# Cyber Security Policy

# AIS Group

## 1. Introduction

### 1.1 Objectives

1) Determine the direction, principles, and frameworks of the requirements for cyber security management.
2) Develop a better understanding for employees to work in compliance with the policies, standards, frameworks, procedure, guidelines, and laws related to the Computer Systems correctly and appropriately.
3) For Employees and those who need to use or connect to the Company's Computer System, to be able to use the Company's Computer Systems properly.
4) Prevent the Company's Computer Systems and Information Technology from intrusion, theft, destruction, disruption, or any other criminal activities that may damage the business of the Company.

### 1.2 Scope

This policy covers protecting and maintaining of the Company's cyber security either on the premises or off the premises, including the cloud that the Company supplies which covers:

1) All Employees and departments of the Company.
2) External Parties have access to the assets related to the Company's Computer System and Information Technology.

### 1.3 Security Principles

This Security policy has an objective to achieve the following principles:

- **Confidentiality** – Protecting the confidentiality of information, including personal information or information under the Company's ownership by preventing access and disclosure of information from an unauthorized person.
- **Integrity** – Ensuring that the Company's information shall not be edited, modified, or destroyed by an unauthorized person.
- **Availability** – Ensuring that authorized users can access information and services quickly and reliably.
- **Accountability** – Specification of an individual's responsibilities, including liability and responsibility of the result made.
- **Authentication** – Ensuring the access right shall go through a complete identity verification process.
- **Authorization** – Ensuring to give the right to access Computer System and Information Technology based on the least privilege and following the need to know basis.

- **Non-repudiation** – Ensuring that parties involved in the transaction cannot deny that there is no connection to the transaction made.

Adequate Security shall have an agreement and get attention in all matters involved. Which includes:

- Security is the duty of all Employees.
- Management and practice in Security is a process that must be done continuously at all times.
- Conscience, self-discipline, responsible, and pay attention to work in compliance with the practices specified in the standard policies, standards, frameworks, procedures, guidelines, and processes are the most crucial part of Security. A clear explanation to Employees to develop a better understanding of the roles and responsibilities of the Security that they are responsible ensures the Security operation is running effectively.

**1.4 Definitions**

1) **"Company"** refers to Advanced Info Service Public Company Limited and any other subsidiary companies in the AIS group.
2) **"Employee"** refers to an employee who is employed as a trainee, permanent staff, special contract employee and executives of any level employed by the company.
3) **"User"** refers to the employees, including External Parties, which on the list of authorized users that are allowed to have an access password or/and have a password to access the processing equipment.
4) **"Supervisors"** refers to an Employee who is supervisors of internal departments according to the organization structure of the Company.
5) **"Computer System"** refers to all kinds of computer tools or equipments including hardware and software of all sizes, wired and wireless network equipments, data storage and transfer equipment, internet and intranet systems, as well as electrical equipment and various telecommunications that can work or can be used in the same way or similar to a computer. The system including the ones belongs to the Company, Company's partner, other companies that are under installation and not yet delivered or the ones that the Company's Employee is taking to install or for using within the Company premises.
6) **"Information Technology (IT)"** refers to information, news, records, history, document content, computer program, computer data in images, sounds, marks, and symbols, whether stored in a format that can convey meaning to a person directly or through tools or any equipments.
7) **"Sensitive Information"** refers to Information Technology which is important to the Company's business operation or which the Company has obligations under the laws, business ethics, or contracts neither to disclose such information to other person nor to use such information for any benefits other than the Company's business objective. Any leakages of such information may cause interruption or less efficiency to the Company's business operation or disgrace to the Company's reputation.
8) **"Important Systems"** refers to a Computer System that the Company uses to provide business services that generate direct revenue, and the systems that support income generation including any other electronic systems that help the business operating normally and systems that have

been defined by the information Security agency and Company's information systems. However, if such vital systems stop working or lack of efficiency, it may cause the business operation to a halt or ineffective.

9) **" Remote Access"** refers to a connection to access the computer or the Company's network system (via internal communication channels) or from outside the Company (via the Internet)

10) **"System Owner"** refers to internal departments that own Computer Systems and are responsible for that Computer System.

11) **" Custodian"** refers to a person assigned by the owner of the Computer System or Information Technology to support the work and control of the access to the Information Technology to comply with the requirements or the level of authorization that the Computer System or Information Technology owner determines.

12) **" Administrator"** refers to an employee assigned to responsible for using and maintaining the Computer Systems, including hardware, software, and any other peripherals that are assembled into a Computer System. The administrator is authorized to change, add, edit, and adjust the Company's Computer System to operate appropriately with efficiency in line with business needs and safety.

