Policy

Acceptable Use Policy

Hexagon’s Asset Lifecycle Intelligence and Safety, Infrastructure & Geospatial, and Hexagon Capability Center India IT Policy

Policy Manager: Elizabeth Henson

Document #: IT-POL-00073-2018

Status: APPROVED

Revision: 5.2

Scope: Global IT

Last Reviewed: 01 Dec 2022

Approval:	John T. Ferguson Executive Director, IT Global IT Services of the ALI and SIG divisions Hexagon	Signed: Date: 05 Dec 2022

Contents

1. Introduction

Hexagon’s Asset Lifecycle Intelligence (ALI), and Safety, Infrastructure & Geospatial (SIG), and Hexagon Capability Center India (HCCI) Information Technologies(Global IT) is committed to protecting our employees, clients, partners, and the company from illegal or detrimental, intentional, or unintentional actions by known or unknown persons.

This policy is in place to protect the employee and Hexagon.

Unauthorized and inappropriate use of the systems subjects Hexagon to unnecessary risks, including malware, cyber-attacks, viruses, legal sanctions, financial penalties, and revenue loss.

Hexagon management reserves the right to suspend access to Hexagon systems at any time.

Each employee is responsible for understanding this policy and to govern their actions and behavior accordingly.

2. Scope

This policy applies to the use of information, electronic and computing devices, and network resources used to conduct Hexagon business or interact with internal networks and systems, whether owned or leased by Hexagon, the employee, or a third party.

3. Definitions

The following definitions apply to this policy:

Employee is defined as

- All employees in Hexagon’s Asset Lifecycle Intelligence (ALI), Safety, Infrastructure & Geospatial (SIG), and/or Hexagon Capability Center India (HCCI) and other Hexagon entities requiring access to ALI’s, SIG’s, and/or HCCI’s networks, systems, and/or applications
- Interns / students participating as part of an HR approved program
- External contractors or external consultants
- Any other classification of an employee, external contractor or external consultant that may perform work on behalf of ALI, SIG, and/or HCCI, and/or its subsidiaries

Systems are defined as anything related, but not limited to:

- Hexagon owned computer equipment or other equipment that connects to a Hexagon network
- Employee owned computer equipment authorized to connect to a Hexagon network via Removable Media & BYOD Policy.
- Software
- Operating systems
- Storage media
- Domain accounts
- Email
- Networking services (internet, intranet, external networks)
- Web browsing
- Cloud services
- Other IT services/systems

Personal Data is defined as any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Examples of personal data are name, address, email address, phone number, IP address, gender, personal identification number, job position, resume (CV), salary, interests, purchase history, health information, location data, work capacity, marital status, log-in details, etc.

For additional information refer to Hexagon Data Protection site.

Intellectual Property means all forms of intellectual property including, but not limited to, patents, trademarks, copyrights, trade secrets, methodologies, logos, techniques, processes, know-how, formulae, algorithms, logic designs, screen displays, schematics, source and object code computer programs or software, documentation, mask work rights, design, ideas, product information, inventions and improvements thereto (whether or not patentable), and all works of authorship fixed in any medium of expression (including any form of online, digital, or electronic medium), whether or not copyrightable and whether registered or not.

Hexagon Proprietary Information is defined as all data/information developed, created, architected by employees, contractors, and consultants employed on behalf of Hexagon/Intergraph and data/information otherwise owned by Hexagon/Intergraph or its affiliates.

Trade Secret means any information, item, device, practice, process, method, practice, or technique, Hexagon/Intergraph uses in business and that is that is not generally known in the industry or to competitors of Hexagon.

Confidential means any data or information, tangible, or intangible, that is not generally known in the industry or to competitors of Hexagon.

4. Responsibilities

All employees are responsible for using good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Hexagon policies and standards, local laws, and regulations.

4.1 General Use and Ownership

4.1.1 All Hexagon Proprietary Information, on any medium or system, is and remains the sole property of Hexagon.

4.1.2 Employees must ensure that Hexagon Proprietary Information and Intellectual Property are always protected and secured and will not engage in any activity that could endanger the security of information on any system.

NOTE: If sensitivity/classification of any Hexagon information is unknown, the information must be treated as Confidential.

Employees may not copy Hexagon proprietary information, intellectual property or Trade Secrets onto

- Portable media (such as a disk, thumb drive, hard drive, etc.)
- Cloud based storage/application that have not been sanctioned by Hexagon
- Personal computing device

unless the employee has specifically been given the right to engage in such activity by management. Refer to Information Transfer and Storage of Hexagon Data.

Any Personal Data covered under the Hexagon Data Protection Compliance Programme Manual and commercially sensitive or confidential information (intellectual property, trade secrets, financial information, etc.) approved to be transmitted or provided to a non-Hexagon employee or a 3rd party application must be encrypted unless the employee has specifically been given the right to provide un-encrypted personal data, sensitive or confidential information by management.

