in length including one uppercase letter, one special character (except '<' and '&'), and one numerical digit. All passwords are set to have a specified expiry period as determined by Hexagon.
- Customers and their Authorized 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 has identifiable owners of encryption keys/certificates and key/certificate management standards are in place via Hexagon's Third-Party Service Provider(s) in respect of the Cloud Services.
- Hexagon has policies, procedures, and mechanisms established for effective key/certificate management to support encryption of data in transmission for the key components of the Cloud Services.
- Encryption keys used within the Cloud Services infrastructure are managed by Hexagon and Third Party Service Provider(s). Keys are stored in secure vault which is used to manage and control key access. Dual controls are required for essential functions such as generating, deleting, or exporting keys. Key custodian forms are required as part of the generation of new keys. Cryptographic management is undertaken by a specific team within the security group.
- Hexagon restricts access to Customer Data. Hexagon encrypts Customer Data transmitted to and from the Data Centers (where Cloud Services are hosted) over public networks. Hexagon uses encryption for replication of non-public Customer Data between Data Centers.

Hexagon endeavors to use the highest encryption standards available, in line with industry best practices, technical functionality and to the extent it does not store key data.

- Encryption for Customer Data in transit and encryption for Customer Data at rest is available.
 - o **Encryption in Transit.** Cloud Services customers access their estate or application over https using certificates from trusted certificate authorities. Customers are required to use TLS version 1.2 or above on the browser to access the Cloud Services. All end-user access to Cloud Services attempted over HTTP are redirected to HTTPS.
 - o **Encryption at Rest.** The Cloud Services leverage cloud provider storage encryption and it is encrypted and decrypted transparently using AES encryption.

Authentication & Authorization

The Cloud Services provide customers with several authentication options that can be used simultaneously within a Customer Environment. Customers can integrate their Customer Environment with their Identity Provider (IdP) via single sign-on (SSO) technologies, such SAML, to access multiple applications. This means that Authorized User accounts can be managed within the customers' existing processes and standards.

- **Security Assertion Markup Language (SAML).** The Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between security domains. SAML exchanges security information between an identity provider such as the customer's ADFS and a service provider such as the Cloud Services.

- **Built-in “native” authentication.** In the case of native authentication, passwords are managed solely by customers within the Cloud Services. This is the only authentication method where both the username and password are stored within the Cloud Services. When using native the Cloud Services authentication, properties such as the length, complexity, rotation, and uniqueness of passwords requirements are specified and documented in a password policy. For customers who will be using the Cloud Services’ native authentication, 2FA is a mandatory requirement.

OAuth 2.0. Smart APIs are secured with OAuth2.0 or OIDC. The only OAuth flows supported for customers connecting to Smart APIs are OAuth Authorization Flow with PKCE and OAuth Client Credentials. For customers who have Cloud Services subscriptions that include API access, an Authorized User can be configured to have access to the API with their Cloud Services credentials. After an Authorized User is configured to have access to an API, they can connect to the API using their Cloud Services credentials with the OAuth Authorization Flow with PKCE. The Authorization Flow with PKCE is strictly limited to integrations that require user interaction and the applicable user of the integration/application passes their specific respective authorization to the API. For customers who have server-to-server (non-user interactive) integrations, these are only permitted by using the OAuth Client Credentials flow. Authorized Users who are Customer Environment Administrators can issue a set of Client Credentials for their organization by contacting support.

SMART API

The Cloud Services may include Smart APIs to allow customers to build on and benefit from the Cloud Services by creating software, services, or modules that connect to Spectades’s platform or have access to the data within Spectades’s platform via our APIs (an “Integration”).

