

SECURITY POLICY

June 2025



HORSE SECURITY POLICY.....	2
1. Presentation of the document	3
1.1. Scope.....	3
1.2. Definition of responsibilities.....	3
2. Document management	4
2.1. Document Governance	4
2.2. Contact Person	4
2.3. Document Update and Review Cycle	4
2.4. Compliance	4
2.5. Exceptions	5
3. Content of the Document	5
3.1. Organizational aspects	5
3.2. Human resources security	7
3.3. Asset management.....	8
3.4. Identity and Access Control	8
3.5. Cryptography	9
3.6. Physical and environmental security	9
3.7. Operational security	10
3.8. Network security	10
3.9. System acquisition, development and maintenance	11
3.10. Supplier relationships.....	12
3.11. Incident response	12
3.12. Business continuity	12
3.13. Regulatory and legal compliance.....	13
3.14. Information security risk management.....	13
4. Glossary	13
5. References	14



HORSE SECURITY POLICY

RULE / PROCEDURE				
Reference:	Version:	Language:	Date of application:	Next revision date:
RPIF-XXXXX-AAAA-9999	1.0	EN	DD/MM/YYYY	DD/MM/YYYY
Status:	Issuing Function:		Issuing Department:	
Applicable	Cybersecurity		IS/IT	
Document subject:	The HORSE Security Policy establishes guidelines and processes to protect information assets and systems, ensuring the security, confidentiality, availability, and integrity of customer-sensitive information. Non-compliance could result in business risks, misuse of systems, and breaches of legal obligations. Every HORSE employee: headquarters, Spain, Portugal, Brazil, Argentina, Chile, Turkey, Romania			
Associated Process:	ISMS: Information Security Management			
Recipients:	2- Horse Internal			

	NAME	FUNCTION	DATE OF SIGNATURE
Author:	Javier Asenjo, Ezequiel Wolf, Francisco Calzado	Global Security Team	24/04/2025
Validated by:	María Luisa Redondo	CISO – Chief Security Officer	29/04/2025
Approved by:	Patrice Haettel	CEO	-
Approved by:	Edouard Simon	CIO	-
Approved by:	María Luisa Redondo	CISO	-

OTHER FEATURES (OPTIONAL)

To remember:	
Collection or documentary class related:	
Parent document:	Click Here
Previous reference:	Click Here
Other documents referred:	Click Here
Regulatory requirement:	ISO21434, ISO 27001, NIS2, TSAX Click Here

VERSION HISTORY

Version	Application	Purpose of main modifications	Author
1	DD/MM/YYYY	New Policy	Global Cybersecurity Team
	DD/MM/YYYY		



1. Presentation of the document

The protection of our information assets is vital to the success of our business. The HORSE SECURITY POLICY (from here: the Policy) establishes that guidelines and process for ensuring the protection of information and information systems used to support HORSE's overarching mission of ensuring the security, confidentiality, availability, and integrity of customer sensitive information. A failure to do so would represent a business risk and could adversely impact the reputation of HORSE and the value of our constituent business.

A failure to comply with this policy could expose HORSE to misuse of information systems, breaches of confidentiality, corruption of data, theft, or loss of intellectual property and customer information, and breaches of our legislative, regulatory, and contractual obligations.

This document establishes the foundation of the HORSE Cyber Corporate Regulatory Framework, outlining the mandatory guidelines and principles that govern cybersecurity practices within the organization.

- **External content:** HORSE Technologies Division, a multinational company headquartered in Madrid, employs over 9,000 professionals dedicated to advancing the automotive industry. Our organizational structure is optimized to support innovation and operational efficiency across diverse geographical locations, with manufacturing facilities in Turkey, Romania, Latin America, Brazil, Portugal, and Spain. Specializing in the design and production of transmissions and engines, we pride ourselves on driving excellence and sustainability in every factor of our operations. The company culture fosters an environment of collaboration and continuous improvement, empowering our skilled workforce to pioneer innovative solutions. We maintain strong internal relationships and stakeholder engagement to align with our strategic goals and fulfil our mission to lead in powertrain technology.
- **Internal content:** HORSE Technologies Division operates with a robust organizational framework designed to foster innovation and efficiency. The company champions a culture rooted in excellence and sustainability, aiming to reduce environmental impact while enhancing product performance. Our team is composed of highly skilled professionals dedicated to continuous improvement and innovation, ensuring that we remain at the forefront of technology and industry standards. Strong internal collaborations and stakeholder engagement are key to our success, allowing us to align closely with organizational goals and shareholder expectations.

