Information Security Policy

AIS Group

Information Security Policy

1. The Company will do everything in its power to enable the system of required business services such as computer system, mobile phone network system, and other telecommunication system to be continuously used, and the information is most reliable. Therefore, the Company gives the highest priority to secure such systems.
2. The Company has Obligations under the laws and promises to customer, partner, investor, and employee to maintain confidentiality of the information given to the Company by those parties including the personal information of individual or juristic person obtained from the computer process or the communication through the Company's network. Therefore, executives and employees must strictly follow the standard regulation, guidelines, and security procedures to prevent the disclosure of such information or any unauthorized access to such information.
3. The Company has set up the department which will be directly responsible to observe and secure the Computer and IT System according to this policy and to follow up and regularly investigate the operation of each department to ensure that the overall computer system and IT security meets the standard specified by the Company.

Objective

1. To create awareness and understanding for employees to correctly follow the policy including the laws relating to the computer system and IT security.
2. To enable employees and those who are required to use or connect to the Company's Computer System to access and appropriately use the Computer System and IT.
3. To prevent the Company's Computer System and IT from intrusion, theft, destruction, disruption of work, or any other criminal activities that may cause damages to the business operation of the Company.

Duties and responsibilities

1. **Duties of a managing office**

    1.1. To explain all policy, orders, and guidelines of the Company which are related to Computer System and IT security to the employee.

    1.2. To supervise, advice and give warnings when discovering any inappropriate behaviors.

    1.3. To take an appropriate and fair disciplinary action to the violator.

2. **Duties of employee**

    2.1. To study, understand, and strictly follow all policy, orders, and guidelines of the Company regarding the Computer System and IT security.

    2.2. To fully cooperate with the Company to maintain the Computer System and IT security.

    2.3. To notify the Company immediately when discovering any inappropriate behaviors, intrusions, thefts, destructions, disruptive of work, or other criminal activities that may cause damages to the Company.

3. **Employee whose duties involve with a third party** must ensure that such third party shall comply with the Company's policy on Computer System and IT security at all times.

Definition

1. **"Company"** means Advance Info Service Public Company Limited and any other subsidiary companies in the AIS group.
2. **"Employee"** means an employee who is employed as a trainee, permanent staff, special contract employee and executives of any level employed by the company.
3. **"Computer System"** means all kinds of computer tools or equipments including hardware and software of any scales, wired or wireless network equipments, data storage, retention and transfer equipments, Internet system, Intranet system, including electrical and telecommunication equipments that work or can be used in the same or similar way as a computer whether they are the Computer's asset, the asset of the Company's partner, other Company's asset pending installation stage but not yet handed

over to the Company, or the Employee's asset which has been installed and used inside the Company's premises.

4. **"Information Technology (IT)"** means information, news, record, history, text in documents, computer program, computer information in picture, sound, sign and any symbols stored in a form which are interpretable either by an individual directly or by the means of any other tools or equipment.
5. **"Security"** means any processes or actions such as prevention, sternness, precaution, care in use and maintenance of Computer/IT Systems and Important Information to prevent any attempts of either in-house employee or outsider from accessing with intention to steal, destroy, disrupt such system which may cause damages to the Company's business.
6. **"Important Information"** or **"Confidential Information"** means 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.

Discipline and Punishment

1. A by-line supervisor must take responsibility to ensure that his/her subordinates comply with and refrain from any violation of the discipline. If there is ignorance or a violation of such discipline, the supervisor must appropriately punish the violator.
2. The Company reserves the right to monitor the use of the Computer System and Information Technology of all employees to ensure that the security or such information and system are appropriately maintained and the company may do so at any time.
3. The punishment need not be imposed sequentially. The Company may choose a level of punishment which is suitable for the severity of the offense.
4. This Information Security Policy for AIS group is part of a working procedure