

Cyber Security Standard for Third Party (Translation)

AIS Group

Version: 2.0

Document Owner: Cyber Security

Effective Date: 25 August 2026

Table of Contents

1. INTRODUCTION.....	4
1.1 OBJECTIVES.....	4
1.2 SCOPE.....	4
1.3 DEFINITIONS	4
1.4 EXCEPTIONS	7
1.5 CONSEQUENCES FOR NON-COMPLIANCE.....	7
2. ROLES AND RESPONSIBILITIES	8
2.1 COMPANY'S DESIGNATED PROJECT REPRESENTATIVE	8
2.2 THIRD PARTY	8
3. CYBER SECURITY STANDARD	8
3.1 REGULATORY AND COMPLIANCE	8
3.2 HUMAN RESOURCE MANAGEMENT	9
3.3 SUBCONTRACT MANAGEMENT.....	9
3.4 CYBER SECURITY RISK MANAGEMENT.....	10
3.5 ASSET MANAGEMENT	10
3.6 MANAGEMENT OF TECHNICAL VULNERABILITIES	11
3.7 PHYSICAL AND EQUIPMENT SECURITY	14
3.8 ACCESS CONTROL MANAGEMENT	15
3.8.1 Identity and Access Management.....	15
3.8.2 Password Management.....	16
3.8.3 Remote Access.....	18
3.8.4 Network Access Control	18
3.8.5 Access to Source Code.....	19
3.9 ENDPOINT SECURITY MANAGEMENT	19
3.9.1 Clear Desk and Clear Screen	19
3.9.2 Protection Against Malicious Software.....	20
3.9.3 Software Licensing.....	20
3.9.4 Mobile Computing and Teleworking.....	20
3.10 CHANGE MANAGEMENT	21
3.11 APPLICATION SECURITY MANAGEMENT.....	22
3.11.1 Application Security Requirements.....	22
3.11.2 Secure Coding	22
3.11.3 Separation of Development, Test, and Production Environments	22
3.11.4 Automatic Session Timeout.....	23

3.11.5	API and Third-Party Component Security	23
3.12	DATA SECURITY MANAGEMENT	23
3.12.1	Data Classification and Handling	23
3.12.2	Data Encryption	24
3.12.3	Data at Rest.....	24
3.12.4	Data in Transit	25
3.12.5	Data Backup and Restoration	26
3.12.6	Information Disposal	26
3.12.7	Test Information	27
3.13	INFRASTRUCTURE SECURITY MANAGEMENT	27
3.13.1	Cloud Security Management	27
3.13.2	Network Security Management	28
3.13.3	Logging and Monitoring	28
3.13.4	System Management.....	30
3.14	ARTIFICIAL INTELLIGENCE SECURITY MANAGEMENT.....	31
3.15	AWARENESS, EDUCATION AND TRAINING	32
3.16	CYBER SECURITY INCIDENT MANAGEMENT	32
3.17	BUSINESS CONTINUITY MANAGEMENT	33

Cyber Security Standard for Third Party

1. Introduction

1.1 Objectives

- 1) To establish cyber security standards for the control and governance of Third Parties that connect to, access, use, or perform activities involving the Company's information systems, computer systems, and information assets, including external service providers, business partners, contractors, subcontractors, and any other parties performing services or acting on behalf of the Company.
- 2) To protect the Company's information systems, computer systems, and information assets from unauthorized access, cyberattacks, theft, destruction, disruption, malware, cyber threats, or activities performed by Third Parties that may adversely affect the Company's business operations.
- 3) To reduce cyber security, information system security, and information security risks to the Company arising from Third Party connectivity, access, service provision, or operational activities.
- 4) To ensure that activities, services, and operations performed by Third Parties in connection with the Company are conducted securely and in compliance with the Company's requirements, applicable laws, regulations, contractual obligations, and relevant standards.

1.2 Scope

This Standard covers the cyber security, information system security, and information security requirements for protecting the Company's information systems, computer systems, and information assets in relation to services, connectivity, system or information access, and activities performed by Third Parties, including service providers, business partners, contractors, and subcontractors that interact with the Company's information technology environment or perform services on behalf of the Company.

1.3 Definitions

- 1) **"Company"** refers to Advanced Info Service Public Company Limited and its subsidiaries within the AIS Group.
- 2) **"Third Party"** refers to any external personnel, organization, or entity that conducts business or provides services may be granted access to the company's information and information processing equipment. The term also includes any Third Party personnel or organization that are granted rights to access the company's customers' data as below:
 - Business Partner

- Outsource
 - Supplier
 - Service Provider
 - Consultant
 - External Auditor
- 3) **“Information”** refers to information, historical records, messages in documents, computer programs, computer data, images, sounds, marks and symbols, whether stored in a form that can be interpreted for individuals to understand directly or through any equipment or device.
- 4) **“Sensitive Information”** refers to important information that may affect the business operations of the Company. Information that is subject to the requirements of the law, including personal data, must be protected and may not be disclosed to other persons or used for other purposes not related to the business operations of the Company. The leakage of this information may affect operational performance, disrupt business operations, or cause damage to the Company.
- 5) **“Digital Identity”** refers to a digital data set or attribute that is created, stored, and managed by the company to identify and verify the identity of individuals, users, systems, applications, or devices within the company's digital environment. Digital ID is a fundamental component of the authentication process, defining and controlling access rights (Authorization), and managing identities and access to systems (Identity and Access Management: IAM). It also supports secure, reliable electronic transactions.
- 6) **Identity Type** refers to the separation of the characteristics of a person or thing recorded in electronic form, namely, employees, third parties, and RPAs (Robotic Process Automation).
- 7) **“Account”** refers to the user-ID for accessing the Company's computer systems and information, whether it is an employee account, a third party account, a shared account, a central account, including Non-Human such as an RPA account (Robotic Process Automation).
- 8) **“Shared Account”** refers to an account that is shared by more than one person using the same authentication information, such as the same username and password.
- 9) **“Central Account”** refers to a central account formally designated by the Company for use in the administration, control, supervision, or reference as a representative of the System Identity, for its intended purpose and use in a specific manner as required, and with appropriate control, access, and monitoring processes.
- 10) **“Service Account”** refers to a user account created for the use of systems, applications, or services for authentication and the assignment of access rights to resources within the Company's information systems. Such accounts may not be used directly by Non-Interactive Account users but are defined solely to support the operation of automated processes or communication between systems.