4.1.3 Hexagon employees are required to report any loss, theft, or unauthorized disclosure immediately to their manager and IT. The report shall be logged as a security incident in the IT Service Ticketing System. Refer to the Refer to the Lost or Stolen Device Reporting Policy.

4.1.4 Before sharing Hexagon intellectual property, the employee must consult management to determine if a Non-Disclosure Agreement (NDA) is needed.

4.1.5 Employees are responsible for exercising good judgment regarding the reasonableness of personal use of systems.

- Personal use of a Hexagon-owned system by an individual who is not a Hexagon employee (this includes family members, friends, etc.) is prohibited.
- Individual departments are responsible for creating guidelines concerning personal use of systems. In the absence of such guidelines on personal use, and if there is any uncertainty, employees should consult their manager.
- Reasonable judgement should always be used regarding the personal use of Hexagon assets and systems.
- The employee should consult their manager if there are questions regarding what is or is not acceptable.

4.1.6 Only authorized employees may monitor equipment and/or network traffic in their efforts to support and maintain the systems. IT authorization shall be obtained by logging the activity in the IT Service Ticketing System.

4.1.7 Employees must not attempt to scan, stress, probe, test or carry out any activity that could compromise the confidentiality, integrity or availability of Hexagon, customer or third-party information assets, or systems unless authorized by management and IT is made aware of the planned activity. IT authorization shall be obtained by logging the activity in the IT Service Ticketing System.

4.1.8 Hexagon reserves the right to audit Hexagon's networks and systems on a periodic basis to:

- Protect employees and Hexagon
- Prevent unauthorized and inappropriate use of the systems that could subject Hexagon to unnecessary risks, including malware, cyber-attacks, viruses, legal sanctions, financial penalties, and revenue loss

4.1.9 Employees must not disable, reconfigure, or attempt to bypass any security measures, for example anti-virus, laptop encryption, multifactor authentication, etc. (unless explicitly authorized by IT).

4.1.10 Employees should make all reasonable efforts to protect passwords and to secure resources against unauthorized use (i.e., passwords, encryption keys, etc.). Passwords must never be visible in the employee's workspace, or physically attached to a computer (sticky note, piece of paper, label, etc.).

4.1.11 Employees must protect hardware in a way that reasonably prevents unauthorized users from accessing Hexagon's network, data, or systems (i.e., lock screen when a system is unattended in the office, do not leave laptops in an unguarded location, secure laptop with a cable lock, etc.).

4.2 Security and Proprietary Information

4.2.1 All devices that connect to any Hexagon physical or wireless network must comply with this policy. This is not limited to Hexagon owned devices, but also includes all devices not owned by Hexagon (e.g., devices owned by employee).

Removable Media & BYOD Policy and Mobile Device Best Practices provide guidance for the use of mobile devices provided by Hexagon and the use of personal mobile devices.

4.2.2 All passwords shall comply with the Hexagon password requirements. Refer to the INGRNET Password Policy.

4.2.3 Employees must lock their system or log off when the device is unattended.

All domain connected systems shall be secured with a password-protected screensaver or lock feature with an automatic timeout feature as defined in the Screen Lock Policy.

For exceptions, refer to IT Exceptions Policy.

4.2.4 Employees should use extreme caution when opening emails with attachments that are from unknown senders or if an attachment from a known sender appears suspicious. These could be associated with phishing or malware.

If there is any doubt about the validity of a suspicious email, please contact IT for assistance. Refer to Identifying and Reporting Phishing Emails.

4.2.5 Clear Desk / Protecting Non-Public Data

(a) At the end of each working day, any information that cannot be shared with the general public (i.e., Confidential, Intellectual Property, Hexagon Proprietary Information, internal only information, etc.) must be locked away in appropriate secure storage. Refer to IT Data Sensitivity Classification or divisional/group guidance for information regarding data classification.

(b) Hexagon will provide, at the request of the employee, suitable secure storage for any material required to be securely stored.

(c) When working in an environment with non-employees, do not leave non-public information where it can be accessed or viewed by others.

(d) Always assess the security of a location (i.e., Hexagon common areas or offsite locations) before leaving or making non-public information accessible to non-employees.

(e) Ensure people within close proximity cannot read sensitive information. This may involve temporarily working elsewhere.

(f) Any document or paper containing non-public information should be securely disposed (i.e., shredded).

(g) Non-paper information assets should be securely destroyed or discarded. Refer to the Media Destruction and Sanitation Policy.

