POLICY Information Security Management System Policy

Document File Name
Full saved document name and reference:
Information Security Management System Policy

Date Approved by Owner/Revisions made
30 July 2025 v3

Subject to change. This policy should be reviewed annually but may be amended or replaced at any time.

Owner
Department:
IT Department
Position:
IT Security Manager

Applies to
Unless otherwise indicated, this policy/procedure applies to all staff, officers, directors, consultants, contractors, part or fixed-term employees, casual and agency staff and volunteers (collectively referred to as "staff" in this document). They do not form part of the terms of your contract.

Jurisdictional Coverage
ALL

Mandatory

Breaches of this policy may result in disciplinary action, up to and including dismissal.

1. PURPOSE

1.1 To determine the basic rules to prevent unauthorized access, damage and intervention to physical environments to protect the confidentiality, integrity and accessibility of information and to ensure its continuity.

2. RESPONSIBILITIES

2.1 IT Security Manager.

3. INFORMATION SECURITY MANAGEMENT SYSTEM POLICY

3.1 Organizational activities and environments involving corporate information, whether owned by the organization itself or by its suppliers, are critical for the business and activities of the organization and must be appropriately protected. All Genel Energy employees are primarily responsible for the security of information and information assets. The concept of security consists of three main components: confidentiality (preventing unauthorized access to information), integrity (ensuring information is complete, accurate, and has not been altered without authorization), and availability (being ready for use when needed). Any security vulnerability in one of these three main components can have a significant impact on Genel Energy 's reputation and the integrity of its business activities.

3.2 The Information Security Policy is designed to ensure the proper protection of information assets belonging to Genel Energy and its customers. The Information Security Policy applies to all Genel Energy employees, third-party users accessing our information assets, and our service providers. Regardless of their duties and positions, all Genel Energy employees and suppliers must adhere to relevant legal regulations, policies, procedures, regulations, and security principles specified in contracts, to mitigate risks and work within accepted practices.

3.3 Each department manager is primarily responsible for taking necessary measures and monitoring compliance with the Information Security Policy and related policies within their respective departments.

3.4 Genel Energy aims to protect the information and information assets of the organization and stakeholders through the Information Security Management System. Genel Energy Management commits to using the necessary resources to establish, implement, operate, and continuously improve the Information Security Management System to achieve this goal.

3.5 Non-compliance with the Information Security Policy and other policies and procedures related to the Information Security Management System by Genel Energy stakeholders, employees, and suppliers may be considered a violation, and punitive measures may be applied according to the Genel Energy Discipline Procedure.

3.6 "Operating the Information Security Management System in accordance with the ISO 27001 standard will support the protection of our reputation and ensure the continuity of our business success. The attention and support of all Genel Energy employees is required for information security.

3.7 Ensuring the continuity of the three fundamental elements of Information Security Management System in all activities conducted:

- Confidentiality: Preventing unauthorized access to sensitive information.
- Integrity: Demonstrating the accuracy and integrity of information.
- Availability: Demonstrating the availability of information to authorized personnel, when necessary.

3.8 IT Security Manager is appointed as Management Representative and has several duties:

- Ensuring the security of all data, not only electronically stored data but also data in written, printed, verbal, and similar forms.
- Providing Information Security Management training to all personnel to raise awareness.
- Developing, maintaining, and testing business continuity plans.

- Conducting periodic assessments of Information Security to identify existing risks. Reviewing and monitoring action plans based on assessment results.
- Preventing any disputes and conflicts of interest arising from contracts.
- Meeting the requirements of the job for accessibility to information and information systems.

4. ENFORCEMENT

Disciplinary procedures shall be applied to all personnel who do not comply with this policy.

Revised On	Version	Description
28.02.2017	02	
30.07.2025	03	Revision history table has been added. & New format has been adapted.