1.1. Scope

This Policy applies to all functional departments of HORSE operating in all geographical locations. It governs all electronic and physical information that is created or received in the conduct of HORSE business. All employees, contractors, and third parties with access to HORSE information and HORSE IT Systems are expected to comply with this policy, regardless of their location and worker status.

1.2. Definition of responsibilities

The Global Security is responsible for defining the security requirements for the Cyber Corporate Security Framework of the group, and then the plant department managers are responsible for implementing and maintaining each document at each entity level. In addition, each country may develop each own version of the documents inheriting the global requirements.



2. Document management

2.1. Document Governance

ROLE	DEFINITION OF ROLE	ASSIGNED TO
Responsible/Document Owner	Person(s) responsible for developing and verifying compliance of the policy.	CISO
Accountable	Person(s) who have actions to be performed include as part of the policy.	CISO, Global Security Team
Consulted	Person(s) or groups to be consulted prior to final policy implementation or amendment.	Compliance, CISO, IS/IT ILT.
Informed	Person(s) or groups to be informed after policy implementation or amendment.	Global Security Team, all employees, contractors and relevant third parties.

To ensure the continued effectiveness and relevance of this policy, HORSE shall establish periodic internal reviews and audits that assess compliance, identify areas for improvement, and incorporate lessons learned from security incidents or changes in the business, regulatory, or technological environment. These reviews must align with the organization's commitment to continuous improvement and be guided by the objectives and risk appetite defined by senior management.

2.2. Contact Person

Questions and feedback regarding this document should be submitted to the above listed Document Owner or his designated delegate.

2.3. Document Update and Review Cycle

HORSE reserves the right to amend this policy at any time and will publish updated versions to all employees and relevant third parties. For further information on information Security, please contact HORSE CISO and Security Team. The Document Owner will review (and update, where required) this document every year or whenever changes in business environment demand such a review.

2.4. Compliance

HORSE Senior Management is in charge of promoting and supporting the establishment of technical, organizational, and control measures to ensure the authenticity, integrity, availability, confidentiality, and auditability of information.

The Global Security Team is in charge of managing this Policy and handling any questions that arise regarding its application, in addition to reviewing it at least yearly, either to update its content or as part of a scheduled review. The Department must always verify its effectiveness.

Compliance of this Policy is mandatory, and its violations shall be reported to HORSE Global Security Team and CISO. Any failure to comply with this Policy may result in disciplinary actions, in line with the internal



processes of HORSE with the employment laws. All members of the company must notify the Information Security team of any event that may result in a breach of any of the clauses defined in this regulation. In cases where it is determined that a breach or violation of HORSE Policies, Standards or Procedures has occurred, management will initiate corrective measures including restricting access to services or initiating disciplinary action up to and including dismissal, or in the case of contractors or third parties the termination of a contract or agreement.

2.5. Exceptions

Any exceptions to this Policy must be duly justified, documented by the requestor and reported to the Global Security Team to the corresponding authorization of the Document Owner. and subsequent approval by the relevant Information Owners or Functional department Heads.

These exceptions must follow the internal process defined of the document HORSE Security Standards Change Management Process. All the changes tracked must be included on the document HORSE Security Exception Inventory.

3. Content of the Document

3.1. Organizational aspects

- 3.1.1. HORSE must appoint a Chief Information Security Officer (CISO) to achieve the defined cybersecurity objectives. To achieve these objectives and follow the defined strategy, a roadmap must be established
- 3.1.2. HORSE's strategy for information security has established and effective, forward-looking Information Security Management Program clearly aligned with the commercial direction and supported by a strong professional capability across the organization.
- 3.1.3. HORSE must be able to demonstrate that customers, business partners, and employees can have full confidence in the confidentiality, integrity, and availability of our information and IT systems.
- 3.1.4. The Board of Directors actively supports information security within HORSE by promoting actions aimed at integrating information security as part of the HORSE's strategy and processes. As a manifestation of this commitment:
 - 3.1.4.1. Is informed of the Policy and is responsible for providing the necessary leadership, the necessary management structure, and the resources for its implementation within the Group.
 - 3.1.4.2. Ensures the implementation of the requirements defined in this Policy in all business processes.
 - 3.1.4.3. Participates in the review of information security policies and activities.
 - 3.1.4.4. Is informed of the implementation of the Policy in the different areas and departments, including legal and regulatory compliance.
 - 3.1.4.5. Is committed to facilitating and promoting compliance with the HORSE Cyber corporate Regulatory Framework in the field of information security and personal data protection.
 - 3.1.4.6. Ensures the provision of the necessary economic and human resources for Information Security activities.
 - 3.1.4.7. Undertakes to consider the risk of information security and personal data protection when making decisions.