4.2.6 Printing and Shredding Non-Public Information – refer to Printing and Shredding Best Practice Guide.

4.2.7 Employees must comply with the Anti-Virus Policy, Laptop Encryption Policy, Multifactor Authentication Policy and Remote Access Policy.

4.2.8 Any employee who receives a request from a representative of a governmental agency, law enforcement, regulatory agency, insurance company, customer, etc. for Hexagon information that is Confidential, Personal Data, Hexagon Proprietary Information, Intellectual Property or a Trade Secret must contact their Hexagon Legal Department before taking any action.

4.3 Email and Electronic Communication Activities

4.3.1 When systems (Hexagon provided or personal) are used to access the internet via Hexagon provided services, employees must always be aware that they represent the Hexagon organization.

4.3.2 Employees should not use their Hexagon email address for posting to newsgroups, online communities, and social media etc., unless the use is in direct support of their role and duties as a Hexagon employee.

4.3.3 Employees should not send any unsolicited electronic communications, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.

4.3.4 Sending SPAM emails and/or malicious electronic communications are prohibited.

4.3.5 Caution should be taken when using “reply all” or “forward” options for email that contains customer and/or commercially sensitive or confidential information, or that may pass Personal Data without having gained appropriate consent. Refer questions related to data protection to the division’s privacy lead(s) and/or privacy officer. Also refer to the Hexagon Data Protection Site.

4.3.6 If forwarding or sharing an email or other content derived from managed collaboration and communication tools (chat, online meetings, etc.) to customers or other external third parties, ensure the content of the communication is business appropriate. This includes:

- Removing Hexagon Proprietary Information or Intellectual Property not authorized for distribution.
- Gaining stakeholder approval before sharing or distributing internal communications.

4.3.7 Providing Hexagon employees, partners, or customer contact information to external parties without consent is prohibited.

4.3.8 Employees should not engage in any form of harassment via electronic means. This includes, but is not limited to, email, telephone calls, text messages, social media, etc., whether harassment is through the language used, frequency of messages, type of messages or size of messages.

4.3.9 Unauthorized use, forging of email header information, or other identification component of an electronic communication is prohibited.

4.3.10 Email solicitation with the intent to harass or collect personal (non-business related) information is prohibited

4.3.11 The creation, distribution, or the forwarding of "chain letters", "Ponzi" or any other electronic communication schemes is prohibited.

4.3.12 Do not send email messages using another employee's email account. If an employee has been properly authorized to send email on behalf of another employee, then it must be clear to the recipients the email was sent on behalf of the other employee.

4.3.13 Despite informality of email, it is held to be a written communication and the employee may bind the company by the commitments contained within the email.

4.3.14 Email and electronic communications are subject to monitoring in accordance with Hexagon's Employee Privacy Notice.

4.4 Social Media

4.4.1 The use of Social Media by Hexagon employees using Hexagon systems is subject to the terms and restrictions set forth in this policy and the *Hexagon Employee Social Media Policy* from the Hexagon Policy and Guidelines Downloads site.

4.4.2 Limited and occasional use of systems to engage in the use of social media is acceptable. Any activity from a system is subject to monitoring in accordance with Hexagon's Employee Privacy Notice.

4.4.3 When using social media, Hexagon employees are prohibited from revealing any Confidential, Hexagon Proprietary Information, Trade Secrets, or any other material covered by the *Hexagon Code of Business Conduct and Ethics* on the Hexagon Policy and Guidelines Downloads site or the Hexagon Data Protection Site.

4.4.4 Hexagon employees shall not engage in any social media that may harm or tarnish the image, reputation and/or goodwill of the company and/or any of its employees. Employees are bound by the *Hexagon Code of Business Conduct and Ethics* on the Hexagon Policy and Guidelines Downloads site

4.4.5 Employees assume all risk and responsibilities associated with their social media activities and internet usage. Employees are not allowed to imply or express that their personal beliefs or opinions are those of any Hexagon employee or the company.

4.4.6 Employees must obey all laws and regulations regarding the use of copyrighted, trademark, logo, and any other intellectual property to be used in connection with any social media activities.

4.5 Inappropriate and Unacceptable Use

The activities listed below are prohibited. The list below is not exhaustive, and the absence of an activity does not indicate it is allowed. The list is provided as a reference guideline for unacceptable activities.

The use of Hexagon systems, assets or services in the commission of any activity deemed illegal by municipal, state, federal or international laws is strictly prohibited.

The following system and network activities are **strictly prohibited**, with no exceptions:

4.5.1 Infringement upon any rights associated with trade secrets, patents, copyright, or other intellectual property including pirated software, music or licenses not legally owned by Hexagon.

This includes downloading any software utilities/programs not legally owned, purchased, or licensed by Hexagon.

