Appendix 1 of the Resolution No. 29 of the Board of Directors of
Premium Nexus JSC dated 20 August 2025

INFORMATION SECURITY POLICY

GENERAL PROVISIONS

This Information Security ("**IS**") Policy (the "**Policy**") is the primary document that governs the Information Security Management System ("**ISMS**") of Premium Nexus JSC (the "**Company**"), aligning it with the Company's core strategic objectives.

SCOPE

This Policy applies to the Company's head office, all branch stores, and distribution center operations.

DEFINITIONS AND ABBREVIATIONS

- **"Management"** refers to the Deputy Chief Executive Officer of the Company;
- **"Management Team"** refers to the Company's Division Directors;
- **"Confidentiality"** means ensuring information cannot be accessed without authorization;
- **"Availability"** means authorized access, collection, and use of information;
- **"Integrity"** means protection of information from unauthorized deletion or alteration;
- **"Information Security Procedural Package"** refers to the following:
  - General IS Procedure;
  - Physical Security Procedure;
  - Information Technology Operations Procedure;
  - IS Risk Management Procedure;
  - Access Control Procedure;
  - Incident Management Procedure;
  - Secure Development Procedure;
  - IS Change Management Procedure;
  - Business Continuity Procedure;
  - Documented Information Control Procedure;
  - Internal Audit Procedure of the Integrated Management System;
  - Management Review Procedure.

PRINCIPLES

In implementing the ISMS, the Company shall adhere to the following principles:

- Unified governance;
- Based on science, advanced technology, and innovation;
- Support for national products, services, and human resource capacity;
- Risk-based assessment;
- Public-private partnership;
- Development of international cooperation;
- Non-violation of human rights and freedoms;

- Respect for human rights and legitimate interests;
- Non-discrimination;
- Collection, processing, and use of information only on legal grounds or with the owner's consent;
- Assurance of IS;
- Preservation of accuracy and integrity of information.

LEADERSHIP

The Management Team commits to supporting and ensuring the effectiveness of the ISMS by implementing the following:

- Establishing IS policies and objectives consistent with the Company's strategy of automation and digital transformation to expand business and enhance employee productivity;
- Integrating ISMS with core and supporting processes of the Company;
- Supporting risk-based and process-based thinking;
- Providing necessary resources for implementation, operation, and sustainability of ISMS;
- Supporting leadership in ISMS at all management levels;
- Communicating the importance of ISMS effectiveness and compliance to all employees;
- Continuously promoting ISMS improvement.

POLICY

The Management Team directs IS operations based on the following policy:

- While implementing medium- and long-term business plans, the Company ensures confidentiality, availability, and integrity of physical and electronic information and data of employees, shareholders, investors, suppliers, contractors, and customers.
- The Company identifies, assesses, and manages IS risks through risk management.
- Operations comply with applicable IS laws and regulatory requirements.
- The IS management system will be implemented effectively, continuously monitored, and improved.
- The Company fosters mutual trust-based cooperation with partners, suppliers, and contractors, aligning their operations with IS requirements, and promoting clean, transparent, and fair business practices.
- Employees shall use Company assets and information appropriately for business purposes and contribute to ISMS.

ROLES AND RESPONSIBILITIES

Management

- Define Company context, establish strategy and direction, approve IS Policy, ensure implementation, oversee ISMS objectives, goals, and plans, and provide resources.

Division Heads, Department Heads, and Managers

- Enforce ISMS policy and procedures within their units;
- Integrate IS requirements into relevant instructions;

- Support IS risk identification and assessment processes;
- Align unit objectives with IS objectives, monitor implementation, and improve;
- Ensure effectiveness and continuity of ISMS within their units;
- Regularly enroll staff in IS training;
- Protect Company's information assets and ensure proper classified use.

Internal Audit

- Monitor IS standards, rules, and procedures;
- Develop and implement IS audit programs;
- Report nonconformities and recommendations to Management;
- Notify IS responsible staff of identified risks;
- Organize external audits of ISMS.

Administration & HR Department

- Support ISMS implementation;
- Ensure compliance with the Law on Personal Data Protection in HR policies and procedures;
- Ensure confidentiality when handling employee personal data;
- Reflect general IS responsibilities in job descriptions;
- Impose disciplinary measures for IS violations in accordance with law and internal regulations;
- Ensure proper documentation under Records Management procedures;
- Organize IS training and awareness for all staff.

Finance Department

- Record tangible and intangible information assets in financial systems;
- Prepare transfer/acceptance acts for asset custodians and manage movements.

Risk Reduction Department & Legal Department

- Lead incident management in IS;
- Register and monitor IS risks in the Company's risk matrix;
- Define and manage IS risk indicators;
- Monitor IS risk assessments and mitigation plans;
- Support IT in incident resolution;
- Detect, block, and respond to cyberattacks;
- Ensure IS during planning and implementation of changes;
- Ensure equipment, physical, and environmental security;
- Organize ISMS audits jointly;
- Ensure compliance with laws;
- Incorporate IS requirements into third-party contracts and monitor compliance;

- Inform relevant units of new legal requirements;
- Align ISMS with other standards and laws.

All Employees

- Comply with internal IS rules and procedures;
- Immediately report actual or potential IS risks or incidents;
- Participate in IS training and development programs;
- Consistently apply IS in daily operations.

Suppliers & Contractors

- Immediately report IS incidents identified during cooperation;
- Comply with IS requirements under contracts with the Company.

Information Technology Department

- Ensure security of information exchange and transmission;
- Manage network security and access rights;
- Manage IS incidents;
- Develop business continuity plans;
- Ensure communications and operational management;
- Develop, deliver, and maintain software;
- Develop and implement ISMS objectives and plans.

CONTROL

This Policy shall be reviewed annually by the Management Team and submitted to the Board of Directors for amendment as required.