



Energy
SPACEWELL

Spacewell Energy (Dexma)
Security Policy – Global Security Policy

Table of contents

1	Introduction	3
2	Objective	4
3	Scope of application	6
4	Review and publication.....	7
5	Responsibilities.....	8
6	Global Security policy details	9
6.1	7.1 General considerations	9
6.2	7.2 Information security in Spacewell Energy (Dexma) projects	9
6.3	7.3 Information security in supplier relations	9
6.4	7.4 Protection of business records	10
6.5	7.5 Information Security Risk Analysis and Management	10
6.6	7.6 Detailed security policies.....	10
7	Enforcement.....	11

1 Introduction

The Global Security Policy provides definitive information on the prescribed measures used to establish and enforce the IT security program at SPACEWELL ENERGY (DEXMA) .

SPACEWELL ENERGY (DEXMA) is committed to protecting its employees, partners, clients and SPACEWELL ENERGY (DEXMA) from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every SPACEWELL ENERGY (DEXMA) user who interacts with data and information systems. Therefore, it is the responsibility of every user to know these policies and to conduct their activities accordingly.

Protecting company information and the systems that collect, process, and maintain this information is of critical importance. Consequently, the security of information systems must include controls and safeguards to offset possible threats, as well as controls to ensure accountability, availability, integrity, and confidentiality of the data:

- CONFIDENTIALITY – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.
- INTEGRITY – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- AVAILABILITY – Availability addresses ensuring timely and reliable access to and use of information.

Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of data and information systems. This also includes against accidental loss or destruction.

2 Objective

The Global Security Policy requires that a comprehensive framework is established in order to meet the following **Information Security Objectives**:

- **Create and maintain an Information Security Management System (ISMS)** in accordance with ISO27001:2013.
 - The degree to which this objective is achieved will be measured by ongoing supervision by company management, the results of internal and external audits, and the progress of planned continuous improvement activities.
- **Protect SPACEWELL ENERGY (DEXMA) 's information assets so that they are only used for authorized business activities** and are always available when required for those activities; in this manner shareholder value is also protected.
 - The degree to which this objective is achieved will be measured by reviewing security incident indicators and evaluating denial of service and ransomware attempts and trends, as well as carrying out access right reviews, reviewing the progress of focused security actions or projects, and improving the maturity of related security controls.
- **Ensure the confidentiality and integrity of SPACEWELL ENERGY (DEXMA) 's business information and knowledge.**
 - The degree to which this objective is achieved will be measured by reviewing security incident indicators and evaluating hacking and phishing attempts and trends and improving the maturity of related security controls.
- **Safeguard the personal safety** of SPACEWELL ENERGY (DEXMA) personnel, clients and visitors, **as well as their personal information**, when they are in the company's offices or working remotely.
 - The degree to which this objective is achieved will be measured by evaluating the improvement in the maturity of related physical environment, remote working and personal data security controls.
- **Ensure compliance with legal requirements and corporate ethical standards.**
 - The degree to which this objective is achieved will be measured by ongoing supervision by company management, reviewing the results of internal and external audits, and by evaluating the improvement in the maturity of related security controls, in particular regarding the Acceptable Use policy being up-to-date and adhered to.

Detailed security policies are developed and implemented, and they must be maintained in order to achieve the above Information Security Objectives. The focus of these security policies is driven by many factors, with the key factor being risk. These detailed security policies set out the ground rules under which SPACEWELL ENERGY (DEXMA) operates and safeguards its data and information systems to both reduce risk and minimize the effect of potential incidents.

These policies, including their related standards, procedures, and guidelines, are necessary to support the management of information risks in daily operations. The development of policies provides due care to

ensure SPACEWELL ENERGY (DEXMA) users understand their day-to-day security responsibilities and the threats that could impact the company.