- 11) **“User Type”** refers to the separation of users by the company's level of access to computer systems and information, including User Level, Privileged Level, and Service Account Level.
- 12) **“Birthright Access”** refers to a right of access granted to an employee or third party in accordance with its duties and responsibilities as soon as digital IDs and user accounts are created in the system for use in its performance.
- 13) **“Need to know basis”** refers to the principle of disclosing confidential or sensitive information only to users of information who have relevant duties or need to know such information.
- 14) **“Least Privilege”** refers to the granting of access to computer systems and access to information only as necessary for the performance of work.
- 15) **“Authentication”** refers to the process of verifying identity by verifying what is used to verify identity.
- 16) **“Computer System”** refers to all computer tools or device, including hardware and software, networking equipment, wired and wireless, materials, equipment, storage and data transfer, Internet and Intranet systems, as well as electrical and telecommunications equipment that can operate or operate in the same way or similar to computers, both as property of the Company, of its partners and other companies in the process of installation and undelivered, or of employees imported into, installed or used within the Company's business premises.
- 17) **“Critical System”** refers to any information system, application, technology infrastructure, or system that plays an important role in the operation of the business, the provision of services, compliance with laws and requirements, including the security and reputation of the organization. If such systems are interrupted, damaged, breached, or rendered unusable, they may have a significant impact on the Company's operations, finances, compliance with laws, and stakeholder confidence.
- 18) **“Production Environment”** refers to the actual service environment of the Company that supports real corporate and customer information. This environment requires the most stringent security controls, including access measures, event recording, data protection, and change management, to maintain the confidentiality, integrity, and availability of key corporate information and services.
- 19) **“Non-Production Environment”** refers to an environment used for the development, testing, quality inspection, or preparation of a system before implementation. This environment may include Development, Test, QA, UAT, Staging, or Sandbox environments.
- 20) **“Removable Media”** refers to devices or storage media that can be removed from a computer device or electronic device and can be used to store, transfer, or move data between systems

such as USB Flash drive/Thumb drive, hard drive (HDD/SSD), Memory Card (SD Card, MicroSD Card, CF Card), CD/DVD/Blu-ray Disc, and other portable storage devices of similar nature, excluding magnetic tape/tape cartridge storage media and server hard drive applications.

- 21) **“Network Segmentation”** refers to the process of designing, administering, and controlling a network structure, divided into multiple parts or domains, in order to limit the communication between networks according to the level of risk and reliability, and reduce the impact of unauthorized access or the spread of threats.
- 22) **“Remote Access”** refers to the connection to access the Company's computer or network system (through internal communication channels) or from outside the Company (through the Internet).
- 23) **“Vulnerability”** refers to deficiencies or weaknesses of information systems, information assets, processes, personnel, or security control measures that may be exploited or triggered by threats and may lead to breaches of confidentiality, integrity, or availability of corporate information, systems, or services.
- 24) **“Residual Risk”** refers to the level of risk that persists after various control measures have been implemented.
- 25) **“Penetration Test”** refers to the proactive testing of security using the same techniques, tools, and methods that an attacker may use to assess the effectiveness of security control measures, identify vulnerabilities, and provide remediation recommendations to help reduce risks and increase the level of security of an organization's information systems.
- 26) **“Rollback”** refers to the operation of restoring the condition of an information system, application, or data to a version or state prior to a change, such as an update, installation, or system update, if such a change causes a fault, affects service, or poses a risk to the organization.
- 27) **“Artificial Intelligence (AI)”** refers to technology created to enable computers to mimic human behavior, such as learning, thinking, analyzing, making decisions, solving problems, and relying on large amounts of information to train themselves to be able to work more efficiently and accurately.

1.4 Exceptions

If a Third Party is unable to comply with this Standard, it shall notify the Company's designated project representative for review and consideration under the Company's risk management process.

1.5 Consequences for Non-Compliance

If a Third Party violates this Standard or any of the Company's policies, standards, guidelines, or procedures, and such violation results in or may result in damage to the Company, the Company reserves the right to take actions in accordance with the applicable service agreement or contractual obligations.

2. Roles and Responsibilities

2.1 Company's Designated Project Representative

The Company's designated project representative shall coordinate with Third Parties and oversee compliance with the Company's policies and this Standard.

2.2 Third Party

- 1) Third Parties shall learn, understand, and strictly comply with the Company's policies, standards, procedures, guidelines, instructions, and processes related to cyber security.
- 2) Third Parties shall fully cooperate with the Company in protecting the Company's computer systems, information systems, and information assets.
- 3) Third Parties shall immediately notify the Company upon becoming aware of any improper or inappropriate activities, or any attempt to compromise, steal, damage, disrupt, or unlawfully access the Company's systems or information assets that may cause harm to the Company.

3. Cyber Security Standard

The Third Parties shall follow the security practices to achieve the following objectives:

- **Confidentiality** – Protecting the confidentiality of information. Prevents access and disclosure of information by unauthorized persons and protects personal or the Company's proprietary information.
- **Integrity** – Ensuring that the Company's information is not altered, modified, or destroyed by any unauthorized person.
- **Availability** – Ensuring authorized users can access information and services quickly and reliably.

3.1 Regulatory and Compliance

Objective: To ensure that Third Parties comply with applicable laws, regulations, regulatory requirements, and contractual obligations related to the provision of services, access to the Company's information systems, or processing of the Company's information, in a complete and appropriate manner.

- 1) Third Parties shall comply with all applicable laws, regulations, regulatory requirements, and contractual obligations related to the services provided to the Company, including requirements concerning cyber security, personal data protection, intellectual property, and other relevant requirements applicable to the nature of the services.
- 2) Any software, tools, or digital resources used by Third Parties in providing services to the Company shall be lawfully acquired and must not infringe upon the intellectual property rights of any third party.

- 3) Third Parties shall protect the confidentiality of the Company's information in accordance with the applicable Non-Disclosure Agreement (NDA) and shall not use, disclose, reproduce, transfer, or distribute such information beyond the authorized purpose or to any unauthorized person.
- 4) Third Parties shall promptly notify the Company of any actual or suspected non-compliance with applicable laws, regulatory requirements, or contractual obligations that may affect the Company's services, information, or systems.

3.2 Human Resource Management

Objective: *To reduce cyber security and data protection risks arising from personnel of Third Parties who perform work for the Company or have access to the Company's information, information systems, or computer systems.*

- 1) Third Parties shall ensure that their personnel who perform work for the Company or have access to the Company's information or information systems receive appropriate cyber security and personal data protection communications, training, or awareness programs commensurate with their roles, responsibilities, and associated risk levels.
- 2) The communications, training, or awareness programs specified in Clause 1) shall, at a minimum, cover the protection of Company information, information confidentiality, appropriate use of systems and access rights, reporting of cyber security incidents or anomalies, and personal data protection requirements relevant to their duties.
- 3) Where the nature of the work involves elevated risk or access to sensitive information, critical systems, or personal data, the Company may require personnel of Third Parties to complete additional training, acknowledge specific requirements, or undergo an assessment of understanding prior to commencing work, as deemed appropriate by the Company.
- 4) Third Parties shall ensure that their personnel are informed of and comply with the Company's policies, standards, procedures, and cyber security and data protection requirements relevant to their work.

3.3 Subcontract Management

Objective: *To reduce cyber security and information security risks that may arise from the use of subcontractors by requiring Third Parties providing services to the Company to appropriately oversee, control, and remain responsible for the activities and performance of their subcontractors based on the associated risk level.*

- 1) Third Parties shall notify the Company of any subcontractors, subcontracted service providers, or other external parties engaged in providing services to the Company, including the scope of work

and the nature of their access to the Company's systems or information, as required by the Company.