- Customers will only access the API using OAuth or an API key. If customers have an Integration, the Authorized Users must have the option to log in via OAuth or their API key. Customers must not prompt Authorized Users to provide their Cloud Services username, password, or other security prompts.
- API usage at all times must be compliant with the Documentation and Acceptable Use Policy. APIs may under no circumstance be used to modify or circumvent the setup of the Cloud Services infrastructure and policies. Hexagon may from time to time monitor and confirm Customer’s proper usage of the Smart API.
- Spectades may update or modify the APIs from time to time by posting the changes on the Cloud Services website or notifying customers via email. These changes may affect the use of the APIs or the way customers’ Integrations interacts with the APIs.

Audit & Compliance

- Each year, Hexagon will undergo a third-party audit of the Cloud Services by internationally recognized auditors to validate that Hexagon has independent attestation of compliance with its ISO 27001 aligned policies and procedures for security, privacy, and continuity.

- Hexagon implements and maintains appropriate technical and organizational measures, internal controls, and information security processes to ensure protection of Customer Data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction.
- A process has been established for identifying and implementing changes to services in response to changes in applicable statutes and regulations.
- Cloud Services customers are responsible for compliance with laws and regulations applicable to their industry or particular use of Cloud Services.
- To maintain the security and confidentiality of the entire Cloud Environment Hexagon **does not** allow customers to conduct individual security audits and/or security testing (including penetration tests), but Hexagon will share the AICPA SOC Type 2 report and copy of ISO 27001 certificates, if available for the applicable Software Product, which are conducted by independent third-party ISO auditors, with customers upon request (with specific information regarding the types of security equipment, security software vendors, versions, protocols, etc. used to secure Cloud Environment **redacted**).
- In respect of Data Protection Legislation, direct access to Hexagon's networks, infrastructure, systems and/or physical premises or those belonging to Third-Party Service Providers, will not be provided to either Customer or a third-party auditor on behalf of Customer. In such regard, Customer shall rely, in respect of Hexagon or Hexagon Group Companies (as applicable) on the above provision of summary results, and in respect of Third-Party Service Providers on such information and reports as is customarily made available by such applicable Third-Party Service Provider.

Business Continuity Management

- Business continuity for the Cloud Services are tested on a regular basis.
- The Data Centers facilities used to deliver Cloud Services follow industry certification standards. These facilities are monitored and controlled 24/7 by trained staff.
- The architecture of the Cloud Environment is designed to facilitate failover conditions and to minimize single points of failure while maintaining secure data flow for Customer Data within the public cloud platform.
- As part of Cloud Services, Hexagon backs up infrastructure and Customer Data daily and validates restoration of data periodically for recovery purposes.
- Cloud Services 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.

- Standard Operating Procedures and system documentation is formally documented and approved by Hexagon management in respect of Cloud Services.
- Access to system documentation is restricted to the respective Hexagon teams within Cloud Services based on their job roles.
- System documentation is reviewed regularly to reflect any changes to production systems.
- Data retention policies and procedures for Cloud Services are defined and maintained in accordance with regulatory, statutory, contractual, and business requirements.

Change Control & Configuration Management

- Cloud Services 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 criterion/checklist to assess overall risk/impact; and
 - Testing, authorization and change management based on entry/exit criteria for DEV (development), INT (Integration Testing), STAGE (Pre-production) and PROD (production) environments as appropriate.
- Changes to the underlying infrastructure within the Cloud Environment are reviewed and tested, at a minimum, for their quality, performance, impact on other systems, recovery objectives and security features before they are moved into production.
- Changes are tested in various test environments and signed off prior to deployment into production.

Data and Data Center Security & Information Lifecycle Management

- Cloud Services classifies data according to the Cloud Services data classification scheme and then implements a standard set of security and privacy attributes. Hexagon does not classify data uploaded and stored by customers in Cloud Services but treats all Customer Data in accordance with the commitment outlined.
- The network environment upon which the Cloud Services resides has been designed to have multiple separate network segments. This segmentation helps to provide separation of critical, back-end servers and storage from the public-facing interfaces.