NOTES:

- Many “free”, “trial”, “open source” software downloads have license agreements where use is designated as free for personal use but must be purchased for commercial use.
- Any non-purchased software downloaded or obtained as free/trial software, open source, etc. should be reviewed by Hexagon’s ALI/SIG legal or contracts departments before use.

4.5.2 The copying or distribution of any copyrighted electronic or non-electronic material for which Hexagon or the end user is not licensed. This includes books, brochures, photographs, and copyrighted music.

4.5.3 The export of any software, security technology, or technical information not in accordance with export control laws. The appropriate management should be consulted prior to export of any material that is in question.

4.5.4 The intentional introduction of malicious software or programs into the Hexagon environment. This includes, but is not limited to, any software used to deliver viruses, malware or establish end user surveillance.

4.5.5 Providing system / network access credentials to any non-Hexagon employee, and sharing of credentials with family, friends, and other employees.

4.5.6 Utilizing any Hexagon technology assets to harass, threaten or create a hostile workplace for any person.

4.5.7 Using any Hexagon system or service to defraud any person.

4.5.8 Performing any unauthorized data sniffing or packet capture on the internal Hexagon network.

4.5.9 Attempting to circumvent or thwart any in-place security measure.

4.5.10 Implementing any action, program, software, or script that would deny service (DoS or DDoS) to an authorized employee or to authorized external clients.

4.5.11 Participating in any denial of service attack (interrupting an authorized user's access to a system with malicious intent).

4.5.12 Providing information about or lists of Hexagon employees, customers, or partners to parties outside of Hexagon without consent. Refer to the Hexagon Data Protection Site.

4.5.13 Using any part of a system or Hexagon network for unauthorized commercial purposes including collecting, earning, storing, marketing, mining, or production of any form of electronic currency, cryptocurrency, digital assets or internet currency (e.g., Bitcoins), or providing processing work for personal financial gain.

4.5.14 Theft of Hexagon data, assets, systems, intellectual property, personal data, or any form of electronic or tangible Hexagon property or information.

4.5.15 Distributing or misappropriating Hexagon Confidential, Hexagon Proprietary Information, Intellectual Property, Trade Secrets, or sensitive information without proper authorization.

4.6 Security Incidents/Events/Investigations

4.6.1 Employees must report any suspected or observed security incidents/events to IT and the incident/event shall be recorded in the IT Service Ticketing System. Refer to IT Mandatory Security Incident and Outage Reporting Policy and Lost or Stolen Device Reporting Policy.

4.6.2 Employees are required to cooperate fully with any investigation related to security incidents/events.

4.7 Policy Compliance

4.7.1 Compliance Measurement – Global IT will verify compliance to this policy through various methods, including, but not limited to:

- Business tool reports
- Internal and external audits
- Feedback to IT

4.7.2 Exceptions - refer to the IT Exceptions Policy.

4.7.3 Non-Compliance - An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Exceptions

Exceptions to this policy must be approved by IT and recorded in the IT Service Ticketing System as referenced in the IT Exceptions Policy.

6. Review

Refer to the IT Document Review Policy.

7. Artifacts

Artifacts related to non-compliance will be maintained in a secured repository.

8. IT Standards Controls

NIST 800-171 R1: 3.1.22, 3.8.1

ISO 27001: A.6.2.1, A.6.2.2, A.9.1, A.9.1.1, A.9.1 2, A.9.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3, A.9.4.1, A.9.4.2, A.9.4.4, A.9.4.5, A.11.2.6, A.11.2.8, A.11.2.9, A.13.1.1, A.13.1.3, A.13.2,1, A.14.1.2, A.14.1.3, A.18.1.3

