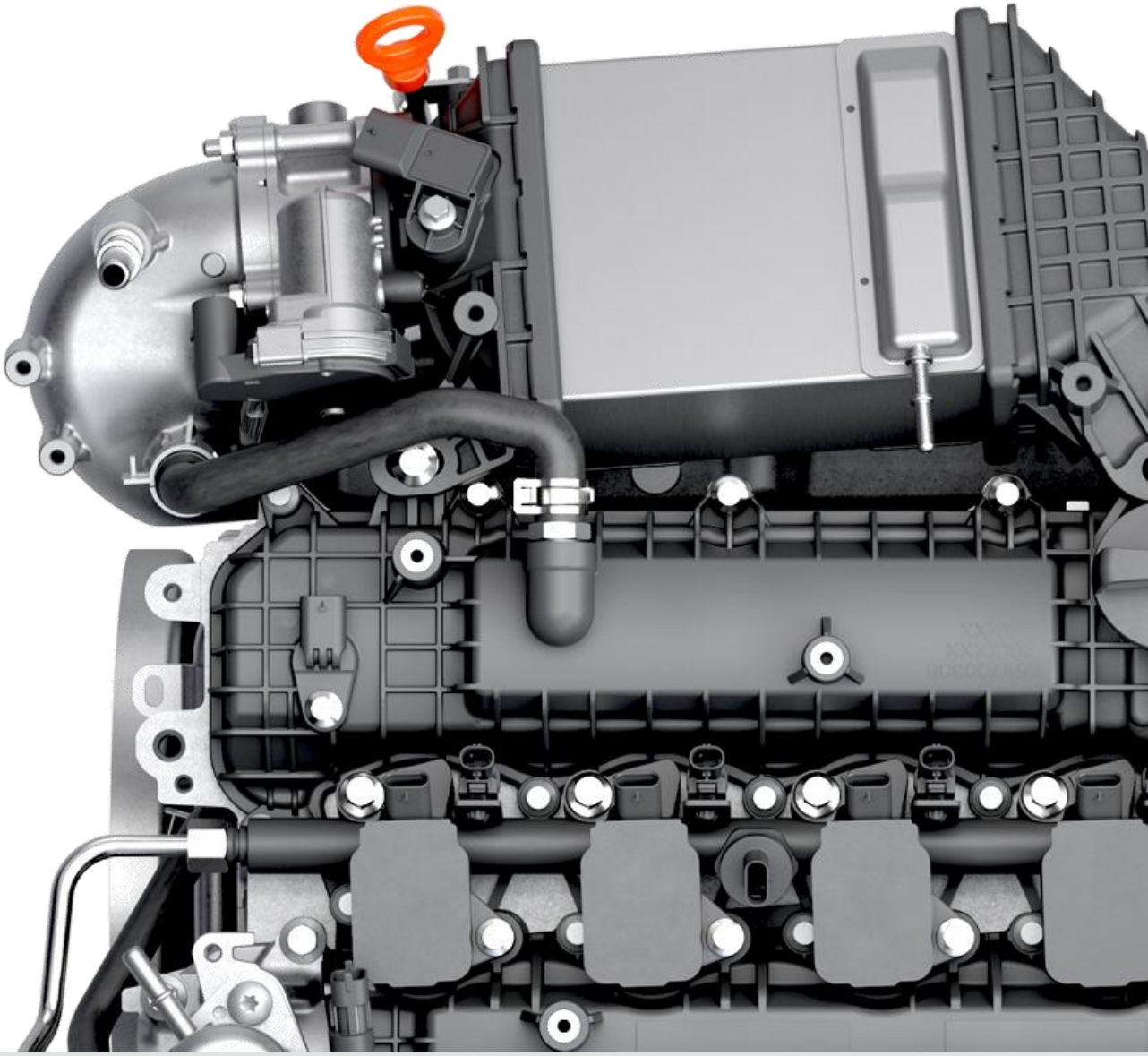
INFORMATION SECURITY POLICY



Registered Office Address
Monomark House
27 Old Gloucester Street
London, England, WC1N 3AX
Registration Nº: 15239961

Visiting Office Address
Paddington Central
4 Kingdom Street
London, England, W2 6BD
United Kingdom

Author: IT
Approved on: 2026-03-30
Security Class: 1

Table of Contents

1 Introduction

This Information Security Policy (Thereafter “the Policy”) was adopted by CEO, Matias Giannini, on 2026-03-30 and applies to all Horse Powertrain[1] Employees[2].

