We fortify our digital ecosystem

Cyber Security & Resilience

Information / Cyber Security

Policy

Information / Cyber Security Management Program - Information / Cyber Security & Assurance

August 2025

v1.0

Contents

Introduction

As a modern, forward-looking business, TITAN Group recognizes at senior levels the need to ensure that its business operates smoothly and without interruption to benefit its customers, shareholders, and other stakeholders. Information is a critical asset to the TITAN Group's operations and the ability to achieve its strategic business objectives. As a result, protecting this information's confidentiality, integrity, and availability is imperative to the business. Equivalently, priority is given to ensuring the protection of industrial assets, compliance with health and safety (H&S) requirements and standards, and minimizing environmental emissions, while enhancing reliability and productivity, which take precedence when it comes to Operational Technology (OT) environments where downtime or cyber incidents may have serious consequences for the organization.

This document defines the information / cyber security policy of TITAN Group, and the goal is to provide the main principles required to protect information assets from a wide range of threats and effectively eliminate or, if not possible under the circumstances, lower the business risk. Cornerstone of this effort is the formal assignment of a Group Chief Information Security Officer (CISO) who will be responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

In order to provide a level of continuous operation, TITAN Group has implemented an Information / Cyber Security Management System (ICSMS) in line with the International Standard for Information Security, ISO/IEC 27001:2022, as well as with the ISA/IEC 62443 series of standards that address security for operational technology in automation and control systems. These standards define the requirements for an ICSMS based on internationally recognized best practices.

The operation of the Information / Cyber Security Management System (ICSMS) has many benefits for the business, including:

- Protection of company and customer data
- Protection of revenue streams and company profitability
- Ensuring the supply of goods and services to customers
- Maintenance and enhancement of shareholder value
- Compliance with legal and regulatory requirements

TITAN Group has decided to maintain full alignment with ISO/IEC 27001:2022 in order that the effective adoption of information security best practices may be validated in the future by an independent third party. In addition, the guidance contained in the codes of practice ISO/IEC 27017:2015 and ISO/IEC 27018:2019 has been adopted as these have particular relevance for the provision of cloud services.

This Information / Cyber Security Policy applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to TITAN Group systems, and must be communicated to all in-scope personnel at least annually, after review and approval and after any significant change to the policy occurs. Most importantly, this policy must be consistently adhered to when establishing, implementing, maintaining, and continually improving the Information / Cyber Security Framework.

Information / Cyber Security Policy

Information / Cyber Security Requirements

A clear definition of the requirements for information / cyber security within TITAN Group will be agreed upon and maintained within the internal business, i.e., between the Group Corporate Center (GCC) and all the Business Units across Group's regions/entities, so that all Information / Cyber Security Management System (ICSMS) activity is focused on the fulfilment of those requirements. Statutory, regulatory, and contractual requirements will also be documented and input into the planning process. Specific requirements about the security of new or changed systems or services will be captured as part of the design stage of each project.

It is a fundamental principle of the TITAN Group's Information / Cyber Security Management System (ICSMS) that business needs drive the controls implemented in strict conformity to the relevant regulatory framework, and this will be regularly communicated to all staff in the most efficient way (e.g., through team meetings and briefing documents).

Framework for Setting Objectives

A regular cycle will be used for the setting of objectives for information / cyber security to coincide with the budget planning cycle. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the regulatory and business requirements, informed by the management review process, during which the views of relevant interested parties may be obtained.

Information / cyber security objectives will be documented for an agreed time period, together with details of how they will be achieved. These will be evaluated and monitored as part of management reviews to ensure that they remain valid.

High-Level Information / Cyber Security Objectives

The goal of the TITAN Group Information / Cyber Security Framework is to manage risk within the organization and achieve its information / cyber security objectives through the establishment of supporting policies, processes, and operations. The information / cyber security objectives of TITAN Group – at a high level – are to:

1. Enable the TITAN Group business strategy through the protection of both information and operational assets, ensuring the security and resilience of IT and OT environments;
2. Ensure that information and operational systems are managed securely to protect critical infrastructure, preserve privacy, prevent disruptions, and maintain process integrity;
3. Comply with applicable local laws, regulations, and contractual obligations, including industry-specific cybersecurity and operational H&S standards;
4. Establish an information / cyber security governance structure - supported by harmonized and common standards across the Group and the different Business Units - that effectively manages both Information and Operational Technology Security Frameworks, ensuring collaboration between IT, OT, and business leadership;
5. Identify information and operational assets and classify them based on their role in the TITAN's technology landscape, so as to understand which assets are crucial for safety, performance, and operation, their vulnerabilities, and the threats (both current and emerging) that may exploit these weaknesses, impacting business operations, H&S, and reliability;
6. Manage identified risks to an acceptable level through the design, implementation, and maintenance of risk treatment plans that account for both cyber threats and physical safety risks in IT and OT environments;
7. Enhance brand recognition by applying industry-leading security practices in both IT and OT, prioritizing protection of industrial assets, H&S, environmental impact, reliability, and compliance with sector-specific regulations;
8. Continuously improve the Information / Cyber Security Frameworks, supporting policies, processes, tools, and documentation to adapt to evolving cyber threats, operational risks, and emerging technologies.