Cyber Essentials: N/A

9. Revision History

Rev.	Rev. Date	Reason for Revision	Revised By
1.0	01-Jul-2017	Initial Document	Tony Zana (Legal) Jennifer Kaplan (PPM HR) Joseph Seays (IT)
2.0	04-Oct-2018	Revision of the previous Acceptable Use Policy 1.0 dated 01-Jul-2017	Karen Paulukaitis
2.0	04-Oct-2018	Reviewed and approved.	Dena Vogelpohl
2.1	02-Jan-2019	• Added section 3.1.8 unauthorized activities that compromise systems, 3.1.9 disable anti-virus • 3.2.1 Added link to Mobile Device Management policy • Added sections 3.2.5 Added Clear Desk, 3.2.6 Printing of Non-Public information, 3.2.7 Added Anti-Virus requirement • In section 3.3, added link to Employee Handbook with reference to Section 5.4 Company Communication Systems • 3.3.1 – removed “Whenever an EMPLOYEE states or indicates an affiliation with the Hexagon organization or its brand, that EMPLOYEE is required to clearly state and indicate that "the opinions expressed are my own and not necessarily those of the company" and addressed in 3.4.2. • 3.3.2 – moved from section 3.2 • 3.3.2 Moved to 3.3.3 • 3.3.4 was previously 3.3.8 • 3.3.5 was added for GDPR • Added 3.3.6 forwarding emails guideline • 3.3.7 included customer • 3.3.8 replaced tweets with social media • Added sections 3.3.12 sending email from another Employee’s account, 3.3.13 email sent to a customer • In section 3.4, Added links to Hexagon Data Protection site, Hexagon Code of Business Conduct and Ethics, and Hexagon Policies and Guidelines. • 3.4.1 replaced blogging with social media • 3.4.2 added from Hexagon Social Media Policy, replaced “you” with “EMPLOYEE” and “group” with “Hexagon” • 3.4.4 added link to Hexagon Data Protection site • 3.4.5 replaced specific forms of social media with “social media” and replaced specific examples of undesirable conduct with being bound to Hexagon Code of Ethics (link) • 3.4.6 replaced blogging and social media with “social media” • 3.5 removed “In general” from the start of the 2nd paragraph • 3.5.13, 3.5.14 added	Karen Paulukaitis
2.1	09-Jan-2019	Reviewed and approved.	Dena Vogelpohl
2.1	24-Jan-2019	Reviewed and approved pending clarification on 3.3.13.	John Ferguson
2.1	05-Feb-2019	Approved	John Ferguson
2.2	15-Feb-2019	• Removed "Hexagon owned SYSTEMS are to be used strictly for purposes of the organization, clients, partners and daily operations of the Hexagon business. • Definition of Employee: Add US to employee specification and removed "including all personnel affiliated with third parties interacting with Hexagon SYSTEMS" • 3.1.2 – added "intellectual property" and provided a link to Legal Services - Intellectual Property	Karen Paulukaitis

Rev.	Rev. Date	Reason for Revision	Revised By
		• 3.1.3 - Changed from Hexagon EMPLOYEES are required to report any loss, theft, or unauthorized disclosure immediately to their manager and Global IT to "Hexagon EMPLOYEES are required to report any loss, theft, or unauthorized disclosure immediately to their manager and Global IT and. shall be logged as a security incident in the IT Service Ticketing System." • 3.1.6 – changed “monitor equipment, network traffic” to “monitor equipment and/or network traffic” • 3.2.2 – added reference to INGRNET Password Policy. • 3.2.3 Changed should to shall and added "For exceptions, refer to the IT Exception Policy" • 3.2.6 – removed content and added reference to Printing and Shredding Best Practice Guide. • 3.3.5 Added "Refer questions related to privacy to your division’s privacy lead and/or privacy officer." • 3.4.6 – removed the word blogging • 3.5.7 – changed “sexually harass” to “harass” • 3.6.2 Changed "Exceptions - Any exception to the policy must be approved in advance by Hexagon Legal, Hexagon HR, AND Global IT." to "Exceptions - Refer to IT Policy Exceptions."	
2.2	21-Feb-2019	Reviewed and approved	John Ferguson
2.3	25-Feb-2019	3.1.9 changed Anti-Virus to anti-virus, laptop encryption, multifactor authentication, etc. 3.2.7, added referenced to Laptop Encryption Policy and Multifactor Authentication Policy	Karen Paulukaitis
2.3	25-Feb-2019	Reviewed and approved	John Ferguson
2.4	18-Mar-2019	• Added “Interns / Students participating as part of an HR approved program” to definition of EMPLOYEE per suggestion from Nico van der Werf. • 3.5.6 – changed “work colleagues” to “other EMPLOYEES” • Removed US from the scope. • Removed 3.5.3 as it contradicts 3.1.5 3.5.3 Utilizing credentials to access any data or SYSTEM for any purpose not directly related to the support or operation of the Hexagon business operations or its customers (under the heading “The following SYSTEM and network activities are strictly prohibited, with no exceptions:”)	Karen Paulukaitis
2.4	25-Mar-2019	Changes reviewed and approved	Dena Vogelpohl
2.4	01-Apr-2019	Changes reviewed and approved	John Ferguson
2.4	10-Apr-2019	Reviewed	Tony Zana (Legal), Jennifer Kaplan (PPM HR), Jay Cobb (SIG HR)
2.5	02-May-2019	• 3.1.2 Added “and will not engage in any activity that could endanger the security of information on the system”. Employees may not copy Hexagon intellectual property or trade secrets onto portable media such as a disk, thumb drive, or hard drive, or onto a personal computing device unless the employee has specifically been given the right to engage in such activity by management and/or the legal department. Any personally identifying information covered under the General Data Protection Regulation (GDPR) and commercially sensitive or confidential information (intellectual property, trade secrets, financial information, etc.) approved to be transmitted or provided	Karen Paulukaitis