The Horse Powertrain Limited (hereafter: HPL) Information Security Policy establishes guidelines and principles to protect information assets and systems. It aims to ensure confidentiality, integrity, availability and traceability:

- **Confidentiality:** Information originating from customers, suppliers, and partners must not be made available to or disclosed to unauthorized individuals.
- **Integrity:** Information must be correct and reliable. It should be protected against unauthorized changes, distortion, and manipulation.
- **Availability:** Employees, customers, suppliers, and partners must have access to the information they need for their operations, at the right time, and in a user-friendly manner.
- **Traceability:** Activities should be traceable afterwards with a high level of detail. This is necessary for audit purposes.

Subsidiaries should have their own additional policies and procedures to complement the Policy.

All HPL information assets (physical, digital, and unrepresented, such as verbal information) managed by all Employees, and all third parties such as, but not limited to, customers and providers must be protected according to guidelines and principles marked in this policy.

[1] “Horse Powertrain” means HORSE Powertrain, Ltd. and its subsidiaries (i.e. all persons and entities directly or indirectly controlled by HORSE Powertrain, Ltd., where control may be by management authority, equity interest or otherwise).

[2] For purposes of this Policy, the notion of “Employees” includes:

(I) all Horse employees, regardless of function, position or location, whether working full-time or part- time, under a permanent contract or on a temporary basis, as well as

(II) consultants and agency personnel who work at Horse premises or under the direction of Horse (who usually have a Horse identification and/or an Horse email address) – Note that this Policy shall not be construed as an employment contract and does not give consultants or agency personnel any right to continued employment by Horse; and

(III) the members of the Board of Directors of any Horse group company.

2 Commitments and expectations

Directions of the entities of HPL are committed to ensure that the principles and guidelines are followed in their entities. They must ensure that organizational, technical and human resources are available for this purpose.

HPL shall set a Global Information Security Committee. It is relevant to share insights and leverage on frameworks and challenges across the entities. Also, each entity shall have its own information security committee to take all relevant decisions and lead all processes related to information security.

It is the responsibility of all parties to comply with all the information security policies, standards and procedures developed by its own entity. All these developed documents shall always be compliant with global and local applicable legislations, regulations and standards.

The policy will be:

- Communicated and established within the entities of HPL, in their businesses, in their organizational units, and with their product owners.
- Communicated to all relevant employees and third parties annually in line with operational and quality reviews.
- Stored on each entity internal communication platform and made accessible to all relevant employees and third parties within the joint venture.

Reviewed annually by CISOs of each entity of the joint venture and updated upon request from the joint venture's board.

3 Definitions

Term / Acronym	Description
HPL (Horse Powertrain Limited)	The legal entity Horse Powertrain Limited, including all its subsidiaries and controlled entities.
HPL Entities	All subsidiaries, business units, or organizations that are part of Horse Powertrain Limited.
The Policy	Refers to the Horse Powertrain Limited Joint Venture Information Security Policy.
Employee(s)	All permanent or temporary staff, contractors, consultants, agency personnel, and members of the Board working under HPL's direction.
Information Assets	Any data, system, device, infrastructure, process, or verbal information that has value for HPL. Includes physical, digital, and unrepresented information.
Confidentiality	The assurance that information is accessible only to authorized individuals.
Integrity	The accuracy, completeness, and reliability of information and processing methods.
Availability	The property that information and systems are accessible and usable upon demand by authorized users.
Traceability	The capability to reconstruct or trace activities, events, and changes relating to information and systems.
Information Security Management System (ISMS)	A set of policies, procedures, and controls that systematically manage information security risks (based on ISO/IEC 27001:2022).
Cyber Security Management System (CSMS)	A structured framework for managing cybersecurity risks, typically applied to operational technologies (OT) or product cybersecurity domains.
Information Security Committee	A governance body within each HPL entity responsible for decision-making and oversight of security processes.
Global Information Security Committee	A joint governance forum enabling alignment, knowledge-sharing, and cross-entity coordination across all HPL entities.
CISO (Chief Information Security Officer)	The senior executive responsible for overseeing information security strategy and operations within an entity.