Implementing consistent security controls across the company will help SPACEWELL ENERGY (DEXMA) comply with current and future legal obligations to ensure long term due diligence in protecting the confidentiality, integrity, and availability of SPACEWELL ENERGY (DEXMA) data. In particular, the controls implemented in this policy and its sub-policies comply with the security requirements demanded by the regulation of security measures of the EU Regulation 2016/679 of April 27 concerning General Data Protection (GDPR), as well as the Spanish Organic Law 3/2018, of December 5, concerning Data Protection and Guaranteed Digital Rights (LOPDGDD) and are based on the ISO27001 and ISO27002 methodology.

3 Scope of application

The Global Security Policy and its associated detailed security policies, standards, and procedures apply to all SPACEWELL ENERGY (DEXMA) data, information systems, activities, and assets owned, leased, controlled, or used by SPACEWELL ENERGY (DEXMA), its employees, agents, contractors, subcontractors or other business partners on behalf of SPACEWELL ENERGY (DEXMA). These policies apply wherever data is stored or processed, including any third-party contracted by SPACEWELL ENERGY (DEXMA) to handle, process, transmit, store, or dispose of SPACEWELL ENERGY (DEXMA) data.

Beyond this Global Security Policy (“*Global Security Policy*”), the detailed security policies include:

- Security Organization
- Asset Management
- Acceptable Use
- Information Classification
- Information Access Control
- Cryptographic controls
- System Operations
- Communications Security
- Incident Response
- Business Continuity

Separately, the Systems department maintains agreements with certain non-Systems areas in SPACEWELL ENERGY (DEXMA), which establish security objectives and actions that these areas will be responsible for, such as:

- Memo - Administration – administration, invoicing controls
- Memo - People – HR, offices, and general security agreement
- Memo - Development & Data Science - System project development & data analysis controls
- Memo - Local IT Systems - Help desk, device management and user support services
- Memo - Customer Success - Client activation
- Memo - Privacy function - Personal data compliance

Finally, in a similar manner to the inter-departmental internal agreements, security control objectives that are managed by externalized IT support are controlled via a contractual annex with the company that provides these services.

Some information security policies are explicitly directed towards persons with a specific job function (e.g., a System Administrator); otherwise, all internal and external personnel supporting SPACEWELL ENERGY (DEXMA) business functions shall comply with each policy. SPACEWELL ENERGY (DEXMA) departments shall use these policies or may create a more restrictive policy, but not one that is less restrictive, less comprehensive, or less compliant than this policy. These policies do not supersede any other applicable law, higher-level company directive or existing labor management agreement in effect as of the effective date of this policy.

SPACEWELL ENERGY (DEXMA) reserves the right to revoke, change, or supplement these policies, procedures, standards, and guidelines at any time without prior notice. Such changes shall be effective immediately upon approval by management, unless otherwise stated.

4 Review and publication

SPACEWELL ENERGY (DEXMA) 's Information Security Lead, in coordination with management through the Information Security Committee, will periodically review the Global Security policy for applicability, revising it if necessary, in order to address organizational changes and problems identified during implementation or security assessments.

This review and updating process will take place at least annually, or whenever changes occur in the business processes, systems, or the threat environment that make such a review advisable.

SPACEWELL ENERGY (DEXMA) Management – through the Information Security Committee – will approve all policy changes before they are published.

The policies will be disseminated to the appropriate parties to ensure all SPACEWELL ENERGY (DEXMA) personnel and external stakeholders understand their applicable requirements.

5 Responsibilities

SPACEWELL ENERGY (DEXMA) has appointed an Information Security Lead, who is assigned with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

The authority and responsibility for managing the information security program which are delegated to the Information Security Lead includes the requirement to perform or delegate the following information security management responsibilities:

- Establish, document, and distribute detailed security policies and procedures;
- Monitor and analyze security alerts, incidents and associated information;
- Distribute and escalate security alerts and incidents to appropriate personnel;
- Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
- Periodically measure compliance to information security policies and procedures, or to technical security measures. Any significant non-compliance should be immediately reported to Management and measures taken to close the gap.

The SPACEWELL ENERGY (DEXMA) Information Security Management System and its corresponding policies and procedures will be continuously updated on the basis of the experience of its implementation and maintenance.