Rev.	Rev. Date	Reason for Revision	Revised By
		to a non-Hexagon employee or a 3rd party application must be encrypted unless the employee has specifically been given the right to provide un-encrypted GDPR, sensitive or confidential information by management and/or the legal department. (per Tony Zana) • Change definition of employee from: ▪ Hexagon employees in GSP, PPM and SI ▪ Interns / Students participating as part of an HR approved program ▪ Contractors ▪ Consultants ▪ Temporary employees ▪ Other workers at Hexagon GSP, PPM and SI and its subsidiaries To • All Hexagon employees in GSP, PPM and SI • Interns / Students participating as part of an HR approved program • External Contractors or External Consultants • Any other classification of an employee, external contractor or external consultant that may perform work on behalf of Hexagon GSP, PPM and SI and its subsidiaries (per Jay Cobb) • 3.3 Removed “For US based employees, also refer to *Section 5.4 Company Communication Systems* of the Intergraph Corporation Employee Handbook (https://hr.intergraph.com/emphandbk/acknowledgement.pdf)” (per Tony Zana and Jay Cobb)	
2.6	21-Aug-2019	• 3.1.3 Added a reference to the Lost or Stolen Laptop/Mobile Device Reporting Policy • 3.2.1 Removed US from “US Removal Media & BYOD Policy”	Karen Paulukaitis
2.7	04-Sep-2019	Added Last Reviewed on the title page.	Karen Paulukaitis
2.8	6-Nov-2019	• 3.2.5(a) added “or divisional/group guidance” because not every group uses the IT Data Sensitivity Classification categories. • 3.2.3 replaced “set to 10 minutes or less” with a reference to the Screen Lock Policy	Karen Paulukaitis Approved by John Ferguson
3.0	09-Dec-2019	• Definition of System: Replaced “Personal systems connecting to a Hexagon corporate network must also adhere to this policy and the Removable Media & BYOD Policy.” with “Employee owned computer equipment authorized to connect to a Hexagon network via Removable Media & BYOD Policy.” As second bullet under definition of system. • Moved these sentences under the first sentence in the Introduction (they were previously under definitions). This policy is in place to protect the employee and Hexagon. Unauthorized and inappropriate use of the systems subjects Hexagon to unnecessary risks, including malware, cyber-attacks, viruses, legal sanctions, financial penalties and revenue loss. Hexagon Management reserves the right to suspend access to Hexagon systems at any time. Each employee is responsible for understanding this policy and to govern their actions and behavior accordingly. • Moved definitions under Scope. • 3.1.1 Removed the sentence “This includes any device owned or leased by any person or entity” as it was misinterpreted by non-English employees.	Karen Paulukaitis Approved by John Ferguson, Dena Vogelpohl

Rev.	Rev. Date	Reason for Revision	Revised By
		• 3.1.2 & 3.1.4 removed “and/or the legal department” as employees should address concerns to their management and management shall engage the legal department as needed. • 3.1.3 changed “their manager and IT and shall” to “their manager and IT. The report shall”. • 3.1.5 removed “IT shall be contacted to request authorization.” and added “IT authorization shall be obtained by logging the activity in the IT Service Ticketing System.” • Swapped 3.1.7 and 3.1.8 • 3.1.8 Added justification and benefits for auditing as a replacement for “ensure compliance with this policy”. • 3.2.4 added “If an employee has a concern about the validity of a suspicious email, please contact IT for assistance. Refer to Identifying and Reporting Phishing Emails. • 3.2.5 (g) replaced “Non-paper information assets should be sent to IT for secure destruction or disposal.” With “Non-paper information assets should be securely destroyed or discarded. Refer to the Media Destruction and Sanitation Policy.” • 3.4.2 removed the second sentence “3.4.2 Limited and occasional use of systems to engage in the use of Social Media is acceptable. ~~Any activity from a system is subject to monitoring.”~~ Replaced by “Any activity from a system is subject to monitoring in accordance with Hexagon’s Employee Privacy Policy (also available upon request).” per Tony Zana • 3.5.8 changed “~~Performing any data sniffing or capture to gain unauthorized access to data.~~ Performing any unauthorized data sniffing or packet capture on the internal Hexagon network.” • Added 3.1.10, 3.1.11, 3.5.13	
3.0	07-Jan-2020	Reviewed and approved	Jennifer Kaplan (PPM HR)
3.0	15-Jan-2020	Reviewed and approved	Jay Cobb (SIG HR)
3.0	17-Jan-2020	Reviewed and approved	Tony Zana (Legal), John Ferguson
3.1	28-Jan-2020	Added ISO 27001 controls	Karen Paulukaitis
3.2	27-Feb-2020	Updated link to the INGRNET Password Policy to the latest approved version in section 3.2.2.	Karen Paulukaitis
3.3	04-Apr-2020	Put definitions under section 2 Definitions. Added sections 5 Exceptions & 6 Review	Karen Paulukaitis
3.4	05-Aug-2020	4.1.2 – added link to Information Transfer and Storage of Hexagon Data policy. 4.2.1 – added link to Mobile Device Best Practices	Karen Paulukaitis
3.5	08-Sep-2020	4.3.14 – added “Email and electronic communications are subject to monitoring in accordance with Hexagon’s Employee Privacy Notice. 4.4.2 – updated link to the latest Employee Privacy Notice and changed “Policy” to “Notice” to match the document title and removed “(also available upon request)”	Karen Paulukaitis
3.6	04-Jan-2021	Annual Review Changed all references to “GSP and SI” to “SIG” Definition of Employee – added “and other Hexagon entities requiring access to the INGRNET domain” Added definition of Personal Data added 4.1.2 Paragraph 2 – reformatted and added restriction for non-Hexagon approved cloud based storage/application	Karen Paulukaitis & Mike O’Donnell