- 2) Third Parties shall oversee and ensure that their subcontractors comply with the Company's cyber security, data protection, and other applicable requirements at a level no less stringent than those applicable to the Third Parties themselves.
- 3) Third Parties shall remain fully responsible and accountable for the activities, risks, security incidents, and damages arising from the actions or omissions of their subcontractors as if such activities were performed by the Third Parties themselves.
- 4) Third Parties shall not appoint or replace subcontractors that have a material impact on the services provided to the Company without prior notification to, or approval from, the Company in accordance with the Company's requirements.

3.4 Cyber Security Risk Management

Objective: To ensure that Third Parties are able to appropriately identify, assess, monitor, and manage cyber security risks associated with the provision of services, access to the Company's information systems, or processing of the Company's information, in accordance with the applicable level of risk.

- 1) Third Parties shall establish and maintain a cyber security risk management process appropriate to the nature of the services provided and shall perform cyber security risk assessments relevant to the services delivered to the Company.
- 2) Third Parties shall undergo cyber security and data protection risk assessments in accordance with the Company's requirements prior to service commencement, during service delivery, or whenever there are material changes affecting the services provided to the Company.
- 3) Third Parties shall cooperate with the Company by providing information, evidence, documentation, or participating in assessments and audits as required by the Company to enable an appropriate evaluation of the risks associated with the services provided.
- 4) Where risk assessments identify risks or deficiencies requiring remediation, Third Parties shall develop a risk treatment plan or corrective action plan, including implementation timelines, and submit such plans to the Company for review and consideration.
- 5) Third Parties shall implement plans approved by the Company and provide progress updates or implementation results within the timeframes specified by the Company.

3.5 Asset Management

Objective: To ensure that the Company's assets are properly identified, inventoried, and controlled throughout their lifecycle in order to prevent loss, unauthorized access, and cyber security risks in alignment with applicable standards and best practices.

- 1) Third Parties shall establish, maintain, and keep an Asset Inventory for assets, systems, information, networks, connections, and services used in providing services to the Company or associated with the Company's information or systems. At a minimum, the Asset Inventory shall include hardware, software, information, networks, connectivity, and services, including cloud services and outsourced services.
- 2) The Asset Inventory specified in Clause 1) shall include, at a minimum, information relating to asset categorization, information classification, and the ownership or designated responsible party for each relevant asset.
- 3) Third Parties shall review and update the Asset Inventory at least annually or whenever there are changes to assets, systems, information, connectivity, or services provided to the Company.
- 4) Third Parties shall provide the Asset Inventory or other related information to the Company upon request, to the extent necessary for the Company's risk management, assessment, audit, or cyber security governance activities.

3.6 Management of Technical Vulnerabilities

Objective: To identify weaknesses and protect the Company's computer systems and information from technical vulnerabilities that could be exploited to conduct cyberattacks or other malicious activities.

- 1) Operating systems, applications, and network devices connected to the Company's network shall be securely configured in accordance with the minimum security requirements or Security Baselines specified by the Company.
- 2) Vulnerability Assessment and Penetration Testing shall be conducted for computer systems, software, network infrastructure, and any other devices or systems involved in providing services to the Company prior to deployment or use in the Production Environment. Such assessments shall be performed periodically based on the applicable risk level and whenever a Major Change occurs. Identified vulnerabilities shall be remediated in accordance with the processes and timelines specified by the Company.
- 3) Third Parties performing Vulnerability Assessment or Penetration Testing shall submit the testing plan, including the tools to be used, to the Company's designated project representative and obtain the Company's prior written approval before conducting any Vulnerability Assessment or Penetration Testing activities. Personnel performing such testing should possess qualifications or industry-recognized certifications appropriate to the nature of the assessment.
- 4) Approved security patches and firmware updates for servers, network devices, and security-related systems or devices shall be obtained from trusted sources and applied within an appropriate timeframe based on the associated risk level. Records of all installations shall be maintained for audit and traceability purposes. New systems shall be deployed with current security patches applied. Software, operating systems, or devices that have reached End-of-Support (EOS) or End-of-Life (EOL) status should not be used unless a risk assessment has been performed and

appropriate compensating controls have been implemented and accepted through the risk management process.

- 5) Appropriate backups of relevant data shall be performed prior to applying patches or firmware updates to support recovery in the event of adverse impacts resulting from the update process.
- 6) The Company reserves the right to conduct Vulnerability Assessment, Penetration Testing, and other attack simulation activities, including but not limited to Red Team Exercises and Attack Surface Monitoring, on systems providing services to the Company's customers without prior notice.
- 7) Internet-facing Company applications or systems shall undergo Vulnerability Assessment and Penetration Testing at the minimum frequencies specified by the Company, or whenever a Major Change occurs, to identify security weaknesses and assess the overall security posture of the systems, as follows:

System Type	Vulnerability Assessment	Penetration Testing
High-Priority/Significant System	Once per year	Once per year
Medium-Priority System	Once every 24 months	Once every 24 months
Low-Priority System	Once every 36 months	Once every 36 months
System related to PCI DSS	Quarterly	Once per year
System related to CSA Star	Once per year	Once per year
System related to ISO	Once per year	Once per year
System regulated by the Bank of Thailand (BOT)	Once per year	Once per year
Systems related to NDID and Public IDP	Once per year	Once per year

Where vulnerabilities are identified through Vulnerability Assessment or Penetration Testing, remediation shall be performed in accordance with the Company's requirements as follows:

- In the case of a new computer system, application, or feature, deployment to the Production Environment shall be permitted only after the following requirements have been completed:

Severity Level	Remediation Requirement
Critical / High	All vulnerabilities shall be remediated prior to deployment to the Production Environment.

Severity Level	Remediation Requirement
Medium	1. A Vulnerability Remediation Plan shall be submitted to the Company's designated project representative within 15 days of receiving the latest assessment results. 2. Vulnerabilities shall be remediated within 60 days of receiving the latest assessment results. If remediation cannot be completed within the required timeframe, the Third Party shall notify the Company's designated project representative and initiate the Company's Risk Acceptance Process using a Risk Acceptance Form.
Low	1. A Vulnerability Remediation Plan shall be submitted to the Company's designated project representative within 15 days of receiving the latest assessment results. 2. Vulnerabilities shall be remediated within 90 days of receiving the latest assessment results. If remediation cannot be completed within the required timeframe, the Third Party shall notify the Company's designated project representative and initiate the Company's Risk Acceptance Process using a Risk Acceptance Form.

- In the case where vulnerabilities are identified through Vulnerability Assessment and Penetration Testing conducted in accordance with the schedule specified by the Company, the following actions shall be taken:

Severity Level	Requirement
Critical / High	1. A Vulnerability Remediation Plan shall be submitted to the Company's designated project representative within 15 days of receiving the latest assessment results. 2. Vulnerabilities shall be remediated within 45 days of receiving the latest assessment results. If remediation cannot be completed within the required timeframe, the Third Party shall notify the Company's designated project representative and initiate the Company's Risk Acceptance Process using a Risk Acceptance Form.

