Intergraph Smart® Cloud Services

Security Policy

1. Overview

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.

2. Security Summary

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

- PPM maintains an ISO27001 certification for Information Security Management System used to deliver Cloud Services, which is independently audited on a regular basis.
- PPM has a validated and mature security program and risk treatment plan as part of ISO27001 Information Security Management System (“ISMS”).
- Two Factor authentication is used for all PPM administrative staff with access to back end systems of Cloud Services. Access to such back-end systems is not provided to Customer or Users (Authorized Users or otherwise).
- Two Factor authentication is used by default for the Customer’s Authorized Users.
- Regular security audits and assessments are carried out, including PEN testing of PPM Software Products running in Cloud Services.
- Security event monitoring is utilized to provide 24/7 visibility of activity.
- Communications between Customers and the Cloud Portal is encrypted over secure protocols using approved digital certificates.
- Storage of data in Cloud Services uses various encryption mechanisms to protect the data.
- PPM 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 AV scanning solutions which are updated daily.
- Authorized User access to internet browsing services and e-mail 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 by VLANs, firewalls and ACLs.
Customer access is monitored and controlled via the Cloud Portal.

Physical Data Center security is maintained by our public Cloud Third Party Service Providers (e.g. 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, PPM does not provide anyone outside of the Cloud Services business team and 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 Cloud Services.

3. Security Policy Details

PPM Software Products & Interface Security

- PPM applies a Security Development Lifecycle, a software security assurance process used to design, develop, and implement the PPM Software Products which run in the Cloud Environment.

- Cloud Services defines acceptable standards to ensure that data inputs to PPM 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 PPM Software Product system.

- Prior to onboarding to Cloud Services, Customers are required to review and agree to a Cloud master services agreement, which includes usage rights (including an Acceptable Use Policy).

Identity & Access Management

- Access to information systems audit tools are restricted to authorized personnel within Cloud Services.

- PPM have adopted applicable corporate and organizational security policies, including an Information Security Policy for the provision of Cloud Services. The policies are formally approved, published and communicated.

- PPM 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 Users are required to be vetted by Customer before access is allowed 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.

• Source code libraries used for the provisioning of Cloud Services are limited to authorized personnel. Where feasible, source code libraries maintain separate project workspaces for independent projects. PPM staff and contractors used in the provision of Cloud Services are granted access only to those workspaces 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. PPM maintains an audit log, detailing modifications to all source code libraries.

• Access by third-party personnel to the Customer Environment is granted based upon business requirements and only with appropriate management authorization along with the Customer’s explicit authorization.
  o Access to information assets within the Customer Environment is granted by Customer based upon need-to-know and least-privilege principles.
  o 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 Portal 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 PPM from time to time.

• Customers and its 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

• PPM has identifiable owners of encryption keys/certificates and key/certificate management standards are in place via PPM's Third-Party Service Provider in respect of the Cloud Services.
• PPM 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.
• PPM restricts access to Customer Data. PPM encrypts Customer Data transmitted to and from the Data Centers (where Cloud Services are hosted) over public networks. PPM uses private networks with encryption for replication of non-public Customer Data between Data Centers.

• PPM endeavors to use the highest encryption standards available, in line with industry best practices and does not store key data.

Audit & Compliance

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

• PPM 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 specific to their industry or particular use of Cloud Services.

• To maintain the security and confidentiality of the entire Cloud Environment PPM does not allow customers to conduct individual security audits and/or security testing, but PPM will share the summary results of regularly scheduled ISO 27001 audits, 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 applicable data protection laws, direct access to PPM’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 PPM 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 an annual 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, PPM 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 PPM management in respect of Cloud Services.

• Access to system documentation is restricted to the respective PPM 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 to regulatory, statutory, contractual or 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 criteria/check-list to assess overall risk/impact of 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 operating systems (OS) 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. PPM 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.

- Customer Data only moves outside these areas when backup data is replicated to a separate Data Center allocated for the Customer’s geographic region but provided by the same Third Party Service Provider for resilience and/or offsite recovery purposes which are available as Cloud Optional Services.

- PPM applies the segregation of duty principle to ensure that access to non-production and Customer Environments which are used in Production are restricted according to policy.

- PPM provides facilities accessible from within the Cloud Portal to facilitate the secure importing and exporting of Customer Data to and from their own corporate network to the Customer Environment (within the Cloud Environment). While mechanisms are in place to protect and control Customer Data during this process, the 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.

- Cloud Services abides by a formal policy that requires information assets (the definition of “information asset” includes Customer Data and virtual appliances) used to provide Cloud Services to be accounted for and have a designated information asset owner from a Customer perspective. Information asset owners are responsible for maintaining up-to-date information regarding their information assets. Customers are responsible for being the steward of their own data.
Access to Data Centers used in the provision of Cloud Services is restricted by job function so that only essential personnel receive authorization to manage Cloud 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.

Governance & Risk Management

- The Cloud Services risk assessment framework is based on the ISO27001 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.

- PPM maintains a risk register and regularly assesses and reviews risk in accordance with its ISMS and ISO 27001 certification requirements.

- PPM 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 1 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 Staff for review. All Cloud Services staff represent that they have reviewed, and agree to adhere to, all policies within the Policy documents. All Cloud Services contractor staff agree to adhere to the relevant policies within the Policy. Should one of these parties not have access to this policy for any reason, the supervising PPM representative is responsible for distributing the policy to them.

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.
• The Operating Systems used on Cloud Services server estates are built to only run services that are required by the business operation of these systems. Anti-malware 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 Cloud Services.

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. 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 in order to minimize risks. Cloud Services also has non-disclosure provisions in our employee contracts.

• 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:

  o **Identification** – System and security alerts may be harvested, correlated, and analyzed. Events are investigated by PPM operational and security organizations. If an event indicates a security issue, the incident is assigned a severity classification and appropriately escalated within PPM. 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 breached or otherwise subject to unauthorized access, the Customer will be notified as soon as possible.