Term / Acronym	Description
Third Party	Any external individual or organization accessing HPL assets — including suppliers, contractors, consultants, and partners.
Asset Owner	The individual or role responsible for an information asset's lifecycle, classification, protection, and compliance with security policies.
Authentication	The process of verifying the identity of a user, device, or system.
Multi-Factor Authentication (MFA)	An authentication method requiring two or more independent credentials (e.g., password + mobile token).
Encryption	The process of converting information into a coded form to prevent unauthorized access.
Encryption Keys	Cryptographic keys used to encrypt or decrypt information; considered sensitive assets requiring strict protection.
Identity Lifecycle Management	The process covering the creation, modification, and deletion of user accounts and access rights.
Administrative Privileges	Elevated access rights allowing users to perform critical system-level operations.
Change Management	Formal procedures to ensure controlled and secure modifications to information systems or environments.
Vulnerability Management	Processes to identify, assess, prioritize, remediate, and monitor security vulnerabilities.
Malware	Malicious software designed to harm systems or data (e.g., viruses, ransomware, spyware).
Back-up	A copy of data taken to ensure restoration in case of loss, corruption, or incident.
Network Segmentation	Dividing networks into isolated segments to improve security and minimize the spread of threats.
OT (Operational Technology)	Hardware and software used to monitor or control industrial equipment or processes.
BYOD (Bring Your Own Device)	A policy allowing employees to use their personal devices for work.
Public Cloud	Shared computing resources provided by third-party cloud service providers (CSPs).

Term / Acronym	Description
Incident Response	The set of processes for detecting, reporting, analyzing, and responding to information security incidents.
Information Security Incident	Any event that compromises — or has the potential to compromise — confidentiality, integrity, availability, or traceability of information or systems.
Logging	Recording events and activities in systems to facilitate monitoring, audits, and investigations.
Data Centre	A facility hosting critical IT infrastructure, servers, data storage, and network equipment.
Clean Desk Policy	A policy requiring employees to secure sensitive information and maintain clear, secure workspaces.
Business Continuity	The capability of the organization to continue essential operations during and after a disruption.
Supplier	Any external organization providing products or services to HPL, including outsourced system development or maintenance.
AI (Artificial Intelligence)	Technologies that perform tasks requiring human-like intelligence; subject to specific use and compliance controls.
Non-public Information	Any information not intended for public disclosure, including confidential, strictly confidential, or internal use data.

4 How to Act

4.1 Organizational aspects

- Directions and management levels shall be fully committed with information security.
- All employees and third parties shall know their responsibilities in terms of information security.
- All parties shall know where the information security policies and procedures are available.
- Information security shall be aligned with business objectives and fully integrated with business processes.
- All Business processes shall be designed to comply with information security policies and procedures.
- All information security guidelines shall be regularly updated and modified according to the current information security risks.
- All information security policies and procedures shall be aligned with global and local regulations, laws and businesses' applicable standards.

4.2 Human resources security

- Information security clauses shall be integrated in contracts with employees and contractors.
- Onboarding shall include mandatory information security awareness training.
- Mandatory information security awareness training shall be given to all employees on a regular and scheduled basis.
- Offboarding shall include signing information security and confidentiality clauses.
- Remote work policy shall consider information security aspects.

4.3 Asset Management

- All information assets shall be protected to ensure confidentiality, integrity, availability and traceability.
- The entities of HPL shall implement all necessary technologies to protect assets against cybersecurity threats.
- All information assets property of one entity of HPL shall be inventoried, classified and have a designated owner.
- Asset's owner is responsible for complying with information security policies to protect its asset.
- The correct use of each type of technology such as email, Internet, instant messaging, social media, shall be defined and communicated.
- The correct use of mobile devices such as laptops, mobile phones, USB, removable storage devices, tablets, BYOD devices shall be defined and communicated.
- All asset's lifecycle shall be considered in the information security policies including reuse or disposal of all types of devices to ensure all information is correctly destroyed and avoid data leaks.
- Procedures and requirements for encryption shall be aligned with the asset classifications levels.
- Assets might need to be encrypted according to their classification. Personal Data might need to be encrypted.
- Encryption keys, other secrets related to encryption are critical assets and shall be protected as such.