Severity Level	Requirement
Medium	1. A Vulnerability Remediation Plan shall be submitted to the Company's designated project representative within 15 days of receiving the latest assessment results. 2. Vulnerabilities shall be remediated within 60 days of receiving the latest assessment results. If remediation cannot be completed within the required timeframe, the Third Party shall notify the Company's designated project representative and initiate the Company's Risk Acceptance Process using a Risk Acceptance Form.
Low	1. A Vulnerability Remediation Plan shall be submitted to the Company's designated project representative within 15 days of receiving the latest assessment results. 2. Vulnerabilities shall be remediated within 90 days of receiving the latest assessment results. If remediation cannot be completed within the required timeframe, the Third Party shall notify the Company's designated project representative and initiate the Company's Risk Acceptance Process using a Risk Acceptance Form.

3.7 Physical and Equipment Security

***Objective:** To prevent unauthorized access to premises and equipment that may cause damage to or interfere with the operation of the Company's computer systems.*

3.7.1 Physical Security

- 1) Third Parties entering or performing work at the Company's premises shall properly wear identification badges issued by the Company in a clearly visible manner at all times while working at the Company's premises.
- 2) Third Parties shall not disclose the locations of critical areas, such as data processing areas, executive rooms, or any other restricted or critical areas designated by the Company.
- 3) Areas containing the Company's critical information or systems shall be protected by appropriate physical and environmental security measures. Such measures shall, at a minimum, cover 24x7 monitoring, fire detection, alarm systems, automatic fire suppression,

temperature and humidity control, contingency plans for electrical systems, and emergency switches installed in appropriate locations.

- 4) Any movement of equipment into or out of critical areas shall be authorized by the responsible party and recorded each time. Controls shall also be implemented for the transportation of equipment or storage media to prevent loss or unauthorized access.

3.7.2 Equipment Security

- 1) Third Parties shall ensure that equipment and supporting facilities used in providing services to the Company are regularly maintained to ensure their availability. Maintenance activities shall be recorded and reviewed at appropriate intervals.
- 2) The Company does not permit the use of any type of Removable Media in order to prevent risks relating to data leakage, unauthorized access to information, and malware propagation, unless an exception has been specifically approved in accordance with the Company's procedures.
- 3) Prior to disposal or reuse of equipment or storage media, data shall be securely erased or destroyed in accordance with the Company's requirements. Where data cannot be completely sanitized, physical destruction shall be performed in accordance with applicable requirements.

3.8 Access Control Management

Objective: To ensure that access to information and computer systems is restricted to authorized users only, and to prevent unauthorized access to systems and services.

3.8.1 Identity and Access Management

- 1) Third Parties shall establish an appropriate process for managing identities, user accounts, and access rights to information or computer systems. Such process shall cover user registration, access requests, approvals, changes, suspension, and revocation of access rights. Where the Third Party owns the system, such process shall be documented in writing. Where the Third Party accesses the Company's information or computer systems, the Third Party shall comply with the process specified by the Company.
- 2) Third Parties shall define and manage access rights in accordance with the Least Privilege Principle and apply appropriate access control models, such as Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC). An access rights register or role register shall be maintained, as appropriate, and access rights shall be reviewed at least annually.
- 3) Users and system administrators shall have user IDs that can identify and be traced back to the account owner, in accordance with the principle of one person per user ID, unless

there are technical limitations or approved justifications, together with appropriate additional control measures.

- 4) Segregation of Duties (SoD) shall be implemented to reduce the risks of fraud, errors, and control bypass. At a minimum, duties shall be segregated among the requester, approver, operator, and reviewer. Where segregation of duties cannot be implemented, compensating controls shall be established.
- 5) The granting or modification of access rights shall be based on a justified business need, approved by an authorized person, and aligned with the user's roles and responsibilities, the Least Privilege Principle, and the period necessary for performing the work. For Third Party access rights, an expiration date or access period shall be specified in all cases.
- 6) The use of shared accounts, central accounts, or Privileged Accounts shall be limited to necessary cases due to technical or operational constraints. Such accounts shall have clearly assigned account owners, a register linking users to the accounts, usage controls, and monitoring or periodic reviews as specified.
- 7) User access rights shall be reviewed and updated when there are changes to roles, duties, responsibilities, or when access to information or computer systems is no longer required.
- 8) Access rights to systems and services shall be appropriately suspended or revoked upon expiration of the authorized access period, completion of work, contract termination, or when access is no longer required. The user register shall also be updated within no more than three business days from the effective date of suspension or revocation of access rights.

3.8.2 Password Management

3.8.2.1 Password Configuration

- 1) Passwords that are easy to guess or susceptible to brute-force attacks shall not be used, including passwords based on personal information, passwords identical to the user ID, or blank passwords.
- 2) Passwords used for external systems outside the organization shall not be reused for the Company's systems.
- 3) Password configuration shall comply with the Company's requirements as follows:

Requirement Area	Systems that access sensitive information, personal data, or are classified as high risk	Others
Length and Expiration Period	User-level passwords shall be at least 12 characters in length and changed at least every 90 days.	Reference may be made to international

Requirement Area	Systems that access sensitive information, personal data, or are classified as high risk	Others
	- Privileged User passwords shall be at least 20 characters in length and changed at least every 90 days. - Service Account passwords shall be at least 30 characters in length and changed at least annually.	standards, such as NIST SP 800-63B-4
Complexity	Passwords shall meet the following requirements: - Contain lowercase letters, uppercase letters, numbers, and special characters, such as @ or #. - Not contain sequential numbers or running numbers, such as 12345678. - Not contain easily guessable words or dictionary words, such as Password - Not reuse at least the previous 5 passwords.	Reference may be made to international standards, such as NIST SP 800-63B-4
Failed Password Attempts	Incorrect password entry shall be tolerated for no more than 5 attempts. If the number of incorrect attempts exceeds the specified limit, the computer system shall immediately and temporarily suspend or lock the relevant user account.	Reference may be made to international standards, such as NIST SP 800-63B-4
Password History	The system shall be able to verify users' password history to prevent password reuse. At a minimum, the system shall be able to check against the previous 5 passwords.	Reference may be made to international standards, such as NIST SP 800-63B-4

3.8.2.2 Password Usage

- 1) Third Parties shall keep passwords confidential and personal to the account holder. Passwords shall not be disclosed, shared, transferred, or used jointly with any other person.
- 2) Default passwords shall not be used. The system shall require users to change their passwords immediately after first login, or when a new system is installed or a computer system is upgraded.
- 3) Passwords shall not be hard-coded in computer systems.
- 4) Where passwords are required to be stored, they shall be stored in encrypted form or managed using a password management tool approved by the Company. Passwords shall not be stored in clear text.
- 5) A secure method shall be established for distributing passwords or user IDs to users.

3.8.3 Remote Access

- 1) Third Parties shall implement appropriate controls for Remote Access and shall assign access rights in accordance with the Least Privilege Principle, define the access period, and regularly review access rights to prevent unauthorized access to computer systems, networks, and servers. Any access to the Company's systems or networks shall also comply with the Company's requirements.
- 2) Remote Access to the Company's systems shall be subject to the established access request process. The access period or expiration date of access rights shall be specified, Multi-Factor Authentication (MFA) shall be used, and all access logs shall be retained for audit and traceability purposes.
- 3) Remote Access to the Production Environment shall be strictly controlled and limited to what is necessary for the intended purpose. Access rights shall be suspended or revoked immediately when they are no longer required.

