Group Cyber Security Framework

Information Security Statement

Table of Contents

Leveraging Information Security for Business Growth

At the core of our Information Security Strategy are five key principles designed to create and protect business value:

1. **Strategic Business Alignment**
   - Security needs are based on overall enterprise business goals.
   - Security practices are tailored to fit business processes.
   - Security investments align with enterprise strategy and agreed-upon risk levels.
   - Security is integrated into systems and processes from the beginning ("security by design").

2. **Value Delivery**
   - Standard security practices are established, following industry best practices.
   - Efforts are focused on areas with the highest risk and business impact.
   - Controls and processes are standardized, repeatable, and scalable.
   - Comprehensive security capabilities address people, processes, and technology elements.
   - A culture of continuous improvement is promoted.

3. **Risk Management**
   - A shared understanding of the company's risk tolerance.
   - Clear insight into current risk exposure.
   - Awareness of key risk management priorities.

4. **Performance Measurement**
   - Defined security metrics are in place.
   - Progress is tracked through a structured measurement process.
   - Independent reviews provide objective assurance.

5. **Compliance Maintenance**
   - Privacy is embedded into systems and processes by design.
   - Controls are based on recognized frameworks, standards and regulations (e.g., ISO27001 standard, NIST Cybersecurity framework, NIS 2 regulation, etc.).
   - Adherence to applicable regulations and legislations.

Information Security Policy

The Information Security Policy serves as the cornerstone of our security strategy to build a resilient and secure digital environment aligned with business objectives. It directs the definition of standards, procedures, and guidelines and plays a central role in shaping operational security controls, driving regulatory compliance, and enabling proactive risk management across all Business Units. The policy is aligned with internationally recognized industry best practices and regulatory requirements and contains 14 sections, including among others Information Classification, Access Control, Asset Control, Business Continuity Management etc.

The Information Security Policy affirms its commitment, including but not limited to, the following:

- Establish clear governance structures and policies to align information security efforts with business objectives and regulatory requirements.
- Continuously identify and assess risks to our assets, data, systems and third parties to prioritize security investments and actions.
- Implement safeguards such as access controls, encryption, and employee training to ensure all personnel understand and fulfill their security responsibilities and prevent unauthorized access and data breaches.
- Deploy monitoring tools and processes to promptly detect information security events and anomalies across our environment.

- Maintain and regularly update incident response plans to effectively contain and mitigate the impact of security incidents.
- Develop and test recovery procedures to restore normal operations swiftly and incorporate lessons learned to improve resilience.

We are dedicated to the ongoing enhancement and continuous improvement of our information security practices, ensuring the confidentiality, integrity, availability and safety of our information assets and data entrusted to us.

Data Privacy and Personal Data Protection Policies

Protecting the personal data we handle as part of our business operations is a core responsibility we take seriously. We ensure that personal data is processed lawfully, fairly, and transparently, for clearly defined and legitimate purposes. Through our policies, we promote data minimization, maintain accurate and up-to-date records, and implement appropriate retention practices. We have established strong technical and organizational safeguards to preserve the integrity and confidentiality of personal data. Furthermore, our leadership embraces the principle of accountability by actively supporting privacy governance, assigning clear responsibilities, and continuously monitoring compliance to foster a culture of trust and responsibility. Our policies comply with the applicable legislative and regulatory requirements regarding the processing of personal data.

Information Security Management Roles and Responsibilities

Information security roles and responsibilities are formally established and distributed across IT and business functions to ensure effective risk management. Segregation of duties is enforced to prevent potential conflicts of interest and to safeguard against unauthorized or accidental access and data misuse. The Chief Information Security Officer (CISO) is responsible for leading and sustaining our overarching information security program and possesses a strong understanding of information security, technology, and relevant cyber security standards and regulations. The CISO ensures effective communication of cyber security matters, priorities and risks to the Audit and Risk Committee and Board of Directors, fostering a security-conscious culture at the highest levels of the organization and providing to the Board access to internal and external expertise in this area, as required.

The Executive Leadership Team is responsible for setting the tone at the top by demonstrating visible commitment to information security. They provide strategic direction and ensure adequate resources are allocated to implement and maintain the security program. Leadership endorses and enforces information security policies, promotes a culture of security awareness throughout the Group, and ensures compliance with relevant laws and regulations. They regularly review security performance, support risk management efforts, and hold all employees accountable for their security responsibilities to protect our information assets.