Additionally, and in accordance with ISO/IEC 27001:2022 and ISA/IEC 62443, the organization will adopt and implement security controls appropriate to its IT and OT environments. The reference controls detailed in Annex A of ISO/IEC 27001 and the security levels and foundational requirements outlined in ISA/IEC 62443 will be applied where relevant. These controls will be regularly reviewed based on risk assessment outcomes and cybersecurity risk treatment plans.

In addition, enhanced and additional controls from the following codes of practice will be adopted and implemented where appropriate:

- ISO/IEC 27002:2022 – Code of practice for information security controls
- ISO/IEC 27017:2015 – Code of practice for information security controls for cloud services
- ISO/IEC 27018:2019 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27701:2019 – Requirement and guidelines to be used in extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management

The adoption of these codes of practice will provide additional assurance to individuals (staff, suppliers, customers, and other stakeholders) and help further our compliance with the General Data Protection Regulation (GDPR) and other applicable data protection legislation.

Leadership and Commitment

TITAN Group must provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the Information / Cyber Security Framework by:

1. Establishing the Information / Cyber Security Policy and objectives, compatible with the strategic direction of TITAN Group;
2. Confirming that the requirements of the Information / Cyber Security Framework are integrated within TITAN Group processes;
3. Establishing roles and responsibilities for information / cyber security;
4. Communicating to the organization the importance of meeting the Information / Cyber Security Framework objectives and requirements and complying with the applicable laws and regulations;
5. Providing sufficient resources to establish, implement, operate, monitor, review, maintain, and improve the Information / Cyber Security Framework;
6. Directing and supporting TITAN Group personnel to contribute to the effectiveness of the Information / Cyber Security Framework;
7. Supporting other relevant management roles within TITAN Group to demonstrate information / cyber security management's leadership as applicable to their area of responsibility;
8. Determining the criteria for accepting risk and acceptable levels of risk;
9. Implementing and maintaining a continuous information / cyber security awareness training program to ensure that personnel understand their responsibilities, stay informed of evolving threats, and adopt best practices for safeguarding information assets;
10. Confirming that internal Information / Cyber Security Framework audits are conducted;
11. Conducting management reviews of the Information / Cyber Security Framework; and
12. Confirming that corrective actions are taken based on the outcome of internal audits, management reviews, security incidents, external audits, etc., and thus promoting continual improvement and confirming that the Information / Cyber Security Framework achieves its intended outcomes.

Information / Cyber Security in Project Management

Information / Cyber security should be integrated into TITAN Group project management methodology to ensure that information / cyber security risks are properly identified and addressed as part of every project. This applies generally to any project regardless of its characteristics and requires the following:

1. Information / Cyber security objectives to be included – and documented – in project objectives;
2. An information / cyber security risk assessment is formally conducted – and documented – at an early stage of the project to identify information / cyber security risks related to projects, any implemented and additional necessary controls, as well as to ensure continuous monitoring throughout a project's lifecycle; and
3. Information / Cyber security is part of all phases of the applied project methodology.

Continual Improvement of the Information / Cyber Security Management System (ICSMS)

TITAN Group's policy regarding continual improvement is to:

- Continually improve the effectiveness of the Information / Cyber Security Management System (ICSMS);
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001:2022, ISA/IEC 62443, and other related standards;
- Achieve ISO/IEC 27001:2022 full alignment and maintain it on an ongoing basis;
- Increase the level of proactivity (and the stakeholder perception of proactivity) with regards to information / cyber security and the ongoing management of ICSMS;
- Make information / cyber security processes and controls more measurable in order to provide a sound basis for informed decisions;
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data;
- Obtain ideas for improvement via regular meetings and other forms of communication with interested parties;
- Review ideas for improvement at regular management meetings, so as to prioritize and assess timescales and benefits.

Ideas for improvements may be obtained from any source, including employees, customers, suppliers, IT/OT staff, risk assessments, and service reports. Once identified, they will be recorded and evaluated as part of management reviews.

Policy Documentation

TITAN Group defines policies in a wide variety of information / cyber security-related areas, which are described in detail in a comprehensive set of policy documentation that accompanies this overarching information / cyber security policy.

Each of these policies is defined and agreed upon by one or more people with competence in the relevant area and, once formally approved, is communicated to an appropriate audience, both within and external to the organization.

Application of Information / Cyber Security Policy

The policy statements made in this document and in the set of supporting policies and procedures mentioned above have been reviewed and approved by the Executive Committee of TITAN Group and must always be complied with. Failure by an employee to comply with these policies may result in disciplinary action being taken in accordance with the organization's respective procedure, and the applicable legislation.

Questions regarding any TITAN Group policy should be addressed in the first instance to the employee's immediate line manager.