3.8.4 Network Access Control

- 1) Third Parties shall implement Network Segregation and appropriate security controls to prevent attacks or unauthorized access to networks. Where connectivity to the Company's network is required, Third Parties shall comply with the Company's requirements.
- 2) Network access by Third Parties to the Company's network shall be restricted to authorized users only, and secure authentication shall be implemented to prevent source spoofing.
- 3) Devices connected to the Company's network shall be authorized in accordance with the established process. Non-Company devices, including devices used by Third Parties for work purposes, shall connect only through the secure Wi-Fi network provided by the Company.

- 4) Third Parties accessing the Company's network or network devices shall be authenticated using a secure authentication mechanism. Where required by the Company, Multi-Factor Authentication (MFA) shall be applied.

3.8.5 Access to Source Code

- 1) Access to the Company's source code shall be restricted to authorized personnel who have been assigned and have a legitimate need to access such source code based on their duties. Access rights shall be assigned in accordance with the Least Privilege Principle and shall be subject to oversight by the designated responsible party.
- 2) Access rights to the Company's source code shall be reviewed regularly, at least annually, or whenever there is a change in the user's roles or responsibilities.
- 3) Access to or modification of source code shall be performed only through channels, tools, and processes approved by the Company. Activities and change history shall be logged and traceable for audit purposes.
- 4) Third Parties shall implement measures to prevent source code from being leaked, lost, modified without authorization, or used beyond the specified purpose. The Company shall be notified immediately upon becoming aware of, or suspecting, any abnormal event involving the Company's source code.
- 5) Upon contract termination, service termination, or upon request by the Company, the Third Party shall terminate access rights and return or delete the source code and all copies thereof in accordance with the method specified by the Company. Evidence confirming completion of such actions shall be provided upon request.
- 6) Where it is necessary for a Third Party to access or receive the Company's source code, prior written approval from the Company shall be obtained, and appropriate security agreements and a Non-Disclosure Agreement (NDA) shall be in place before such access or disclosure is permitted.

3.9 Endpoint Security Management

Objective: To ensure that endpoints connected to the Company's information systems are appropriately protected, controlled, and managed in order to reduce risks arising from malware, unauthorized access, data leakage, and cyber security threats that may originate from endpoint devices.

3.9.1 Clear Desk and Clear Screen

- 1) Third Parties shall not leave workstations, terminals, or devices used for work purposes unattended without appropriate controls, and shall lock the screen or log out when such devices are not in use.
- 2) Password-protected screen savers shall be configured to activate after a specified period of inactivity to prevent unauthorized access.

- 3) Sensitive information media, whether in paper or electronic form, shall not be left unattended on desks, in meeting rooms, or in unlocked cabinets without appropriate controls.

3.9.2 Protection Against Malicious Software

- 1) Third Parties shall implement appropriate measures to prevent, detect, and/or remediate threats from viruses and malicious software on computer systems used in providing services to the Company.
- 2) Computer devices connected to the Company's computer systems or networks shall have anti-virus and anti-malware software approved by the Company installed, enabled, and kept up to date at all times. Regular malware scanning shall also be scheduled. Where required by the Company, additional security tools, such as Endpoint Detection and Response (EDR), may also be required.

3.9.3 Software Licensing

- 1) Third Parties shall use only lawful licensed software that is relevant to the performance of work for the Company.
- 2) Third Parties shall not install or use hacking tools or other software used for information or system assessment, security testing, vulnerability assessment, or penetration testing, unless prior written approval has been obtained from the Company

3.9.4 Mobile Computing and Teleworking

- 1) Third Parties shall implement appropriate controls for portable computing devices, mobile communication devices, and authorized personal devices used for work purposes or connected to the Company's systems or networks. Such devices shall use lawful software, be kept up to date, and be protected by appropriate security software, such as anti-malware or endpoint protection.
- 2) Third Parties shall ensure that the storage, use, transmission, or backup of the Company's information on portable computing devices and mobile communication devices complies with the Company's requirements on information classification, data governance, and data protection.
- 3) Devices used to connect to the Company's systems or networks shall be subject to appropriate access controls and shall have measures to prevent unauthorized access, such as authentication, security configuration, and network connection controls as specified by the Company.
- 4) Where Third Party-managed devices, systems, or environments are used to access or support the Company's high-criticality or high-impact systems, Third Parties shall ensure that such devices, systems, or environments are appropriately segregated from other systems and protected by suitable environmental, access, and connectivity controls to reduce security risks to the Company's systems and information.

- 5) Teleworking or remote access to the Company's systems shall be conducted only through channels authorized by the Company, with appropriate encryption and security controls applied in accordance with the Company's requirements.
- 6) Third Parties performing teleworking shall strictly comply with the Company's policies, standards, security procedures, Software License Agreements, and requirements relating to data storage or backup.

3.10 Change Management

Objective: To ensure that changes to computer systems, applications, network systems, and cloud systems are appropriately controlled in order to prevent impacts on the security and service continuity of the organization.

- 1) Third Parties shall establish an appropriate Change Management process for changes to computer systems, applications, network systems, and cloud systems, particularly those in the Production Environment. The process shall cover, at a minimum, the following:
 - assessment of risks associated with the change;
 - assessment of security impacts;
 - Vulnerability Assessment;
 - Penetration Testing for web applications, Application Programming Interfaces (APIs), or other systems with risks as specified by the Company;
 - approval of the change by an authorized person prior to implementation; and
 - preparation of a Rollback Plan in the event of errors or failures.
- 2) Any change to systems in the Production Environment shall be subject to security impact assessment and, as appropriate, Vulnerability Assessment or additional review. The results of such activities shall be documented in writing.
- 3) Third Parties shall provide prior notification of any change that may affect the Company's systems, services, or related security.
- 4) A Major Change shall be subject to Vulnerability Assessment and Penetration Testing, as appropriate to the type of system, and a contingency plan or Rollback Plan shall be prepared prior to implementation.
- 5) Where the Company is responsible for system administration, Third Parties shall comply with the Company's Change Management Process.

3.11 Application Security Management

Objective: To ensure that the development, testing, and use of applications comply with cyber security standards and reduce risks arising from vulnerabilities and unauthorized access.

3.11.1 Application Security Requirements

- 1) The design of applications or computer systems shall consider cyber security as a fundamental requirement, including protection against known vulnerabilities and the implementation of controls based on internationally recognized standards.
- 2) Security requirements shall be defined for all types of applications, covering authentication, data encryption, and Role-Based Access Control (RBAC).
- 3) Access to source code, development tools, and software libraries shall be appropriately controlled to prevent accidental or malicious changes and to protect the Company's intellectual property.
- 4) Source code shall be stored only in version control systems approved by the Company or systems that have undergone security assessment. Source code shall not be stored in any channels not authorized by the Company, including public repositories, public cloud storage, or any channels configured for public access.
- 5) Installation or update of software, program libraries, or application-related components shall be performed only by authorized personnel and shall be subject to the Change Management process specified by the Company.

3.11.2 Secure Coding

- 1) Third Parties shall establish application development and Secure Coding standards, and shall develop applications in accordance with appropriate security standards.
- 2) System developers shall apply appropriate data encryption and shall conduct Code Review and security vulnerability testing before deploying systems or applications to the Production Environment.
- 3) Third Parties developing applications for the Company shall receive appropriate training or possess appropriate knowledge and understanding of Secure Coding to ensure that software is developed securely in accordance with relevant standards.