Rev.	Rev. Date	Reason for Revision	Revised By
		4.1.2 Paragraph 3 – replaced “personally identifying information” with “personal data” and replaced GDPR with the Hexagon Data Protection Compliance Programme Manual. 4.3.5 – added commercially sensitive information and replaced “personally identifying information” with “personal data” and removed reference to GDPR.	
3.6	07-Jan-2021	Changes reviewed and approved.	John Ferguson & Dena Vogelpohl
4.0	11-Feb-2021	• Definitions: Added intellectual property, Hexagon proprietary information, trade secret and confidential (and bookmark to reference back to the definitions). • 4.1.2 changed from “Employees must ensure that Hexagon proprietary information (information developed by Hexagon/Intergraph) and intellectual property is always protected and secured and will not engage in any activity that could endanger the security of information on the system. Refer to Legal Services – Intellectual Property” -to- “*Employees must ensure that Hexagon proprietary information and intellectual property is always protected and secured and will not engage in any activity that could endanger the security of information on any system.”* • 4.1.2 added note: *If sensitivity/classification of any Hexagon information is unknown, the information must be treated as confidential. Refer to Legal Services – Marking Intellectual Property, IT Data Sensitivity Classification, and/or divisional/group guidance for information regarding data classification.* • 4.2.1 second sentence added “*that connects to a Hexagon network*” • 4.2.8 added: “*Any employee who receives a request from a representative of a governmental agency, law enforcement, regulatory agency, insurance company, customer, etc. for Hexagon information that is confidential, personal data, proprietary, intellectual property or a trade secret must contact their Hexagon Legal Department before taking any action*.” • 4.4.5 added “*and internet usage”* • 4.5.14 added “*Theft of Hexagon data, assets, systems, intellectual property, personal data, or any form of electronic or tangible Hexagon property or information.”* • 4.5.15 added: “*Distributing or misappropriating Hexagon confidential, proprietary, intellectual property, trade secrets, or sensitive information without proper authorization.”* • Added section 4.6 Security Incidents/Events/Investigations • Added 4.6.1: “*Employees must report any suspected or observed security incidents/events to IT and the incident/event shall be recorded in the IT Service Ticketing System. Refer to IT Mandatory Security Incident and Outage Reporting Policy and Lost or Stolen Laptop/Mobile Device Reporting Policy.”* • Added 4.6.2: *“Employees are required to cooperate fully with any investigation related to security incidents/events.”*	Karen Paulukaitis
4.0	15-Feb-2021	Reviewed and approved	Dena Vogelpohl & Mike O’Donnell
4.0	09-Mar-2021	Reviewed and approved	Alex Molina (PAS)
4.0	16-Mar-2021	Reviewed and approved	John Ferguson
4.0	19-Mar-2021	Reviewed and approved	Jennifer Kaplan (PPM HR)
4.0	30-Mar-2021	Reviewed and approved	Jay Cobb (SIG HR)