- 3.1.5. HORSE relies on ISO 27001:2022 (TISAX also based on ISO) and NIST Framework to identify and deploy security controls consistently across all functional departments.
- 3.1.6. The above are considered to ensure that:
 - 3.1.6.1. HORSE brand is protected.
 - 3.1.6.2. Access to HORSE Information and HORSE IT Systems are only available to authorized persons with a justifiable business need.
 - 3.1.6.3. The confidentiality of HORSE information is assured against unauthorized disclosure.
 - 3.1.6.4. The confidentiality, integrity, and availability of HORSE customer'/clients' information.
 - 3.1.6.5. The integrity of HORSE information is maintained against unauthorized modification.
 - 3.1.6.6. HORSE information is available when required by the relevant business processes.
 - 3.1.6.7. All applicable regulatory, legislative and customer requirements are met.
 - 3.1.6.8. Information security education, awareness and training is available to all employees.
 - 3.1.6.9. All breaches of security and suspected weaknesses are reported, investigated, and documented.
 - 3.1.6.10. Additional standards and guidelines accessible to all employees, exist to support this Policy.
 - 3.1.6.11. Each information asset group will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.
 - 3.1.6.12. It is the responsibility of all individuals who have been granted access to data to handle it appropriately in accordance with its classification.
 - 3.1.6.13. Data will be protected against unauthorised access.
 - 3.1.6.14. Compliance with the Policy will be enforced.
- 3.1.7. Cybersecurity functions and responsibilities of HORSE employees must be defined and assigned, to ensure the correct organization and development of the company's strategy. This guarantees an appropriate segregation of duties and avoids any potential conflicts of interest.
- 3.1.8. Information Security is structured so that strategy, policy, and expert information security resources will be provided from a central function.
- 3.1.9. Cybersecurity committees must be defined to assess strategic and operational issues.
- 3.1.10. Functional department Heads are accountable for information security in their business areas and will delegate the responsibility for representing information security to a role within their department. This role will be supported with information security expertise from HORSE Global Security Team.
- 3.1.11. HORSE will define and implement roles for the management of information security. This includes identification and allocation of security responsibilities to initiate and control the implementation of information security across HORSE.
- 3.1.12. The hierarchy of responsibility is:
 - 3.1.12.1. The IT Risk Register records the risks identified with Information Technology and Information Systems. These Risk Registers are owned by the Senior Management team (business areas) since the acceptance of risks contained therein is their responsibility, given that some of the risks will affect business areas.
 - 3.1.12.2. Senior Management Team (business areas) are responsible for managing risks.
 - 3.1.12.3. The Security & Operational Steering Committee has representatives from all relevant areas of HORSE and its purpose is to influence, oversee, promote, and improve information security by identifying and assessing security requirements and risks.



- 3.1.12.4. IS/IT, GRC and Legal Services, manage information security, providing advice and guidance on the implementation of this Policy or its inherited documents.
- 3.1.12.5. Information owners for IT systems, such as Business Service Owners are responsible for compliance with this Policy.
- 3.1.12.6. IT System Owners are responsible for ensuring that appropriate security arrangements are in place for IT administrative access and security controls on managed systems are compliant.
- 3.1.12.7. Users assume local accountability for compliance with this Policy. They are responsible for reporting any actual or suspected information security issues to IS/IT Security team and Help Desk.
- 3.1.13. The IS/IT Security Team may authorise legally compliant monitoring of IT systems to investigate security incidents and compliance with HORSE' policies.
- 3.1.14. HORSE shall approve, communicate about, and make available the Policy and its derived documents to all employees and ensure it is understandable.
- 3.1.15. HORSE must inform its employees about the security measures they should carry out on a daily basis and how they should use corporate devices and tools.
- 3.1.16. HORSE Security Team will regularly assess for compliance against the HORSE Cyber corporate Regulatory Framework.
- 3.1.17. or compliance with product cybersecurity requirements, HORSE will adhere to the policies, standards, and procedures outlined in its Cybersecurity Management System (CSMS). This system is designed to meet ISO/SAE 21434 and other relevant standards, regulations, or requirements. The CSMS will align with this policy and integrate with other management systems, such as the Quality Management System (QMS).