The Chief Information Security Officer (CISO) is responsible for leading the development, implementation, and management of our information security strategy and program. The CISO oversees risk management activities, ensures compliance with security policies and regulatory requirements, and coordinates incident response efforts. Acting as the key security advisor to executive leadership, the CISO fosters a security-aware culture, manages security awareness training, and continuously monitors the threat landscape to adapt defences and protect our information assets.

All personnel are responsible for adhering to information security policies and procedures to protect corporate data and systems. They must complete required security awareness training, promptly report any security incidents or suspicious activities, and follow established guidelines for handling sensitive information. Employees are expected to practice good cybersecurity hygiene, such as using strong passwords and safeguarding access credentials, to help maintain the confidentiality, integrity, and availability of our information assets.

Risk Management

Effective risk management is key to safeguarding our business and ensuring long-term value for stakeholders. We integrate risk practices across all operations to maintain resilience and compliance. As part of the Company's continuous improvement and annual planning processes, security projects and activities are aligned with defined security objectives and approved by senior management. This alignment is based on current security risks, business requirements, and changes in legal and regulatory framework requirements. The risk management program ensures clear ownership of each risk, mitigation action plans and regular reporting to management.

Human Resources Security

We are committed to maintain a secure and compliant working environment by enforcing comprehensive Information Security practices throughout the entire employee lifecycle. Employment and contractor agreements clearly define individual information security responsibilities for the entire workforce. All personnel are required to comply with the Information Security policies and procedures. A robust escalation process is in place for employees to report incidents, vulnerabilities, or suspicious activities. Depending on the type of incident, the relevant IT and business stakeholders lead the response efforts, focusing on efficient resolution and minimizing any adverse effects on business continuity. This process ensures timely identification, investigation, and resolution of security concerns, with clear guidelines for reporting and corrective actions. The process is communicated to all personnel and consistently followed to maintain a secure environment.

Information Security Training and Awareness

Recognizing the importance of the human factor in Information Security, we promote a strong security and privacy culture by providing ongoing, role-specific training and awareness programs to all employees and contractors. All employees and contractors receive tailored awareness training, along with regular updates on policies and procedures relevant to their respective role. Specifically, they participate in phishing campaigns and Information Security trainings, followed by assessment to evaluate their understanding. Data privacy training is conducted bi-annually, and additional ad-hoc training and awareness initiatives are provided to address emerging risks and reinforce privacy and security best practices.

Asset Management

We are committed to safeguard our information assets through well-defined controls, clear ownership, and established rules for their appropriate use. Information assets are clearly identified, inventoried, assigned on respective stakeholders and controlled for their use. Rules for the acceptable use of information assets and information processing facilities are in place.

Information Classification

To ensure appropriate protection and handling, we classify information based on legal requirements, business value, criticality and sensitivity to unauthorized disclosure or modification. The Information Classification Policy defines how information assets shall be handled in accordance with their classification level.

Media Handling

Procedures for the management of removable media have been implemented in accordance with the adopted classification scheme. Media are disposed of securely and safely when no longer required, whereas media containing information are protected against unauthorized access, misuse or corruption during transportation.

Mobile Devices and Teleworking

We enforce comprehensive security measures to safeguard information accessed and processed on mobile devices and remote work locations. We have implemented supporting security measures to manage the risks introduced from the use of mobile devices.

Access Control

We ensure access to information assets is granted strictly based on user identification, authentication and authorization, ensuring that each individual is only provided with the appropriate level of access based on the need to know and least privilege principles, in alignment with their business role. A formal user access registration, de-registration and re-certification process is in place, ensuring that access rights are consistently managed and aligned with business needs. The allocation and use of privileged access rights is strictly controlled, with regular reviews conducted to ensure compliance.

Authentication

Robust and standardized practices for managing authentication to information assets are in place. Secure log-on procedures are employed, ensuring that access is protected against unauthorized use.

Cryptography

We have in place requirements for the use of encryption, including guidance on standards and the legal and regulatory considerations surrounding encryption. Comprehensive key management procedures have been implemented to ensure proper management throughout the entire lifecycle of encryption keys.

Physical and Environmental Security

To protect our information assets and ensure the safety and integrity of our facilities and equipment, we implement robust physical and environmental security controls. Security perimeters have been defined and implemented to protect areas that contain either sensitive information and information processing facilities. Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Information Technology Operations Management

We implement requirements and controls to ensure adequate integrity and availability of information throughout all data processing operations. Key principles including but not limited to segregation of duties, environment segregation, operational change control, system planning and acceptance, security incidents management, performance management are established.