Rev.	Rev. Date	Reason for Revision	Revised By
4.1	31-Mar-2021	Reviewed and approved with updates to: - the definition of Intellectual Property, Hexagon Proprietary Information, Trade Secret and Confidential - 4.1.2 first 2 paragraphs changed to “Employees must ensure that Hexagon Proprietary Information and Intellectual Property are always protected and secured and will not engage in any activity that could endanger the security of information on any system. NOTE: If sensitivity/classification of any Hexagon information is unknown, the information must be treated as Confidential.”	Richard Morris (Legal)
4.1	01-Apr-2021	Changes approved	John Ferguson, Mike O’Donnell, Dena Vogelpohl
4.1	06-Apr-2021	Reviewed and approved	Erica Luo
4.1	07-Apr-2021	Reviewed and approved	Andreas Peibst, Uday Sakunala
4.2	22-Jul-2021	Updated employee definition, change “INGRNET domain” to “Hexagon PPM and SIG networks, systems and/or applications” – new standard employee definition.	Karen Paulukaitis
4.3	10-Aug-2021	Change Lost or Stolen Laptop/Mobile Device Reporting Policy to updated Lost or Stolen Device Reporting Policy (with updated link)	Karen Paulukaitis
5.0	22-Nov-2021	Applied new template Added to 4.5.1: “This includes downloading any software utilities/programs not legally owned, purchased, or licensed by Hexagon. **NOTES:** • Many “free”, “trial”, “open source” software downloads have license agreements where use is designated as free for personal use but must be purchased for commercial use. • Any non-purchased software downloaded or obtained as free/trial software, open source, etc. should be reviewed by Hexagon’s PPM/SIG legal or contracts departments before use.” 4.1.5 Added “Personal use of a Hexagon-owned system by an individual who is not a Hexagon employee (this includes family members, friends, etc.) is prohibited.” 4.1.8 Changed “network” to “Hexagon’s networks”	Karen Paulukaitis
5.0	22-Nov-2021	Changes reviewed and approved	Mike O’Donnell
5.0	23-Nov-2021	Changes reviewed and approved	John Ferguson, Andreas Peibst, Dena Vogelpohl, Erica Luo, Uday Sakunala
5.0	29-Nov-2021	Reviewed and approved	Jennifer Kaplan, Richard Morris
5.0	30-Nov-2021	Reviewed and approved	Jay Cobb
5.1	24-Jun-2022	Applied new template and branding changes for PPM to ALI. **Subtitle** changed from “Hexagon’s PPM and Safety, Infrastructure & Geospatial IT Policy” to “Hexagon’s Asset Lifecycle Intelligence (ALI) and Safety, Infrastructure & Geospatial (SIG) IT Policy” **Title** for John Ferguson changed from “John Ferguson Executive Director Global IT Hexagon PPM & SIG” to “ John T. Ferguson Executive Director, IT Global IT Services of the ALI and SIG divisions Hexagon” **Section 1. Introduction** - changed “Hexagon PPM & SIG Information Technologies (IT)” to “Hexagon’s Asset Lifecycle Intelligence (ALI) and Safety, Infrastructure & Geospatial (SIG) Information Technologies (IT)	Elizabeth Henson

Rev.	Rev. Date	Reason for Revision	Revised By
		Section 3. Definitions – replaced the acronym "PPM" with "ALI" in all instances. **Section 4**.5.1 - replaced the acronym "PPM" with "ALI"	
5.2	1-Dec-2022	**Subtitle** changed from "Hexagon's Asset Lifecycle Intelligence (ALI) and Safety, Infrastructure & Geospatial (SIG) IT Policy" to "Hexagon's Asset Lifecycle Intelligence and Safety, Infrastructure & Geospatial, and Hexagon Capability Center India IT Policy" Added Policy Manager to Title Page Updated Policy Manager from Dena Vogelpohl to Elizabeth Henson Updated Footers to add original author and remove Last Printed Date properties. **Introduction**: Replaced "Hexagon's Asset Lifecycle Intelligence(ALI) and Safety, Infrastructure & Geospatial (SIG) Information Technologies (IT)" with "Hexagon's Asset Lifecycle Intelligence (ALI), and Safety, Infrastructure & Geospatial (SIG), and Hexagon Capability Center India (HCCI) Information Technologies(Global IT)" **Employee Definition**: Bullet one - replaced "All Hexagon employees in ALI, SIG, and other Hexagon entities requiring access to Hexagon ALI and SIG networks, systems and/or applications" with "All employees in Hexagon's Asset Lifecycle Intelligence (ALI), Safety, Infrastructure & Geospatial (SIG), and/or Hexagon Capability Center India (HCCI) and other Hexagon entities requiring access to ALI's, SIG's, and/or HCCI's networks, systems, and/or applications." Bullet four - replaced "...on behalf of Hexagon ALI, SIG, and its subsidiaries" with "... on behalf of ALI, SIG, and/or HCCI, and/or its subsidiaries"	Elizabeth Henson
5.2	2-Dec-2022	Reviewed and Approved	Erica Luo, Uday Sakunala, Andreas Peibst, Mike O'Donnell, Dena Vogelpohl
5.2	5-Dec-2022	Reviewed and Approved	John Ferguson
5.2	13-Dec-2022	Reviewed and Approved	Jennifer Kaplan, Richard Morris
5.2	14-Dec-2022	Reviewed and Approved	Jay Cobb, Ballav Mundra, Nousheen Khan