[Translation]

System Access Control Policy

1. Introduction

1.1. Objectives

- To establish guidelines and access control to the data, network systems, and information systems of the Company.
- To protect the data, network systems, and information systems of the Company from unauthorized access.
- To establish procedures for managing, approving, or authorizing the creation, modification, withdrawal, and cancellation of user accounts, including important access rights to the Company's information systems.

1.2. Scope

This policy covers access to network systems and information systems, including the use of Company’s data

1.3. Definition

- “Need-to-know” refers to the authorized privilege to access or use information only as necessary for work purposes and requires approval before use.
- “Defense in Depth” refers to maintaining security through multiple layers of protection.
- “Least Privilege” refers to granting the minimum necessary privileges to perform duties.

2. Policy

2.1. General Criteria for Network System Control

- Access to all information systems of the Company must always be authenticated and access to systems should be granted based on the principle of "need-to-know" except for user accounts and email accounts for new employees, which are automatically assigned by the Company.

- Access control to information systems must begin with denying all access requests and then consider approving access only to systems necessary for users.
- The principle of "Defense in Depth" must be implemented by managing risks through various methods, such as using different technologies, defining operational procedures, controlling physical access, or assigning responsibilities to employees. This approach helps to enhance the protection levels of data and information systems.
- External access to information systems and connections to the Company's network from external sources must be strictly controlled in accordance with ISMS-PL-10 Third Party Security Policy and ISMS-PL-04 Network Management Policy.

3. User Access Control

- Control over access to the Company's information systems and services must cover from the initiation of users' permissions to their termination.
- Requests to access the Company's information systems must be reviewed and approved according to the procedures ISMS-PC-01 User Access Request Procedure.
- Only authorized users have the access to the Company's information systems, and access rights must be restricted to the appropriate level according to work responsibilities following the "Least Privilege" principle. Additionally, there must be appropriate Segregation of Duties among employees to prevent any individual from accessing systems beyond their job responsibilities. The Company reserves the right to change, restrict, or revoke user access rights as deemed necessary at all times.
- Each authorized user must have their own user account and must use that account throughout their tenure with the Company. User accounts must be deactivated when the user is no longer employed by the Company. The use of shared user accounts must comply with ISMS-PC-07 Share User Account Procedure.

- Users are responsible for maintaining the security of their user accounts and passwords.
- Users must go through identity verification every time they log in to the system. The method of verification should be chosen based on risk assessment and budget constraints. Generally, user identity verification methods can be categorized into three types:
  1. Something the user knows, such as a password.
  2. Something the user has, such as a magnetic stripe card or a smart card.
  3. Something the user is, such as fingerprint or facial recognition.
- When considering the selection of user identity verification methods for critical systems or applications, it is advisable to employ a combination of at least two types of verification methods to enhance security.
- All types of computers must be protected with passwords, and the operating system must verify the correctness of the password when users log in.
- Server, desktop, and laptop should be configured to automatically log out or lock the screen when not in use for a certain period, unless there are technical limitations, in which case approval must be obtained from the VP of Information Technology Security Department or the authorized personnel.
- Passwords must be secure and at the same time easy for the owner to remember. Passwords must be kept confidential as specified in the Information Security System Regulations and ISMS-ST-02 Password Standard.

4. System and Application Access Control

- Data/System owners must approve access requests to their data/systems, and authorized individuals must be designated to approve access requests in accordance with the procedures ISMS-PC-01 User Access Request Procedure.
- User accounts at the system level (e.g., administrators) must be carefully assigned to users following the procedures specified in ISMS-PC-0 3 Access Matrix Procedure. Users should only use System-level privileges for tasks related to

system administration. For other general tasks, users should utilize regular user-level accounts.

- Privileged access refers to rights beyond normal job duties and must be managed as follows:
  1. Set time limits for the use of accounts with special privileged access.
  2. Revoke privileges and/or user accounts immediately upon completion of the associated activity.
  3. Limit the connection time to important systems/applications to prevent unauthorized access.
  4. Users must not use multiple sessions for critical systems/applications unless necessary. If multiple sessions are used, users are responsible for any negative consequences.
- Approval for granting special privilege access rights, from AVP level upwards in the Information Technology Security Department, must be obtained before approving access requests.
- "Guest" user accounts that can access the Company's systems, applications, and networks must be suspended.
- Employees must not install any code that can bypass access control mechanisms or user identity verification mechanisms, whether they are part of the operating system, access control software, or other applications.
- Critical systems must be operated on computers specifically provided to support those systems, using shared resources with other reliable systems must be documented by the Infrastructure department.
- Database access must be carried out through applications only, and direct access should be limited to cases where necessary or with limitations in the application, such as for database maintenance by system administrators or authorized personnel.
- Access to system utilities with high-level privilege, which allows bypassing various system/application controls, must be limited to users or system administrators who require such access. Temporary approval for accessing and using such

system utilities by other individuals must be reviewed and approved in each case.

- These system utilities must be separated from applications and other software to restrict access to authorized users only.
- Services unrelated to job duties or business operations must be disabled.

4.1. Data Access Control

Access rights to data files must be controlled and granted only as necessary to maintain the accuracy and integrity of the data and to segregate user responsibilities.

4.2. Access Control to Information Systems of External Service Providers or Partners

- Requests to access the Company's information systems by external service providers or partners must undergo review and approval according to ISMS-PC-01 User Access Request Procedure.
- External service providers or partners must agree to comply with the Company's information technology security policies and the Third-Party Code of Conduct before being authorized to access the Company's information systems.
- Connection routes and access control methods must be established to limit external service providers or partners to accessing only the hosts/servers designated by the Company.
- User accounts created for individuals who are not employees of the Company must have their usage periods limited, typically set at 30 days unless otherwise justified. Access to the Company's internal network and information systems must be performed using equipment provided by the Company or authorized equipment registered with the Company.

4.3. Review and Revocation of Information System Access Rights

- All actions involving the creation, revocation, and modification of user accounts by system administrators using special privileges users must be logged.
- Regular reviews of all critical system access rights must be conducted, considering the following criteria:

1. Review in accordance with ISMS-WI-05 Access and Privilege Matrix Work Instruction.
2. User access rights must be reviewed at least once a year.
3. User accounts with special privileges and remote access rights must be reviewed at least once a year.
4. User system access rights must be reviewed whenever there are changes or when the user terminates employment with the Company.

- All system access rights must be revoked immediately when a user no longer requires access to the system. This responsibility lies with the user and the supervisor, who must notify the system administrator that the user no longer requires access to the system.
- Supervisors must promptly inform the system administrator when individuals under their supervision, such as temporary employees or consultants, no longer require access to the Company's information systems and equipment.

5. Reviewing and Updating Policy

Information Security Policies, procedures, and any other guidelines shall be reviewed and updated by management at least once a year to ensure that its content is complete, effective, and can be used appropriately.

6. Penalties

Any breach, violation, negligence, or non-compliance with the policy, work instruction, and relevant supporting documents whether intentional or not, the Company may consider penalties at its discretion or disciplinary action in accordance with the Company’s policies. Any breach or violation of the policy is deemed to be an illegal act, the Company may consider further legal proceedings.

(The policy shall be effective as of 22 August 2023 onwards.)