6 Global Security policy details

6.1 7.1 General considerations

In an effort to ensure an acceptable level of Information Security risk, SPACEWELL ENERGY (DEXMA) 's stakeholders and management recognize the need to design, implement and maintain a coherent set of policies, standards, and procedures to manage risks to its data and information systems.

SPACEWELL ENERGY (DEXMA) establishes, publishes, maintains and disseminates the global security policy, which is:

- Approved and supported by executive management; and
- Disseminated to the appropriate parties to ensure all SPACEWELL ENERGY (DEXMA) personnel understand their applicable requirements.

This Global Security Policy and the related detailed security policies form a roadmap for implementing security measures to protect SPACEWELL ENERGY (DEXMA) 's most valuable assets. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

This Global Security Policy requires SPACEWELL ENERGY (DEXMA) to protect the confidentiality, integrity, and availability (CIA) of its data and information systems, regardless of how its data is created, distributed, or stored. Security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and information systems, in accordance with business risk objectives and in order to meet regulatory, contractual and legal obligations.

6.2 7.2 Information security in Spacewell Energy (Dexma) projects

Any company project – from application development to production architectural implementations – must address information security from the start of the project, identifying security objectives and risks associated with the project, and updating the evaluation of risks as the project advances.

6.3 7.3 Information security in supplier relations

SPACEWELL ENERGY (DEXMA) 's business model works within a complex set of supply chain relations. The Administration and Systems areas of the company will study each relationship that impacts information security, in order to establish and maintain contractual, technical and procedural measures that mitigate any risks associated with suppliers' access to the organization's assets. In addition, the Administration and Systems areas will ensure that suppliers comply with their obligations when carrying out their services, and that any changes in contracted services are done in an approved manner that does not present new risk to SPACEWELL ENERGY (DEXMA) 's information assets.

6.4 7.4 Protection of business records

SPACEWELL ENERGY (DEXMA) has taken measures that ensure that its business records - regardless of their physical, magnetic or digital format – are protected from loss, degradation, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.

6.5 7.5 Information Security Risk Analysis and Management

SPACEWELL ENERGY (DEXMA) has implemented an information risk analysis and management approach based on evaluating risk in its business processes, and establishing a risk treatment plan following an annual cycle. The Risk Analysis and Management Methodology document describes this approach in detail. In summary terms it is based on:

- Identification of business processes, and evaluation of their criticality in terms of loss of Confidentiality, Integrity and Availability;
- Identification of Threats * that SPACEWELL ENERGY (DEXMA) 's ISMS is subject to;
- Evaluation of Probability of Threats against processes and their data;
- Calculation of Inherent Risk levels for combinations of Threats and Processes;
- Evaluation of existing Safeguards/Controls protecting information assets/processes;
- Calculation of Residual Risk levels taking into account current safeguards/controls;
- Management approval of Risk Acceptance Criteria (the maximum acceptable level of risk)
- Creation of a Risk Treatment Plan, based on improving of current safeguards/controls, and implementing focused actions on highest level risks, in order to bring them within the Risk Acceptance Criteria within the current risk management cycle.

** based on Spanish Magerit methodology threat library*

6.6 7.6 Detailed security policies

A detailed set of detailed security policies for information security are to be defined, approved by management, published and communicated to employees and relevant external parties. The detailed security policies that result from this Global Security Policy:

- Provide an overview of the requirements for the information security program and a description of the controls in place, or planned, for meeting those requirements;
- Provide sufficient information about controls to enable an implementation that is unambiguously compliant with the intent of the plan;
- Include roles, responsibilities, management commitment, and compliance;
- Are approved by senior management with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations

7 Enforcement

Intentional non-compliance resulting in a breach of any part of this policy will result in disciplinary action at the discretion of SPACEWELL ENERGY (DEXMA) senior management and within the limitations of applicable legislation.

Severe, deliberate or repeated breaches of the policy may be considered grounds for instant dismissal; or in the case of a SPACEWELL ENERGY (DEXMA) vendor, termination of their contracted services.

All employees and vendors are bound by these policies and are responsible for their strict enforcement.

