Attachment to decision No A/288
of the Executive Officer of the
"Mongolian Stock Exchange"
JSC on November 22, 2023

МОНГОЛЫН
ХӨРӨНГИЙН БИРЖ

INFORMATION SECURITY POLICY

Ulaanbaatar
2023

Version 1.0

For: All staff

Type of document:	Policy
State of document:	
Classification:	Open to the public
Approved date:	2023.11.22
Боловсруулсан ажилтан:	Senior specialist of the Administration and Finance Department
Approved by:	Executive Officer
Document holder:	Operating Department, Information Technology Division, Information Security Specialist

Version history of the document

Version	Last updated date	Note	Employee who changed	Approved
1.0	2023.11.21	First version	Senior specialist of the Administration and Finance Department	

CONTENTS

ONE. GENERAL PROVISIONS

1.1. The purpose of this policy is to implement the information, information systems, and infrastructure used in the operations of "Mongolian Stock Exchange" JSC (hereinafter referred to as the "Company"), their use, storage, protection, confidentiality, integrity, accessibility, continuity of operation and control.

1.2. In information security operations, the company shall conduct operations in accordance with the relevant laws, rules, and regulations of Mongolia and the International Information Security Management System ISO 27001:2022 standard.

1.3. The company shall work in full compliance with the laws, rules, regulations, instructions, recommendations, contractual obligations, and conditions issued by the regulatory body.

1.4. The implementation of the information security policy also applies to employees, outsourced employees, stakeholders, customers, partners, trading system users, and member companies, and the Exchange shall provide necessary information on the policy and cooperate.

1.5. When implementing this policy, relevant procedures and methods shall be developed and followed.

1.6. The information security policy shall be open to the public.

TWO. MANAGERIAL LEADERSHIP

2.1. The Company's Executive Management and Board of Directors shall fully support the implementation of the information security management system and take the following steps to ensure its effectiveness:

- 2.1.1. Develop and approve information security policies and objectives in line with the company's business plans and conditions.
- 2.1.2. Implementation of the information security management system (hereinafter referred to as "ISMS") shall be consistent with the company's business and other operations.
- 2.1.3. Support the introduction, implementation, sustainability, and continuous improvement of the ISMS, and regularly provide the required resources.
- 2.1.4. Have a clear understanding of the importance of optimally organizing activities to ensure information security and meeting the requirements of the ISMS.
- 2.1.5. Encourage all employees to contribute to the effectiveness of the management system by taking all measures to bring the ISMS to its planned results.
- 2.1.6. The company's information security policy, goals, and controls shall be reflected in the responsibilities and performance evaluations of each employee.

THREE. POLICY FOR OPERATIONS

3.1. The Board of Directors shall implement the following policies in order to guide the company's information security activities:

- 3.1.1. The company's IT services and trading systems, internally developed software, products, and services shall ensure the privacy, accessibility, and integrity of the information of customers, members, and cooperating organizations.
- 3.1.2. Identify and assess potential information security risks, manage information security risks in order to prevent and reduce risks, and ensure continuous improvement.
- 3.1.3. Conduct activities that comply with relevant information security laws, regulations, standards, regulatory agency requirements, customer contract requirements, and stakeholders' needs.
- 3.1.4. To ensure information security, an information security management system shall be effectively implemented regularly reviewed, and improved over the long term.

3.2. The Board of Directors shall discuss the activities included in the information security policy and regulations at annual meetings and make the necessary decisions promptly, and rationally.
3.3. The board of directors shall set information security goals for each department and unit in accordance with this policy, monitor and evaluate implementation on a regular basis, and make improvements based on the evaluation.

ДӨРӨВ. АЖИЛТНУУДЫН ХҮЛЭЭХ ҮҮРЭГ

4.1. All employees of the company shall be responsible for the main functions aimed at introducing, implementing and improving the ISMS according to the following schedule:

Duty	Main respondent
Determining the company's state, setting strategies and directions, developing information security policies, and holding management analysis meetings.	• Executive Director • The Board of Direcotrs • Information Security Risk Management Team
Development of goals, objectives, and plans of ISMS	• Information Security Risk Management Team • Information security specialist
ISMS document management	• Information security specialist • Information Security Risk Management Team
To provide training and awareness of information security to all employees.	• Information security specialist • Information Security Risk Management Team
ISMS internal audit	• Internal auditor • Risk management specialist • Risk management team • Information security internal control and audit team
Corrective and preventive operations	• Information security specialist • Risk management specialist • Internal auditor • All staff
Information security risk assessment and risk mitigation plan	• Risk management specialist • Information security specialist • Information Security Risk Management Team
• Compliance of ISMS with other standards and laws • Compliance with laws and regulations	• Information technology department • Legal division

	• Information security specialist • Risk management specialist
Implementation, monitoring, and improvement of the ISMS	• All staff • Information security specialist • Risk management specialist • Information Security Risk Management Team • Information technology department
Alignment of the ISMS when planning and implementing change	• Information technology department
Organization of external inspection and inspection at ISMS	• Information security internal control and audit team
Paying attention to the proper protection of the company's information assets and receiving the information at the appropriate level	• All staff
Human resources security	• Administration and finance department
Safety of equipment and environment	• Information technology department
• Communication and operation management • Security of information exchange and transmission • Network security and access management • Information security management • Business Continuity Plan	• Operation department • Information technology department • Business development division
Software development, delivery, and operation	• Information technology department • Program developer
• Compliance with the requirements of the contract and agreement	• Legal division

FIVE. RESULTS TO BE ACHIEVED

5.1. Establish a system to prevent the loss of information security.
5.2. It is customary to assess the information security of the system.
5.3. Information security risk shall be reduced.
5.4. ISMS shall be provided regularly and continuously improved.

SIX. LIABILITY

6.1. The employee who violates this policy shall be held responsible as stipulated in the relevant laws, internal labor rules, and labor contracts.
6.2. The implementation of this policy shall be monitored by the company's IT department and internal audit specialist.