Protection from Malware

We have in place comprehensive malware controls, complemented by ongoing user awareness programs that promote secure practices and reduce the risk of malware incidents through informed and responsible user behaviour. Controls for the detection, prevention, and recovery from malware are implemented and regularly updated to maintain system resilience and safeguard information assets.

Backup

We maintain regular and tested backup procedures to ensure data availability, support business continuity, and strengthen overall business resilience.

Logging and Monitoring

To ensure accountability, detect incidents promptly, and strengthen cyber defence, we employ comprehensive logging and continuous security monitoring, enhanced with threat intelligence. Information security events are generated, securely stored, and reviewed. Logging facilities and log data are safeguarded against tampering and unauthorized access.

Control of Operational Software

We enforce strict controls over software installation to ensure only authorized and verified applications are deployed, maintaining the integrity and security of operational systems. Formal procedures are in place to control software installation on operational systems. These measures support the integrity, stability, and security of operational environments by preventing unauthorized changes and reducing operational risk.

Vulnerability Response

We actively monitor and collect information about technical vulnerabilities affecting our information systems in a timely manner. Identified risks are evaluated, and appropriate mitigation measures are implemented to reduce exposure.

Patch Management

To protect the security of all network-connected assets and services, we have in place a structured patch management program. Our program sets clear requirements for ensuring that security patches are implemented in a timely manner.

Penetration Testing

We conduct penetration testing as part of the annual assurance schedule to validate system configurations and identify potential vulnerabilities. Externally facing systems undergo regular security reviews, including assessments by independent third parties. Additionally, when changes are made to operating platforms, business-critical applications are reviewed and tested to confirm that security is not adversely affected.

Communications Security

Our networks are actively managed, monitored and controlled to ensure the protection of information. Security mechanisms, service levels, and management requirements for all network services are clearly defined in formal agreements.

Information Systems Acquisition, Development and Maintenance

Information security is integrated as a key requirement throughout the development, implementation, and upgrade of systems. Security-related requirements are incorporated into the specifications for new systems or enhancements to existing systems. Clear guidelines for software and system development are applied consistently. Changes within the development lifecycle are managed through formal change control procedures.

Secure development environments are in place and protected for all system development and integration efforts, covering the entire development lifecycle.

Supplier Relationships

Information security requirements are established, monitored, and enforced throughout the supplier lifecycle. Supplier agreements are in place and include provisions to address information security risks. Prior to the supplier relationship initiation, suppliers agree to comply with our security policies (i.e. Information Security Policy, Acceptable Use Policy, Network Access Agreement etc.). We actively monitor, review, and audit supplier service delivery to ensure ongoing compliance with security standards.

Information Security Incident Management

We maintain a structured incident management framework that enables timely detection, assessment, and response to information security events. We have in place clear management responsibilities and procedures to ensure a prompt, effective, and orderly response to information security incidents. Information security events are reported through designated management channels as quickly as possible. Insights gained from analysing and resolving incidents are used to improve security measures and reduce the likelihood or impact of future events. We have not experienced any significant information security incident in the last five years.

Business Continuity Management & Disaster Recovery

To safeguard operations and ensure organizational resilience, we have established robust Business Continuity and Disaster Recovery frameworks designed to minimize disruption and support rapid recovery. The Business Continuity Management (BCM) policy outlines the requirements to maintain uninterrupted business operations. Business Continuity Plans (BCP) encompass a series of strategies and actions aimed at minimizing the impact of disruptions and facilitating a swift return to normal operations and service delivery. The Disaster Recovery Plan (DRP) specifies the necessary actions to restore operations following a catastrophic event. The Disaster Recovery Plan (DRP) is tested annually to ensure its effectiveness and to validate our ability to recover critical operations following a disruptive event.

Audits (Internal & External)

We have in place a rigorous framework of internal and external reviews, certifications, and audits. Our approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) is reviewed independently at planned intervals or when significant changes occur. Our primary IT service centres have achieved ISO 27001 certification, demonstrating their commitment to a robust Information Security Management System (ISMS). This certification covers the design, implementation, support, and maintenance of information systems and infrastructure, ensuring alignment with industry standards and quality assurance. In addition, we have in place a control framework that provides comprehensive guidelines and best practices for IT controls governance. As part of this framework, audits are conducted by external auditors to evaluate the effectiveness of controls, processes, and IT General Controls (ITGCs) as part of the annual financial audit. The Internal Control department also assesses the design and operational effectiveness of these controls. Furthermore, the Internal Audit department conducts audits across various areas each year, as outlined in its comprehensive annual audit plan.