3.11.3 Separation of Development, Test, and Production Environments

- 1) Third Parties shall ensure clear separation of Development, Test, and Production Environments, with appropriate Physical Access Control and/or Logical Access Control to reduce the risk of accidental changes or unauthorized access to data and applications.
- 2) Application functionality shall be tested in the Test Environment before deployment to the Production Environment to reduce the risk of accidental changes.
- 3) Access to sensitive information in Development and Test Environments shall be controlled to prevent data leakage.

3.11.4 Automatic Session Timeout

Automatic session timeout shall be configured to force users to log out automatically when the specified time is reached or when users remain inactive for the defined period. For systems connected to or providing services involving the Company's sensitive information and customers' personal data, the timeout period shall not exceed 10 minutes. For other systems, the timeout period shall not exceed 15 minutes.

3.11.5 API and Third-Party Component Security

- 1) APIs, libraries, and third-party components in use shall be subject to security review. Their versions shall be appropriately monitored and updated to prevent vulnerabilities that may affect system security.
- 2) Access to APIs shall be appropriately controlled, and data transmitted through APIs shall be encrypted in accordance with recognized security standards or practices.

3.12 Data Security Management

Objective: To protect information by maintaining its confidentiality, integrity, and availability, and to reduce risks arising from data leakage, loss, or unauthorized access that may affect the Company's business operations and reputation.

3.12.1 Data Classification and Handling

- 1) Third Parties shall classify and handle information appropriately based on its level of importance or sensitivity throughout the Data Lifecycle, from creation, use, transfer, and storage to destruction.
- 2) Appropriate controls shall be implemented for access to, use of, and disclosure of personal data in accordance with applicable laws. Such controls may include Data Masking, access restriction based on the Need-to-Know Basis, and logging of access to or use of such data.
- 3) Any transfer or disclosure of the Company's information to external parties or subcontractors shall be approved by the Company, and appropriate data protection measures shall be applied throughout the transmission and storage process.
- 4) Handling of the Company's information in electronic format shall comply with the following requirements:
 - a. The transfer or exchange of the Company's information shall be conducted through channels specified by the Company. For Highly Confidential information, appropriate protective measures shall be applied, such as applying password protection to attachments before transmission and sending the password through a separate channel from the transmitted document.

- b. Photographing, copying, or recording the Company's information without authorization is prohibited, particularly where such information includes customers' personal data, sensitive information, or the Company's internal information.
 - c. The Company's information shall not be published or posted on social media or any other public media without authorization from the Company.
 - d. Deletion or destruction of the Company's sensitive information shall be approved by the Company before implementation, and evidence of such deletion or destruction shall be provided upon request by the Company.
- 5) Handling of the Company's information in publishing format shall comply with the following requirements:
 - a. Printing, copying, or storing confidential information, the Company's sensitive information, or customers' personal data in printed format is prohibited, unless authorized by the Company.
 - b. Destruction of documents containing confidential information, the Company's sensitive information, or personal data shall be approved prior to destruction and shall be performed using appropriate methods in accordance with internationally recognized standards to ensure that the information cannot be recovered, read, or reconstructed.

3.12.2 Data Encryption

- 1) Third Parties shall implement appropriate Cryptographic Key Management controls covering the entire key lifecycle, including key generation, storage, distribution, rotation, revocation, and destruction, in accordance with applicable standards and industry best practices.
- 2) Third Parties shall define and implement data encryption standards that utilize appropriate and secure cryptographic mechanisms to protect data at rest and data in transit from unauthorized access, disclosure, modification, or destruction.
- 3) Cryptographic Keys shall be appropriately protected, and access to such keys shall be restricted to authorized personnel on a need-to-know basis and as required for the performance of assigned duties.
- 4) Sensitive Information, customer Personal Data, and the Company's internal information shall be encrypted or protected by appropriate security measures when stored or transmitted over public networks.

3.12.3 Data at Rest

- 1) Third Parties shall establish data encryption standards for Data at Rest that are appropriate to the classification, criticality, and sensitivity of the information being protected.
- 2) Third Parties shall implement processes for the regular review, control, and revocation of data access rights in accordance with the Need-to-Know Principle and the Principle of Least Privilege.

- 3) Devices, systems, and storage media used for storing or processing the Company's information shall be appropriately protected through both physical and logical security controls, accessible only to authorized personnel, and maintained in secure locations.
- 4) The Company requires Sensitive Information, particularly Personal Data, to be encrypted in accordance with the following minimum standards:
 - a. Symmetric Encryption
 - AES-256 or higher
 - b. Asymmetric Encryption
 - RSA-2048 or higher, particularly for PCI DSS in-scope systems and Digital ID systems
 - ECC-256 or higher
 - DSA-2048 or higher
 - Diffie-Hellman 2048-bit or higher

In addition, the following categories of highly sensitive information requiring enhanced protection shall be protected using field-level encryption:

- 1) National Identification Card Numbers or Passport Numbers, including Laser ID, Chip ID, and Department of Provincial Administration Card Application Numbers (BP1 No.).
- 2) Credit Card or Debit Card Numbers.

3.12.4 Data in Transit

- 1) Third Parties shall implement appropriate security controls for data transmission to maintain the confidentiality and integrity of information during transmission.
- 2) Transmission of the Company's information across networks shall be encrypted in accordance with the following requirements:
 - a. VPN Connections:
 - VPN concentrators shall be configured to support TLS 1.2 or higher.
 - Connections using SSL 3.0 or earlier versions shall not be permitted.
 - b. HTTPS Connections:
 - HTTPS services shall be configured to use TLS 1.2 or higher.
 - Connections using SSL 3.0 or earlier versions shall not be permitted.
 - c. Other Secure Connections:
 - Secure communication protocols with encryption capabilities, such as SFTP, SSH, or other protocols providing an equivalent level of security, shall be used.
 - d. SSH Access:
 - Direct SSH access using the default privileged operating system account (Root User) shall not be permitted.

- 3) Sensitive Information, confidential information, and Personal Data transmitted over public networks shall be encrypted or otherwise protected by appropriate security measures throughout the entire transmission process.

3.12.5 Data Backup and Restoration

- 1) Third Parties shall establish data backup and recovery arrangements appropriate to the criticality of the information and services provided, including appropriate physical and logical security controls for backup systems.
- 2) Backup systems and backup media shall be stored in secure locations or environments and protected against unauthorized access, disclosure, modification, or destruction to ensure that information can be fully restored when required.
- 3) Third Parties shall perform data backups and recovery testing on a regular basis according to the criticality of the systems and information to ensure the completeness and recoverability of backup data.
- 4) Data shall be backed up regularly, and backup data shall be protected with security controls equivalent to those applied to the original data. Protection against ransomware attacks shall also be considered, including the implementation of measures such as Immutable Backups, Offline Backups, or network isolation, as appropriate.
- 5) Recovery testing for critical information shall be conducted at least annually, and the test results shall be documented and retained in writing to verify that information can be restored within the agreed Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified in the applicable agreement or service contract.