3.2. Human resources security

- 3.2.1. Security responsibilities should be included in job role descriptions, person specifications and personal development plans. Individuals accessing HORSE' data must seek advice from IS/IT Security Team they are not clear about their information security responsibilities.
- 3.2.2. Security responsibilities must be taken into account by HR in the selection process, the creation of contracts, and during the working day, with the aim of reducing the risk of manipulation, theft, fraud, or inappropriate use of information.
- 3.2.3. Upon termination of a staff appointment, HR department will revise the staff record system, accordingly, triggering IT systems account termination processes.
- 3.2.4. Employee contracts enforce compliance with HORSE' policies, standards, and procedures.
- 3.2.5. Line managers must ensure that appropriate staff exit procedures are in place to remove access to all systems upon staff exit or change of role. Line managers must ensure that all IT assets owned by HORSE must be returned upon termination of contract.
- 3.2.6. All HORSE personnel must receive an adequate level of information security training and awareness and also be correctly informed of their roles and responsibilities related to information security. This training and awareness must be adequate to their responsibilities.
- 3.2.7. HORSE must define security requirements for remote working.



3.3. Asset management

- 3.3.1. HORSE must establish a set of measures for the organisation of information assets, ensuring their integrity, and protecting against leaks, accidental deletions, or unauthorised accesses.
- 3.3.2. All assets (data, software, processing equipment and IT services) will be identified, inventoried and owners documented.
- 3.3.3. The owners are responsible for the maintenance and protection of those assets in accordance with HORSE's policies.
- 3.3.4. All information created, received, or retained must be protected according to the HORSE's data classification. The more confidential information is considered to be, the more restrictive the controls should be.
- 3.3.5. All HORSE information assets and data will follow HORSE's retention schedules. Data must be stored on facilities provided by HORSE or trusted third parties.
- 3.3.6. HORSE must define the correct use of critical technology (email, Internet, social media, etc.). Email is a communications mechanism and must not be used as a replacement for file storage.
- 3.3.7. HORSE must establish guidelines for the use and management of mobile devices (mobile phones, tablets, etc.) that are provided by the company and make use of its information systems. Removable mass storage devices should be treated in the same way as Confidential data and must be locked away at the end of the working day.
- 3.3.8. HORSE users must be prohibited from storing information belonging to HORSE on non-corporate systems, and the use of personal devices should be restricted unless approved by the Global Security Team. Confidential and Strictly Confidential data must not be copied onto devices.
- 3.3.9. Dispose of physical records containing at least confidential level data securely by using provided confidential waste shredding services or shredders.
- 3.3.10. The methods of disposal of logical storage equipment must be in accordance with the information they store (following the criteria of information classification).
- 3.3.11. HORSE tracks assets assigned to employees, ensuring all company assets are returned and wiped of data when contracts end.

3.4. Identity and Access Control

- 3.4.1. All the company's information systems must have an access control system to identify, authenticate and authorize the user, thus preventing unauthorized access to the information systems.
- 3.4.2. A procedure for user account creation and deletion must be maintained for access to all IT systems.
- 3.4.3. Access will be granted according to an individual's role and the data classification based on the principle of least privilege.
- 3.4.4. Mandatory authentication must be used.
- 3.4.5. Multi factor authentication must be used for accessing Confidential/Strictly Confidential data.
- 3.4.6. Users with administrative rights must use their normal user accounts for standard IT system access and only use elevated privileges when required.
- 3.4.7. Users must not share their login details to access IT services.
- 3.4.8. Passwords must be in accordance with the HORSE's Password definition.



