GENNEXT (PVT) LTD

ISO/IEC 27001:2022

Information Security Management System (ISMS)

Information Security Policy

Document Number: Gennext-ISMS-PO-004
Classification: Internal
Owner: Information Security Officer
Review Frequency: Annually or whenever a significant change occurs
Current Version: 1.0
Effective Date: 1st August 2026

Document History:

Revision No.	Date of Review	Description of amendments	Author (s)	Reviewed by	Approved by
1.0	2026/07/27	Initial release	Gennext	ISSC Committee	ISSC Committee

Gennext is committed to delivering innovative, reliable, and secure digital transformation solutions that enable our customers to achieve their business objectives, while protecting the confidentiality, integrity, and availability of the information entrusted to us by our customers, partners, and employees.

We provide cloud and on-premise infrastructure, IT service management, collaboration, cybersecurity, low-code/no-code, Data & AI solutions, and professional IT services. In doing so we handle business-critical information, including customer information, trade secrets, trade agreements, commercial and employee information, and unpublished financial data, in all forms. This information and the systems that process, store, and transmit it are assets of paramount value and shall be protected throughout their life cycle.

In this policy, information security means safeguarding **Confidentiality** (information is not disclosed to unauthorized persons, organizations, or systems), **Integrity** (information is accurate, complete, and protected from unauthorized or unintended modification), and **Availability** (authorized users have timely and uninterrupted access based on business requirements).

To achieve this commitment, we shall:

- Protect information assets from theft, abuse, misuse, unauthorized access, disclosure, modification, loss, or destruction through appropriate security controls in accordance with ISO/IEC 27001:2022.
- Consistently meet applicable legal, statutory, regulatory, and contractual information security requirements while preserving the reputation and image of Gennext.
- Apply a risk-based approach to identify, assess, and treat information security risks in line with defined risk criteria and acceptable risk levels.
- Establish, monitor, and review measurable information security objectives at relevant functions and levels of the organization.
- Manage user access and operational changes securely and efficiently, applying need-to-know and least-privilege principles.
- Identify, record, report, and respond to information security weaknesses and incidents in a timely manner, and learn from them to prevent recurrence.
- Maintain staff security awareness and competence through annual training, including phishing simulations, awareness campaigns, questionnaires, and training sessions.
- Manage information security risks in relationships with vendors, suppliers, and service providers, and ensure continuity and resilience of critical systems and services.
- Take appropriate action in response to violations of this policy and the Acceptable Usage Policy.
- Continually improve the suitability, adequacy, and effectiveness of our Information Security Management System (ISMS).

This policy provides the framework for establishing and reviewing information security objectives. It shall be documented, communicated to all employees and relevant interested parties, understood, implemented, and maintained at all levels, and made available to interested parties as appropriate.

Top Management is committed to providing the resources necessary to establish, implement, maintain, and continually improve the ISMS, and to reviewing this policy at planned intervals and whenever significant changes occur, so that it remains appropriate to the purpose, context, and strategic direction of Gennext.

"Empowering Digital Transformation Through Security, Trust, and Excellence"

Management Approval

This ISMS Policy has been reviewed , approved, and authorized for issue by the Top Management of Gennext. By signing below, Top Management confirms its commitment to the principles set out in this policy and to the establishment, Implementation,maintance, and continual improvement of the Information security management system in accordance with ISO 27001 requirements.

This policy is effective from the date of signing and shall remain in force until reviewed or superseded. It shall be communicated to all employees, made available to relevant interested parties, and reviewed at planned intervals to ensure its continued suitability, adequacy, and effectiveness.

CEO/Director

Gennext (pvt)Ltd

signature: 

Email: shermal@gennext.lk

Title: CEO/Director