Security Policy Information Technology (IT Security Policy)

The information technology system, network and computers of Prodigy Public Company Limited appropriately, securely and able to support the Company's operations continuously. The system is used in a manner that complies with the requirements of the Computer Crime Act and other relevant laws. As well as to prevent threats that may cause damage to the company, the company therefore sets the information technology security policy as follows:

Objective

To raise awareness of the security of the company's information system that focusing on regulated of operations to manage the information system with complete accuracy always ready to use. Adding disseminating knowledge and understanding to all employees levels within the company. Including creating awareness of the impact that will occur from the threat event or access to the Company's information for all employees levels to comply with the policies set by the Company strictly defined.

Scope

Covering all information system of the Company. Both in the head office and branches. Including the expansion of branches, subsidiaries, affiliates that may occur in the future.

Practical steps

1. Communicate through various channels within the company, so that employees at all levels are aware of the policy and comply their duties appropriately along with protecting the company's information. The employees must sign the agreement for keep the secrets of the company. And review of the user's understanding of the use of the Information system of the Company.
2. The IT department prepares user manuals for various systems as related to work to reduce risks to Information systems of the company.
3. The IT department must keep up with changes in information technology, to develop of the system to be able to effectively prevent and reduce risks from cyber threats and in accordance with the situation current.
4. The IT department has selected a cloud server service provider (Cloud Server) for email hosting (E-mail Hosting) and Web hosting reliable and have a plan to support risks from cyber threats and responsible for service recipients.
5. The IT department has a maintenance plan of the capabilities of IT equipment, both hardware and software annually.

6. The IT department provides Firewall and Antivirus systems as well as tools to protect against threats other. Which's be effective and always updated to protect important information in the Company's information system.
7. The IT department has created a backup Data of the company. There is a backup check and test continuous backup results.
8. Guidelines for selecting vendors and service providers set out in accordance with the TOR. The IT department must periodically review time of product warranty and duration of service by reviewing product and service warranty of sellers and service providers. According to the trade conditions or memorandum of trade agreements that have been specified.
9. IT staff should be trained and developed continuously. For development his/her capabilities regarding information technology and keep up with cyber threats including security technology constantly taking risks
10. All employees must comply with the principles of using E –mail and access to the Internet of the company properly.
11. Banned the employees at all levels are prohibited from using computer programs that are not related to the company's mission in computer of the company. By the IT staff must survey employees' computers on a regular basis.
1 2. If any employee does not comply with the policy which will be punished as if it was a disciplinary action Company.

Event response

Incident Response means the action taken when a threat to an information system arises. The response is IT departments must take action to contain threat attacks, restore systems and notify management as soon as possible. Along with determining methods for improving and developing the Company's information system to prevent and reduce risks that may occur again in the future.

IT departments must have a plan to solve problems from uncertain situations and disasters that may occur with information systems. According to the Company's crisis management plan educating methods for correct actions for users of the system and if there is a problem in the system. The IT department must be informed including in the event of a threat to the information system or other security incidents and must cooperate in Compliance with measures set by the IT department regularly. In addition, the administrators must pay attention to the system development plan clearly defined roles and responsibilities

Data retention

(1) It is the responsibility of the IT department to inquire about the purpose of using the data. To be used to create standards and requirements for data retention that will be used within the company.

(2) Classification of information including customer record documents Transactional data e-mail messages data manage for defragmentation. So that it can be used later conveniently

(3) Data retention should specify the types of data that a business must retain and storage period creating more storage space. In case storage space may be insufficient.

Building security of personnel information systems

Users must understand policies, duties and responsibilities in the use of the Company's information system

(1) To define duties and responsibilities with setting the practice about information system security for individuals or external agencies hired to work.

(2) Users and external agencies who are hired to work must be informed of the Company's information technology security policies.

(3) After changing or termination of employment or the end of the project. Access to information in the information system must be terminated immediately.

Specifying channels for whistleblowing

If you see any questions or get any information related to misconduct in the field of information systems, threats, phishing of related information can be reported to the IT Department who is the direct administrator of the company for inspection.

……..