3.5. Cryptography

- 3.5.1. HORSE must apply cryptographic controls according to the need for these controls, based on the security level required for the information handled.
- 3.5.2. The cryptographic methods should be aligned with the company's data classification scheme.
- 3.5.3. HORSE will provide guidance and tools to ensure proper and effective use of encryption to protect the confidentiality and integrity of data and IT systems.
- 3.5.4. Where a staff member manages their own encryption, it is critical that encryption keys are securely backed up, as forgetting an encryption key will mean the encrypted data is lost for ever.
- 3.5.5. Data encryption is required for Confidential/Strictly Confidential data transmitted over data networks. Confidential/Strictly Confidential data must be encrypted if stored away from HORSE environment.
- 3.5.6. HORSE must implement encryption controls on removable media, such as hard drives, laptops, mobile phones, servers, and databases.
- 3.5.7. The encryption keys will be securely managed and that they can only be accessed via a strict authorisation process.
- 3.5.8. The encryption methods used in the company must be recognized as non-vulnerable by good security practices.
- 3.5.9. When protecting confidential data, such as Personally Identifiable Information (PII), HORSE must consider techniques like data masking, pseudonymization, or anonymization to conceal sensitive information.

3.6. Physical and environmental security

- 3.6.1. HORSE must define physical security measures depending on the different facilities of the company.
- 3.6.2. Data centres, computer rooms, and communications facilities used for hosting equipment for information processing must be physically protected from unauthorized access to prevent theft or damage.
- 3.6.3. Facilities must also be adequately protected against environmental damage and power failures, such as: Uninterruptible Power Systems, generators, fire detection and extinguishing systems, etc.
- 3.6.4. HORSE must establish security measures to protect physical assets both within and external to the working environment.
- 3.6.5. Employees must maintain a clean desk and screen policy to protect sensitive information, locking computers when not in use and promptly managing printed documents. Non-compliance may result in disciplinary action.
- 3.6.6. Computer equipment must be password protected if left unattended.
- 3.6.7. A screen lock must be activated when there is no activity for a short period of time.
- 3.6.8. Passwords must not be written down anywhere near IT equipment.
- 3.6.9. Portable computing devices must be locked away at the end of the working day.
- 3.6.10. All HORSE equipment or provided by RG, must be disposed of in a controlled manner.
- 3.6.11. Final user is responsible for the safe keeping of its device when it is removed from the office and it should be secured when not in use in order to avoid theft or loss. Devices should not be left in cars or other vulnerable locations.
- 3.6.12. Unattended devices must be secured to prevent theft or misuse.



3.6.13. HORSE ensures the physical security of deployed elements outside the office, protecting them against theft and tampering with 24/7 surveillance and formal agreements with external sites. Security measures align with assessed risks.

3.7.Operational security

- 3.7.1. HORSE will document all procedures related to information processing, system use, and security management.
- 3.7.2. Operational changes to equipment, infrastructure, or software affecting HORSE' Production IT services and suppliers must follow change management procedures.
- 3.7.3. HORSE must define the different type of environments needed depending on the business specifications.
- 3.7.4. HORSE must protect their information systems and systems connected to HORSE network from malware threats by implementing robust, scalable, and standardized protection mechanisms that ensure detection, prevention, and response capabilities.
- 3.7.5. Backup guidelines and system recovery measures are defined, in place and teste periodically.
- 3.7.6. Logs should be monitored and analyse to detect and response to security events that could affect HORSE's infrastructure.
- 3.7.7. Any device connected to the HORSE network must comply with the HORSE's patching definition. Devices which are not compliant will be liable to physical or logical disconnection from the network without notice.
- 3.7.8. All devices connected to the network, irrespective of ownership, are subject to monitoring and security testing.
- 3.7.9. Procedures must be implemented that control the installation of software on operating systems belonging to HORSE.
- 3.7.10. HORSE will identify, assess and address vulnerabilities in its information systems. If critical and high vulnerabilities are detected that cannot be mitigated, the system will be disconnected from the network.
- 3.7.11. The organization must implement measures to minimize the risk of data leakage, ensuring sensitive information is identified, monitored, and protected against unauthorized disclosure.
- 3.7.12. To prevent external threats that may compromise service and business objectives and to provide a rapid response to a potential incident, the company must analyse threats in order to generate intelligence and knowledge to address potential threats that may affect the company's assets.
- 3.7.13. The organization must establish, document, and communicate a specific policy regarding the use of cloud services to all relevant stakeholders.
- 3.7.14. Business critical systems and other systems identified as high risk will be regularly penetration tested.

3.8.Network security

- 3.8.1. HORSE maintains network security controls to ensure the protection of data within its network and the internet.
- 3.8.2. A correct segmentation must be carried out in order to protect the network from threats and maintain the security of the systems and applications that use the network.

