INFORMATION SECURITY POLICY

HORSE POWERTRAIN LTD

Table of Contents

1 Introduction 2

2 Commitments and expectations 2

3 Definitions 3

4 How to act 6

5 Consequences of violations of this policy 9

6 How to report a violation 9

7 Guidance and assistance 9

8 Support and resources 9

1 Introduction

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

The 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 Horse Powertrain information assets (physical, digital and unrepresented, such as verbal information) managed by 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.

2 Commitments and expectations

All of Horse Powertrain, including its divisions and entities, is committed to ensure that the principles and guidelines are followed. It must ensure that organizational, technical and human resources are available for this purpose.

Horse Powertrain and each of its entities must have a Global Information Security Committee. It is relevant to share insights and leverage on frameworks and challenges across the entities. 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 must always be compliant with global and local applicable legislations, regulations and standards.

The policy will be:

- Communicated and established within Horse Powertrain, and all parts of its business, organizational units and product owners

---

[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 Powertrain 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 Powertrain premises or under the direction of Horse Powertrain (who usually have a Horse Powertrain identification and/or a Horse Powertrain email address). Note that this policy must not be construed as an employment contract and does not give consultants or agency personnel any right to continued employment by Horse Powertrain; and

III. the members of the Horse Powertrain Board of Directors of any Horse Powertrain entity.

- Communicated to all relevant employees and third parties annually in line with operational and quality reviews
- Stored on each entity's internal communication platform and made accessible to all relevant employees and third parties within the joint venture.

Reviewed annually by Chief Information Security Officer (CISO) of each entity and updated upon request from the joint venture's Board of Directors.

3 Definitions

Term / Acronym	Description
Horse Powertrain Ltd	The legal entity Horse Powertrain Ltd, including all its subsidiaries and controlled entities.
Horse Powertrain Ltd entities	All subsidiaries, business units, or organizations that are part of Horse Powertrain Ltd
The Policy	Refers to the Horse Powertrain Ltd Information Security Policy.
Employee(s)	All permanent or temporary staff, contractors, consultants, agency personnel, and members of the Board working under Horse Powertrain Ltd's direction.
Information assets	Any data, system, device, infrastructure, process or verbal information that has value for Horse Powertrain. 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.

Term / Acronym	Description
Information Security Committee	A governance body within each Horse Powertrain entity responsible for decision-making and oversight of security processes.
Global Information Security Committee	A joint governance forum enabling alignment, knowledge sharing and coordination across all Horse Powertrain entities.
CISO (Chief Information Security Officer)	The senior executive responsible for overseeing information security strategy and operations within an entity.
Third party	Any external individual or organization accessing Horse Powertrain 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 and 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).

Term / Acronym	Description
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.
Operational Technology (OT)	Hardware and software used to monitor or control industrial equipment or processes.
Bring Your Own Device (BYOD)	A policy allowing employees to use their personal devices for work.
Public cloud	Shared computing resources provided by third-party cloud service providers (CSPs).
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 center	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.
Artificial Intelligence (AI)	Technologies that perform tasks requiring human-like intelligence, and are 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 must be fully committed to information security.
- All employees and third parties must know their responsibilities in terms of information security.
- All parties must know where the information security policies and procedures are available.
- Information security must be aligned with business objectives and fully integrated with business processes.
- All business processes must be designed to comply with information security policies and procedures.
- All information security guidelines must be regularly updated and modified according to the current information security risks.
- All information security policies and procedures must be aligned with global and local regulations, laws and applicable standards.

4.2 Human Resources

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

4.3 Asset management

- All information assets must be protected to ensure confidentiality, integrity, availability and traceability.
- The entities of Horse Powertrain must implement all necessary technologies to protect assets against cybersecurity threats.
- All information assets must be inventoried, classified and have a designated owner.
- The asset owner is responsible for complying with information security policy to protect its asset.
- The correct use of each type of technology (email, internet, instant messaging, social media, etc.) must be defined and communicated.
- The correct use of mobile devices (laptops, mobile phones, USB, removable storage devices, tablets, BYOD devices, etc.) must be defined and communicated.
- All assets' lifecycles must be considered in the information security policy 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 must be aligned with the asset's classification levels.
- Assets might need to be encrypted according to their classification. Personal data might need to be encrypted.

- Encryption keys and other secrets related to encryption are critical assets and must be protected as such.

4.4 Identity and access management

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

4.5 Operational security

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

4.6 Network security

- Entities communication networks must be segmented into subnetworks to avoid unwanted disclosures of communications.
- Most critical communications channels must be protected adequately. This must include encryption.
- All internet and internal network accesses must be controlled and restricted to authorized users or devices.

- Communications must 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 must be defined for each Horse Powertrain site. They must depend on the particularities of each site to be well adapted.
- Facilities must be protected against unauthorized access to prevent theft, damages, information or process disclosures.
- Facilities must be protected against environmental damages (fire, water damage, etc.) and power failures.
- Clean desk policies and measures must be implemented such as locking down non-public information and assets, and locking screens while they are not being used.
- All assets and information which need to be disposed of must by destroyed in a safe manner to prevent information theft or disclosure.
- All employees and third parties working on sites must know their role and responsibilities related to physical security.
- Data centers must 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 must be considered in the processes of acquiring, developing and maintaining the systems.
- Projects of implementation, development or maintenance of security systems must consider information security requirements and comply with them.
- For acquisition, development or maintenance externalized projects or services, the suppliers must be advised of the information security requirements they need to comply with.
- Information security requirements must 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 must be defined and the related relevant security controls implemented.
- Change management procedures must be defined and implemented to reduce related information security risks.

4.9 Incident response

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

- Incident response procedures must be aligned with business continuity objectives and must 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 HR representative. If for some reason you are not comfortable with this reporting procedure; you can also contact another manager or Legal & Compliance 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.

See Internal Reporting Policy

7 Guidance and assistance

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 function at cybersecurity@horse-powertrain.com.

8 Support and resources

RESOURCES

Horse Powertrain 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).

[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.

LEADERSHIP AND 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 AND 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 AND 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.