- Hexagon applies the segregation of duty principle to ensure that access to Production Customer Environments are restricted according to policy.
- Customer is responsible for all content and management of Customer Data and should take all reasonably expected and appropriate measures to make sure that only authorized and secure Customer Data is added or removed.

Governance & Risk Management

- The Cloud Services risk assessment framework is compliant with the ISO 27001 standards. An integrated part of the methodology is the Risk Assessment process. As part of the overall ISMS framework, baseline security requirements are constantly reviewed, improved, and implemented.
- Hexagon maintains a risk register and regularly assesses and reviews risk in accordance with its ISMS and ISO 27001 certification requirements.
- Hexagon performs an annual risk assessment of the Cloud Services environment resulting in a formal Risk Assessment report.
- Decisions to update policies and procedures are based on the risk assessment reports. Risk Assessments are regularly reviewed based on periodicity and changes emerging to the risk landscape. Policies and procedures may be updated if risk results alter the relevance of the policy or procedure.
- The Cloud Services Information Security Policy undergoes a formal review and update process at a regularly scheduled interval not to exceed once per year. In the event a significant change is required in the security requirements, it may be reviewed and updated outside of the regular schedule.
- Each management-endorsed version of the Information Security Policy and all subsequent updates are distributed to all relevant stakeholders. The Information Security Policy is made available to all new and existing Cloud Services staff for review. All Cloud Services staff represent that they have reviewed, and agree to adhere to, all policies within the Policy Documentation.

Infrastructure & Virtualization Security

- The network environment upon which the Cloud Services reside has been designed to have multiple separate network segments. This segmentation helps to provide separation of critical, back-end servers and storage devices from the public-facing interfaces. Network ACLs and filters are incorporated to segregate the traffic among the network segments.
- Anti-malware software is deployed as standard and logging is enabled as standard build procedure.

Human Resources

- All employees directly engaged in the provision of Cloud Services are required to successfully complete a standard background check as part of the hiring process, except where not permitted by local law. Background checks may include but are not limited to review of information relating to a candidate's education, employment, and criminal history.
- All employees directly engaged in the provision of Cloud Services take part in a sponsored security-training program and are recipients of periodic security awareness updates. Security education is an ongoing process and is conducted regularly to minimize risks.
- All contractor staff directly engaged in the provision of Cloud Services are required to take any training determined to be appropriate to the services being provided and the role they perform.
- All employees and third parties directly engaged in the provision of Cloud Services are required to sign nondisclosure agreements.

Security Incident Management

- Cloud Services abides by a robust process to facilitate and coordinate response to security incidents if one. A security event may include, among other things unauthorized access resulting in loss, disclosure, or alteration of data.
- Information security incidents are classified into severity levels and processed according to the severity level. Regular reporting of incidents is carried out for inclusion in management reporting.
- The Cloud Services incident response process follows the following phases:
 - **Identification** – System and security alerts may be harvested, correlated, and analyzed. Events are investigated by Hexagon operational and security organizations. If an event indicates a security issue, the incident is assigned a severity classification and appropriately escalated within Hexagon. This escalation includes product, security, and engineering specialists.
 - **Containment** – The escalation team evaluates the scope and impact of an incident. The immediate priority of the escalation team is to ensure the incident is contained and data is safe. The escalation team forms the response, performs appropriate testing, and implements changes. In the case where in-depth investigation is required, content is collected from the subject systems using best-of-breed forensic software and industry best practices.

- **Eradication** – After the situation is contained, the escalation team moves toward eradicating any damage caused by the security breach and identifies the root cause for why the security issue occurred. If vulnerability is determined, the escalation team reports the issue to product engineering.
- **Recovery** – During recovery, software or configuration updates are applied to the system and services are returned to a full working capacity.
- **Lessons Learned** – Each security incident is analyzed to ensure the appropriate mitigations applied to protect against future reoccurrence.
- If Cloud Services personnel determine that Customer Data was subject to unauthorized access, the Customer will be notified in accordance with the Agreement.