- 3.8.3. Segregation must exist between wired and wireless traffic; different environments defined, guest network , and management services according to data classification.
- 3.8.4. Appropriate controls will be enforced between security zones to reduce the risks of compromise, denial of service attacks, malware infection and unauthorised access to data.
- 3.8.5. Guidance should be sought from the IT Security team and CISO for information on secure data transfer.
- 3.8.6. It is not permitted to connect personally owned equipment to any network socket; personally owned devices should use the wireless network.
- 3.8.7. HORSE sets policies to secure information exchange, protecting against unauthorized access and risks. Measures include controlled use of tools, authentication, and staff training on secure practices.
- 3.8.8. HORSE requires contracts with third parties to define secure exchange protocols, roles, and responsibilities for data transfer, including encryption and compliance with data protection laws.
- 3.8.9. Email and messaging tools must be used for professional purposes only. Security and monitoring policies ensure confidentiality and restrict personal account usage.
- 3.8.10. NDAs enforce protection of sensitive information during and after employment. Misuse leads to disciplinary and legal action, with regular reviews to align with current laws and policies.

3.9. System acquisition, development and maintenance

- 3.9.1. Information security requirements must be defined during the development of business requirements for new IT systems and reviewed following significant changes to existing IT systems.
- 3.9.2. IT Security team will provide advice on the security requirements for new IT services and significant changes to existing IT services.
- 3.9.3. All new projects that will implement systems that process personal data must seek advice from the Legal and IT Security Team during the development of business requirements.
- 3.9.4. When acquiring external services, components and/or products with digital elements, the Product Owner shall ensure that suppliers and/or vendors offer, at all times, a level of cybersecurity equivalent to the criticality of the assets.
- 3.9.5. When the system has been already deployed, maintenance must be performed such as including testing, change monitoring, and inventorying.
- 3.9.6. Ensure security in information systems by integrating security needs from the start, using threat modelling, risk assessment, and testing to protect data and comply with business values and regulatory requirements.
- 3.9.7. Protect information on public networks with authentication, authorization, and cryptographic techniques to ensure confidentiality, integrity, and non-repudiation, preventing unauthorized access and fraud.
- 3.9.8. Implement secure development practices, environments, and version control to manage vulnerabilities and protect information throughout the application lifecycle, including when outsourced.
- 3.9.9. Different types of environments (sandbox, testing, pre-production, etc.) will be used depending on the criticality of the business solution or project.
- 3.9.10. Control and log application changes, conduct security reviews post-implementation, and require re testing to ensure no disruption in critical operations.
- 3.9.11. Ensure third-party development adheres to licensing, security standards, and provides documentation and compliance evidence through established contracts and policies.



- 3.9.12. Use structured testing to verify security and quality of new systems, updates, and outsourced developments, ensuring no vulnerabilities are introduced.
- 3.9.13. Protect operational data in testing by avoiding real data, applying access controls, and securely deleting data post-test, with audit logs for accountability.

3.10. Supplier relationships

- 3.10.1. Suppliers must follow HORSE' security policies, change control process, and support arrangements.
- 3.10.2. HORSE must carefully study the selection process, contractual requirements, service level monitoring, and security measures implemented in the facilities of the external providers of these services.
- 3.10.3. Supplier activity may be monitored according to the data classification, IT service and perceived risks to HORSE.
- 3.10.4. As part of the supplier selection and onboarding process, a risk assessment will be conducted to evaluate the supplier's cybersecurity posture and determine their suitability to handle HORSE information or services, both prior to engagement and periodically during the contractual relationship.

3.11. Incident response

- 3.11.1. HORSE will provide the appropriate people, process, and technology resources to identify, respond to, and manage all confirmed and suspected information security incidents affecting HORSE information and HORSE IT Systems.
- 3.11.2. These incidents respond processes will operate in conjunction with the business continuity plan and will be appropriate to the level of criticality of the incident.
- 3.11.3. Information security incidents will be investigated and logged in accordance with the Security incident procedures to determine whether any underlying security concern need to be recorded, corrected, and built into future controls. If appropriate, concerns will be added to the risk register.
- 3.11.4. In case of suspicious activity all employees and external collaborators of HORSE are obliged to notify it to the HOSE Global Security Team.
- 3.11.5. When required by applicable regulations, significant security incidents affecting critical services, personal data, or company operations shall be notified to competent national authorities and/or sectoral CERTs in accordance with GDPR, NIS2, and other legal obligations.