13) **"Security"** refers to any processes or actions such as prevention, sternness, precaution, care in use and maintenance of Computer Systems/ITs and Sensitive Information to prevent any attempts of either in-house Employee or outsider from accessing with intention to steal, destroy, and disrupt such system which may cause damages to the Company's business.

14) **" External Party"** refers to personnel or external agencies that conduct business or provide services that may grant access to IT and the Company's information processing equipment such as:

- Business Partner
- Outsource
- Supplier
- Service Provider
- Consultant

**1.5 Consequence for Non-Compliance**

Refer to the employee manual for work regulations Advanced Info Service Public Company Limited and AIS Group Discipline, penalties and suspension

## 2. Roles and Responsibilities

### 2.1 Supervisor's role

1) Inform Employees about the policies, standard, framework, procedure, work instruction, guideline, and processes of the Company related to cyber security.
2) Look after, advice and warn in case of is any improper or inappropriate behavior.
3) Consider penalty for offenders equally and fairly.

### 2.2 Employee's role

**2.2.1 All Employees** must comply with the following:

1) Learn, understand, and follow the policies, standard, framework, procedure, work instruction, guideline, and processes of the Company related to cyber security strictly.
2) Fully cooperate with the Company to protect the Computer System and Information Technology
3) Inform the Company immediately when seeing improper or inappropriate behavior or intrusion, theft, destruction, disruptive of work, or other criminal activities that may cause damages to the Company.

**2.2.3 Employees with duties related to External Parties** must guide the External Parties to work in compliance with the cyber security policy.

## 3. Cyber Security Risk Management

**Objective**: To demonstrate acceptance and reduce the risk of cyber security which uses a consistent approach to risk management including Security measures to protect information that is consistent with the risk identification and assessment process.

**Description**

3.1 Security Risk Management Methodology

3.2 Internal Organization

3.3 Risk Management with External Parties

## 4. System Management

Objective: To have appropriate measures to protect Company assets

**Description**

4.1 Inventory and Ownership

4.2 Security Classification and Handling

4.3 Software Licensing

## 5. Human Resource Management

**Objective**: To Employees and External Parties who contract with the Company understand their responsibilities including awareness of Security in the operations.

**Description**

5.1 Prior to Employment

5.2 During Employment

5.3 Termination and Change of Employment

## 6. Physical and Equipment Security

**Objective**: To prevent unauthorized physical and equipment accesses which may cause damage and interference in the Company's Computer System.

**Description**

6.1 Physical Security

6.2 Equipment Security

## 7. Communications and Operation Management

**Objective:**

1. Ensure secure operation on the Computer System.
2. Implement and maintain the appropriate level of cyber security and service delivery.
3. Reduce the risk of Computer System failures.
4. Protect and maintain the integrity and availability of information, software, and Computer Systems.
5. Ensure the protection of data in the networks, including protection of other support infrastructure.
6. Prevent unauthorized disclosure, editing, deletion or destruction of assets as well as business activities interruption.
7. Maintain data security which exchanged within the Company and External Parties.
8. Monitor unauthorized data processing.

**Description**

7.1 Operational Procedure and Responsibilities

7.2 External Party Service Delivery Management

7.3 Capacity Management

7.4 Protection Against Malicious Software

7.5 Back Up and Restoration

7.6 Network Security Management

7.7 Removable Media Handling

7.8 Cloud Storage

7.9 Information Transfer

7.10 Monitoring

7.11 Patch Management

## 8. Access Control Management

**Objective**: To control access to information and Computer System that only those who are authorized and prevent unauthorized access to the system and services.

**Description**

8.1 User Access Management

8.2 Password Management

8.3 Access Control

8.4 Mobile Computing and Teleworking

## 9. System Acquisition, Development, and Maintenance

**Objective:** To provide Security as an essential component of procurement, development and maintenance of the system.

**Description**

9.1 Security Requirements for Systems

9.2 Correct Processing in Applications

9.3 Cryptographic Controls

9.4 Security of System Files

9.5 Security in Development and Support Processes

9.6 Vulnerability Management

## 10. Cyber Security Incident Management

**Objective:** To reduce the risk and damage that may occur and ensure that cyber security incident, including weaknesses related to the system, has been communicated and being able to take proper actions in time.

**Description**

10.1 Management of Cyber Security Incident

## 11. Business Continuity Management

**Objective:** To protect essential business processes from the impact of significant failures in Computer Systems or from disasters.

**Description**

11.1 Cyber Security in Business Continuity Management

## 12. Regulatory and Compliance

**Objective:** To avoid violations of legal obligations, regulations, or employment contract relating to security, Computer Crime Act., Cyber Security Act., Electronic Transaction Act., Personal Data Privacy Act. including other relevant laws and regulations that are already in effect or shall be in effect in the future.

**Description**

12.1 Compliance with Legal Requirement

12.2 System Audit Considerations

**Effective Date**: 1 November 2019