4.4 Identity and access management

- Access to all systems, portal, applications and other assets containing non-public information shall be limited to authorized users through an authentication process.
- User's identity lifecycle management shall be defined and shall include account creation, account evolution and account deletion.
- Accounts shall be individual and shall not be shared unless it is strictly necessary for operative reasons.
- Access rights shall be assigned based on the role of each employee or other third party. They shall be limited as much as possible.
- Authentication shall be adapted to the classification level of the accessed asset. Multi-factor authentication shall be used for the most critical assets.
- Administrative privileges shall be restricted to the minimum number of accounts.
- Authentication methods, in particular passwords, shall be secure and adapted to assets classification level.
- Passwords shall be stored securely and shall never be stored in plain text. They shall be correctly encrypted.

4.5 Operational Security

- Back-up procedures shall be defined and implemented for the Information assets, and they shall be aligned with assets' classification.
- Information assets or systems changes shall be managed according to defined changes management procedures.
- Information assets and systems shall be protected by relevant technologies such as antivirus against malware threats.
- Vulnerability management procedures shall be defined and implemented to manage existing vulnerabilities: they shall prioritize critical assets and eliminating most dangerous-rated vulnerabilities.
- Software use shall be controlled. Specifically, used software and operating systems shall be correctly licensed and updated according to defined procedures.
- Minimum technical mechanisms shall be defined and implemented to reduce the possibility of critical data leaks.
- Security technologies and processes shall be defined and implemented to protect communications in the networks of HPL and with Internet.
- The clocks of all relevant information processing systems must be synchronized with an accurate time source.
- AI correct use shall be defined in policies and standards according to local applicable regulations. The relevant related security controls shall be defined and implemented.

4.6 Network Security

- Entities communication networks shall be segmented into subnetworks to avoid unwanted disclosures of communications.
- Most critical communications channels shall be protected adequately. This shall include communications' encryption.
- All Internet and Internal network accesses shall be controlled and restricted to authorized users or devices.
- Communications shall be limited and filtered by the adequate technologies. IT and OT-production networks are to be risk-based segmented.

4.7 Physical Security

- Physical security measures shall be defined for each site of HPL. They shall depend on the particularities of each site to be well adapted.
- Facilities shall be protected against unauthorized access to prevent theft, damages, information or process disclosures.
- Facilities shall be protected against environmental damages (fires, water damages…) and power failures.
- Clean desk policies and measures shall be implemented such as locking down non-public information and assets, locking screens while they are not being used.
- All assets and information which need to be disposed shall by destroyed in a safe manner to prevent information theft or disclosure.
- All employees and third parties working on sites shall know their role and responsibilities related to physical security.
- Data centres shall be particularly well protected against environmental threats, power failure and loss of Internet connection as they are critical assets for the business.

4.8 System acquisition, development and maintenance security

- Information security guidelines and policies shall be considered in the processes of acquiring, developing and maintaining the systems.
- Projects of implementation, development or maintenance of security systems shall consider information security requirements and comply with them.
- For acquisition, development or maintenance externalized projects or services, the suppliers shall be advised of the information security requirements they need to comply with.
- Information security requirements shall be included in the contracts with suppliers. Requirements may be defined in line with the information security risks.
- The correct use of public cloud services shall be defined and the related relevant security controls implemented.
- Change management procedures shall be defined and implemented to reduce related information security risks.

4.9 Incident Response

- Procedures to report possible Information Security incidents shall be implemented. They shall be communicated and available to all interested parties.
- Roles and responsibilities and adequate incident escalation shall be defined for the incident response management.
- Information Security monitoring shall be implemented to be able to investigate what occurred in case of information security incident. Most relevant systems or users' events shall be logged to be auditable. They shall be retained according to applicable local regulations.
- Information Security Monitoring shall be implemented according to global and local regulations, laws and standards. This may include notifying public institutions about the detected incidents.
- Incident response procedures shall be aligned with business continuity objectives and shall prioritize what is priority for the business.