3.12. Business continuity

- 3.12.1. HORSE will protect critical IT services that support business essential services from the impact of major incidents to ensure recovery in line with documented priorities. This includes appropriate backup and resilience.
- 3.12.2. Business continuity plans must be maintained and tested.
- 3.12.3. Business impact analysis should be undertaken of the consequences of major security incidents.
- 3.12.4. Continuously monitor for potential disruptions and review response actions to enhance our business resilience and incorporate lessons learned.



3.13. Regulatory and legal compliance

- 3.13.1. HORSE will establish a program of reviews and audits to ensure that HORSE information and HORSE IT Systems are managed in accordance with this policy and other relevant regulatory, legislative, and contractual requirements.
- 3.13.2. HORSE commits to support the relevant assessments, reviews and audits undertaken by customers, regulators, and external auditors for the purposes of information assurance.
- 3.13.3. HORSE must comply with all relevant legal, regulatory, and contractual requirements.

3.14. Information security risk management

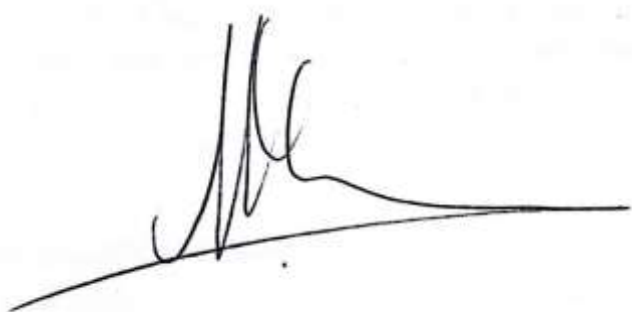
- 3.14.1. HORSE Security team, Information owners, Information Custodians and Technology Service providers are responsible to identify, assess and manage all information security risks to HORSE information and HORSE IT Systems. Risk must be management following HORSE's definition.
- 3.14.2. HORSE follows a risk-based approach to Information Security. To determine the appropriate level of security control applied to IT systems, a risk assessment will identify the likelihood and impact of a security incident and define security requirements. The assessment of risks must be aligned with the risk appetite established by senior management, ensuring that residual risks remain within acceptable thresholds defined by the organization. The GRC Team within the Global Security Team will provide guidance for performing Information Security Risk Assessments. The Legal Department may advise on compliance with applicable Data Protection laws.

4. Glossary

ACRONYMS	DEFINITION
Cyber Corporate Regulatory Framework	A structured set of guidelines and actions designed to manage and enhance information security across the organization. It includes policies, standards, procedures, and best practices that ensure the confidentiality, integrity, and availability of company information and assets.
Policy	A high-level strategic document that outlines the organization's principles and direction regarding information security. It provides the framework for compliance with legal and regulatory requirements and guides decision-making processes within HORSE.
Standard	A detailed, rule-based document that operationalizes policies by specifying criteria and requirements that must be adhered to ensure consistency and effectiveness in security measures. They define the concrete steps for achieving policy objectives.
Procedure	A comprehensive, step-by-step set of instructions that outlines how to execute specific tasks or processes. Procedures are essential for ensuring that operations are carried out consistently and in compliance with policies and standards.
Senior Management	The group of top-level executives responsible for decision-making and overseeing the strategic direction of the organization's information security initiatives.
CIO (Chief Information Officer)	The senior executive responsible for managing and strategizing the use of technology and information systems to ensure alignment with overall organizational goals.
CSO (Chief Security Officer)	The executive responsible for the daily operations of cybersecurity, focused on executing cybersecurity policies and managing threats.
Global Security Team	The team responsible for coordinating and executing all security measures and initiatives as outlined in the Security Plan. They ensure compliance with standards and continuous improvement of the ISMS.
ISMS (Information Security Management System)	A systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability through a comprehensive set of policies, controls, and procedures.

5. References

- ISO/IEC 27001:2022 "Information technology - Security techniques - Information security management systems - Requirements".
- ISO/IEC 27002:2022 "Information technology - Security techniques - Code of practice for information security controls".

A handwritten signature in black ink, appearing to read "Patrice Haettel", written over a horizontal line.

Patrice Haettel

CEO

HORSE TECHNOLOGIES DIVISION