3.12.6 Information Disposal

- 1) Third Parties shall retain the Company's information in accordance with the applicable Retention Period. Upon expiration of the retention period specified in the table below, information shall be securely deleted or destroyed in accordance with recognized industry standards and in compliance with the intended purpose of retention, applicable legal requirements, and the Company's information retention requirements.

No.	Category	Retention Period	Lawful Basis / Company Information Management Requirement
1	Company Sensitive Information, project-related information, and Personal Data	Retained throughout the service period under the applicable service agreement	Service Agreement / Contractual Obligation

No.	Category	Retention Period	Lawful Basis / Company Information Management Requirement
2	Log files	90 days from the date the data is entered into a computer system	Section 26 of the Computer Crime Act

- 2) Upon termination or expiration of the service agreement, Third Parties shall return all Company information, including project-related information jointly developed or maintained for the Company. Following the completion of the data transfer, all remaining information, including copies and backups retained by the Third Party, shall be securely deleted or destroyed within 7 business days, unless retention of Personal Data is required by applicable law.
- 3) Prior to the deletion or destruction of confidential information, including the Company's customer Personal Data, Third Parties shall notify the Company's designated project representative and obtain the Company's approval. Third Parties shall maintain a Deletion Record or Certificate of Destruction and retain supporting evidence of the deletion or destruction process. Such evidence shall be provided to the Company upon request.

3.12.7 Test Information

The use of the Company's Sensitive Information, Personal Data, or confidential information for system development and testing purposes is strictly prohibited. Third Parties shall use only Test Data specifically created for such purposes.

3.13 Infrastructure Security Management

Objective: To ensure that the Company's information technology infrastructure, including cloud environments, network infrastructure, and monitoring systems, is appropriately protected, controlled, and managed to reduce cyber security risks and support secure business operations.

3.13.1 Cloud Security Management

- 1) Third Parties shall establish and maintain cyber security policies, standards, or guidelines aligned with recognized industry standards and covering cloud services used in providing services to the Company.
- 2) Cloud-based systems shall be continuously monitored, reviewed, and assessed to ensure that security configurations remain aligned with applicable security standards and the Company's acceptable risk level.
- 3) Appropriate controls shall be implemented to prevent cloud misconfigurations and the unauthorized exposure of cloud-based information or resources to the public.

- 4) Logging and monitoring capabilities shall be enabled for cloud systems used in providing services to the Company to support the detection, investigation, and forensic analysis of cyber security events.
- 5) Security roles and responsibilities between the Cloud Service Provider (CSP) and the Third Party shall be clearly defined and documented in accordance with the Shared Responsibility Model.

3.13.2 Network Security Management

- 1) Third Parties shall establish and implement appropriate network security controls for networks connected to the Company's network infrastructure.
- 2) Network segmentation shall be implemented based on the criticality of systems and information to reduce the risk of unauthorized access and the spread of cyber security threats.
- 3) Network traffic shall be controlled and filtered through appropriate security devices or technologies, such as firewalls or other equivalent security controls.
- 4) Network security events shall be appropriately monitored, logged, and reviewed to support security event detection, investigation, and forensic analysis.
- 5) Network connections to the Company shall be reviewed on a regular basis, and unnecessary or unused connections shall be removed or terminated.
- 6) Where wireless networks are used, appropriate authentication and encryption mechanisms shall be implemented. Obsolete security standards, insecure protocols, or weak security configurations shall not be used.

3.13.3 Logging and Monitoring

3.13.3.1 Managing Log Information

- 1) Third Parties shall maintain Audit Logs and Activity Logs for significant system events, including activities performed by users and administrators associated with systems or services provided to the Company. Access rights to log information shall be clearly defined and appropriately controlled.
- 2) Logs shall capture events necessary to support audit trails, forensic investigations, and cyber security incident analysis, including but not limited to privileged activities, system or information access, failed login attempts, authentication activities, user account modifications, and the initiation, termination, or modification of logging functions.
- 3) Log retention periods shall be established in accordance with applicable laws, contractual obligations, and other relevant requirements. Logs required for investigation, monitoring, or digital forensic purposes shall be retained for at least 90 days, or longer if required by the Company or applicable law.
- 4) Appropriate controls shall be implemented to protect log information and logging systems against unauthorized modification, tampering, deletion, or access. Access to log information shall be restricted to authorized personnel on a need-to-know basis.

- 5) Logs generated by critical systems, devices, or services shall be stored in secure locations or systems with appropriate security controls. Third Parties shall ensure that log information remains available and accessible for investigation and audit purposes when required.
- 6) Where log information is transmitted across untrusted networks, log transmission channels shall be encrypted or protected using secure communication protocols to prevent unauthorized access to or modification of log information during transmission.
- 7) Where systems or services are subject to specific requirements, such as PCI DSS or other regulatory obligations, Third Parties shall retain and protect log information in accordance with those requirements.

3.13.3.2 Monitoring System Use

- 1) Third Parties shall identify systems, events, and activities that require cyber security monitoring based on the associated risk level, system criticality, and the potential impact on the Company's information, systems, or services.
- 2) Log information from critical systems shall be collected, analyzed, and monitored appropriately to support the detection of abnormal activities, system malfunctions, or security events that may affect the security of the Company's systems or information.
- 3) Where system failures, abnormal activities, or security events are identified, Third Parties shall perform appropriate root cause analysis and implement corrective actions or control improvements to reduce the likelihood of recurrence.
- 4) Alerting mechanisms shall be established to detect abnormal activities or events, including unauthorized access attempts, unusual privileged activities, repeated failed login attempts, or other events that may indicate cyber security threats.
- 5) Services provided to the Company and associated log information shall be regularly monitored and reviewed to ensure that logging and monitoring controls remain effective and sufficient to support the detection, analysis, and response to cyber security incidents.
- 6) Third Parties shall monitor and assess the adequacy of log storage capacity and shall implement alerting mechanisms when log storage resources or related systems are at risk of affecting availability or operational effectiveness.
- 7) For critical systems or systems supporting services provided to the Company, Third Parties shall implement Security Information and Event Management (SIEM) capabilities or other appropriate monitoring solutions to support centralized security event monitoring, analysis, and detection.

3.13.3.3 System Time Synchronization

- 1) Third Parties shall ensure that computer systems, network devices, and systems supporting services provided to the Company are synchronized with a common and reliable time source, such as Coordinated Universal Time (UTC) or another trusted time

source, to ensure the accuracy, integrity, and reliability of log information for audit and investigation purposes.

- 2) System time synchronization shall be periodically reviewed, and any detected time deviations shall be corrected in a timely manner to ensure that log information can be reliably used for event analysis, investigation, and cyber security incident response activities.

3.13.3.4 Intrusion Detection and Investigation

- 1) Third Parties shall establish criteria and procedures for reviewing and analyzing log information to identify attempts or events that may indicate a cyber security breach, taking into consideration threat intelligence, known vulnerabilities, and attack patterns obtained from reliable sources.
- 2) Upon detecting intrusion attempts, suspicious activities, or cyber security incidents, Third Parties shall promptly implement appropriate containment, remediation, and mitigation measures and notify the Company in accordance with the established incident management process.
- 3) Log information required for investigations, event analysis, and digital forensic evidence shall be retained for at least 90 days, or longer if required by applicable laws, contractual obligations, or the Company's requirements.
- 4) High-risk events shall be continuously monitored and investigated, including the correlation of events across multiple systems, to enhance the effectiveness of threat detection and incident response activities.