5 Consequences of violations of this policy

Failure to comply with this Policy could cause significant harm to Horse Powertrain such as loss of business, substantial fines and reputational damage; and may lead to sanctions for the violating Employee(s), up to termination of employment as well as substantial fines and in some cases criminal prosecution.

6 How to report a violation

If you notice any activity or conduct that may result in a violation of this Policy, you are expected to report the issue promptly to either your direct manager or your local People & Culture representative. If for some reason you are not comfortable with this reporting procedure; you can also contact another manager or the Legal & Compliance department or report via the whistleblowing reporting line[3]. For more information about reporting, please refer to the Internal Reporting Policy.

Horse Powertrain will ensure that there are no adverse work-related consequences for any Employee who, in good faith, alerts management to possible violations of this Policy.

Note that in accordance with the Internal Reporting Policy, Employees are required to report any violation of this Policy and failure to do so may result in disciplinary action, up to and including dismissal, within the limits of applicable laws.

[3] Note that in some countries there can be legal restrictions on what can and cannot be reported through the whistleblowing reporting line. Details of these restrictions are presented when accessing the system. If you wish to report concerns about wrongdoing or malpractice, please refer to our Internal Reporting Policy, which contains full details of how to raise a concern, including the reporting channels and further guidance.

7 Guidance and assistance Commitments and expectations

This Policy is an overriding policy document, which sets the framework for managing and protecting Information.

Guidance and assistance regarding this Policy should be sought, first and foremost, from your manager. For further guidance, you may also refer to the corporate directives and guidelines related to this Policy. Inquiries about this Policy may also be directed to your cybersecurity department at cybersecurity@horse-powertrain.com.

7.1 Support and resources

Resources

HPL, and its entities ensure that sufficient resources (financial, technological, and human) are allocated for implementing, maintaining, and improving the Information Security Management System (ISMS) and, when relevant, for the Cyber Security Management System (CSMS).

Leadership & commitment

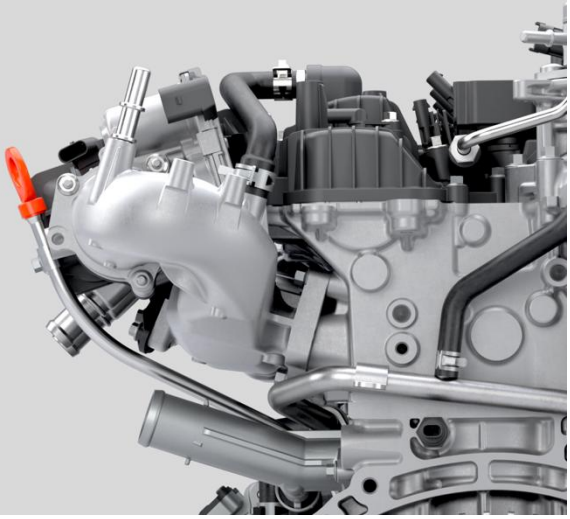
Global Information Security Directions of each entity are accountable for the effectiveness of the ISMS and ensures that information security policies and objectives are established and compatible with strategic plan and business objectives. They provide necessary resources, demonstrate direction and support, and ensure integration of the ISMS requirements into business processes.

Competence & Training

All personnel must possess the necessary competencies and knowledges for their information security responsibilities. A training and awareness program is conducted to ensure employees understand information security policies, standards, procedures, and best practices.

Documentation & Communication

The entities maintain documented information required by ISO/IEC 27001:2022 and any additional internal needs. Relevant documentation (policies, standards, procedures, guidelines and others) is made accessible and communicated to staff and, where appropriate, external parties.



Registered Office Address
Monomark House
27 Old Gloucester Street
London, England, WC1N 3AX
Registration Nº: 15239961

Visiting Office Address
Paddington Central
4 Kingdom Street
London, England, W2 6BD
United Kingdom