3.13.4 System Management

- 1) Third Parties shall establish, maintain, and periodically review operational procedures related to systems or services provided to the Company. Such procedures shall appropriately cover data processing and handling activities, error management processes, and support channels or responsible parties for operational support and issue resolution.
- 2) Third Parties shall monitor and assess the capacity and performance of systems, resources, and services related to the provision of services to the Company to ensure continued operational effectiveness and service availability.
- 3) Third Parties shall establish capacity planning processes to accommodate increases in workload, resource utilization, or changes that may affect system performance, availability, or service continuity.
- 4) Where system resources are identified as insufficient or at risk of impacting services provided to the Company, appropriate corrective actions or mitigation plans shall be implemented.
- 5) Systems supporting services provided to the Company shall be configured with session timeout or automatic logout mechanisms after a defined period of inactivity. Systems that

process, access, or provide Sensitive Information or customer Personal Data shall enforce a session timeout period of no more than 10 minutes. For all other systems, the session timeout period shall not exceed 15 minutes, unless otherwise specified by the Company.

3.14 Artificial Intelligence Security Management

Objective: To ensure that the development, deployment, and use of Artificial Intelligence (AI) systems associated with services provided to the Company are appropriately governed and controlled with respect to cyber security, privacy, and compliance with applicable laws and policies. This includes both internally hosted AI systems (On-Premises/Private) and externally provided AI services (SaaS, PaaS, IaaS, and Model-as-a-Service).

- 1) Third Parties shall implement appropriate cyber security and privacy controls for AI systems, including access control, abnormal behavior detection, AI resilience testing, and the retention of information necessary to support auditability and traceability, such as model versioning, model weights, training datasets, and related configuration parameters.
- 2) The use of the Company's information for training, testing, or operating AI systems shall comply with the Company's requirements for information classification, data governance, encryption, access control, and Personal Data protection.
- 3) Sensitive Information, confidential information, or Personal Data belonging to the Company shall not be used with external AI services unless expressly authorized by the Company and protected through appropriate safeguards, such as Data Masking, De-identification, or equivalent protective measures.
- 4) Security patches, libraries, frameworks, and AI-related components shall be regularly updated to mitigate risks arising from threats such as Model Theft, Model Inversion, Data Poisoning, and Adversarial Inputs.
- 5) The use of external AI services or AI tools that process, access, or support the Company's information, systems, or services shall be subject to assessment and approval in accordance with the Company's established processes. The use of unauthorized AI tools or services (Shadow AI) is prohibited.
- 6) AI-generated outputs that may impact the Company's business operations, customers, legal obligations, or contractual commitments shall be subject to Human Validation prior to use.
- 7) AI shall not be used to generate content that violates applicable laws, intellectual property rights, the rights of other individuals, or the Company's ethical standards.
- 8) In the event of a cyber security incident, Personal Data incident, or legal or regulatory violation related to the use of AI systems, Third Parties shall report, investigate, and manage the incident in accordance with the established incident management process and promptly notify the Company.

3.15 Awareness, Education and Training

Objective: To enhance the cyber security awareness of personnel of Third Parties involved in providing services to the Company, enabling them to recognize, prevent, and appropriately respond to evolving cyber security threats in a timely manner.

- 1) Third Parties shall provide ongoing education, training, and awareness programs covering cyber security, Personal Data protection, and the Company's relevant policies, standards, and requirements. The training content shall be appropriate to the roles and responsibilities of personnel involved in providing services to the Company.
- 2) Third Parties shall regularly update training materials and awareness communications to address emerging threats, security controls, regulatory requirements, and other relevant developments to ensure personnel remain capable of effectively managing new and evolving risks.
- 3) Third Parties shall conduct training effectiveness assessments or knowledge evaluations, as appropriate, and retain evidence of training completion and assessment results for audit and verification purposes upon the Company's request.
- 4) Personnel of Third Parties who are granted access to the Company's information, systems, or information assets shall receive training on, or acknowledge, the Company's cyber security and Personal Data protection requirements prior to, or within an appropriate period after, commencing their duties.
- 5) Third Parties shall periodically review and update their training programs and awareness activities to ensure alignment with changes in cyber security threats, technologies, legal requirements, and other applicable obligations.

3.16 Cyber Security Incident Management

Objective: To ensure that cyber security incidents are managed effectively in accordance with applicable legal requirements and recognized industry standards.

- 1) Third Parties shall establish a Cyber Security Incident Management process to support the effective handling of cyber security incidents. Documented procedures shall be maintained and shall cover incident classification, severity rating, incident reporting structures, and communication procedures with relevant stakeholders. Such procedures shall be communicated to personnel and relevant third parties as appropriate.
- 2) Third Parties shall establish a Cyber Security Incident Response Plan appropriate to the associated risks and ensure that relevant personnel receive appropriate communication, training, or simulation exercises to prepare for cyber security incidents.

- 3) Third Parties shall maintain appropriate tools, techniques, and processes to support system investigations, attack detection, and the identification of unauthorized activities within computer systems.
- 4) Third Parties shall review the Cyber Security Incident Response Plan at least annually from the date of approval, or whenever a significant change occurs.
- 5) Third Parties shall designate at least one (1) cyber security contact responsible for coordinating and reporting cyber security incidents to the Company. The designated contact shall also coordinate with the Company's personnel when the Company identifies a cyber security incident related to the Third Party.
- 6) In the event of a cyber security breach or incident affecting the Company, the Third Party shall notify the Company without undue delay and no later than 12 hours after becoming aware of the incident. The notification shall include all available information at the time of reporting. The Third Party shall provide periodic updates as additional information becomes available and shall submit a complete incident report to the Company as soon as practicable.
- 7) Following the resolution of a cyber security incident, the Third Party shall conduct a root cause analysis, document lessons learned, and implement appropriate improvements to controls, processes, or procedures to reduce the likelihood of recurrence.

3.17 Business Continuity Management

Objective: To prevent and minimize the impact of severe information system failures, emergencies, or disasters on the Company's critical business processes, and to ensure that business operations can continue or be restored within an appropriate timeframe.

- 1) Third Parties shall establish and maintain a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) covering services, connectivity, and access to information related to the services provided to the Company to ensure the continuity of operations and service delivery.
- 2) The Business Continuity Plan and Disaster Recovery Plan should consider risks that may result in disruptions to services, connectivity, or access to information provided by Third Parties, including the impact on service delivery, availability of information and critical resources, communication between the Third Party and the Company, and the timely reporting of incidents or abnormal situations to the Company.
- 3) Third Parties shall test, review, and update the Business Continuity Plan and Disaster Recovery Plan covering services, connectivity, and access to information related to the Company at least annually, or whenever a significant change occurs
- 4) Third Parties shall support or participate in the Company's Business Continuity Plan testing activities as required by the Company.