(Translation)

Information Security Management Policy

Policy Objective

Bangkok Dusit Medical Services Public Company Limited (BDMS) and its subsidiaries have provided Information Technology and Computer Network Systems to facilitate company operations for their employees. In order to secure and protect the Information Technology and Computer Network Systems from any damage and problem as a result of cyber threats or misuses, BDMS has established an Information Security Management Policy to provide a guideline and standard procedure for employees and third parties whose duties are related to operations of the company.

This policy applies to everyone using information and information systems of the companies without exception.

The Information Security Management Policy provides important details as follows:

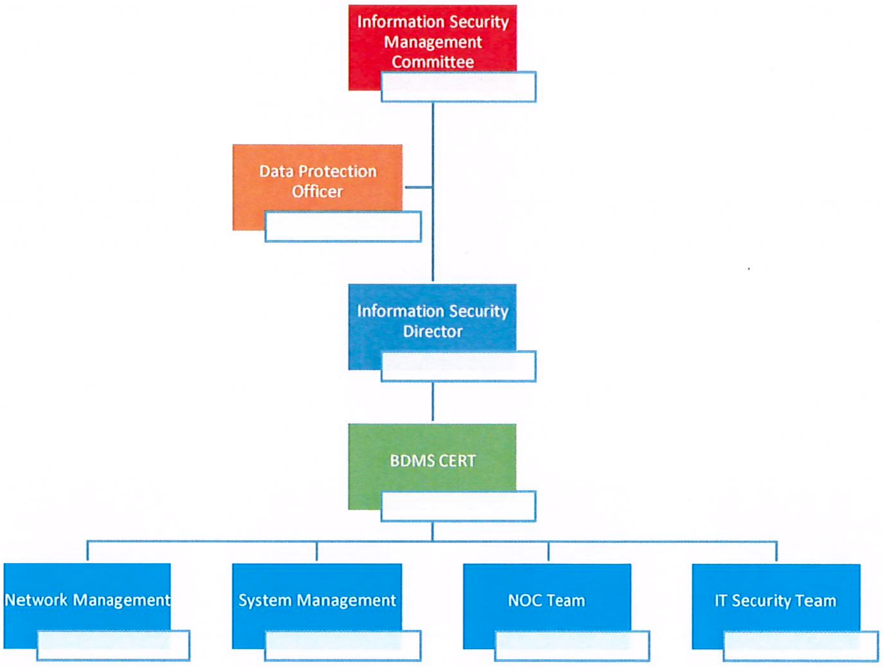
- General Definition
- Structure and Roles of Committee
- Practice Guidelines
- Practice, Audit and Discipline

General Definition: The definitions used in this Information Security Management Policy are

- "Company" means Bangkok Dusit Medical Services Public Company Limited (BDMS) and its subsidiaries holding more than 50% of shares.
- "Management" means persons with authority to direct the company business according to the structure of the company.
- "Information Security Management Committee" means a group of persons who officially assigned by President.
- "Employee" means staffs and employees as well as persons who are assigned to work under agreements or contracts of the company.
- "Information" means media representing a meaning, story, fact or information regardless of the formats of the media such as document, file, report, book, chart, map, picture, photo, film, video or voice record, a record using a computer or other means to display it.
- "Computer Network" means computers and other computing devices are connected to each other to share resources including Internet and Intranet system of the company.
- "Computer Network Administrator" means employees assigned by management to control and govern the computer network that have an authority to access the network to manage the computer network database.
- "User Account" means a username and password individually issued by the company for accessing and using the information technology resources.
- "Information Technology Resource" means the company's computer network including computer desktops, computer notebooks, servers, portable electronic devices, mobile phones and computer accessories approved to use within the

company which are and are not owned by the company as well as data and software that are stored and used.

Structure of Committee: The company provides roles and responsibilities of the Information Security Management through the organizational structure as follows:



- Information Security Management Committee (ISMC): consists of top management from BDMS and its subsidiaries having roles and responsibilities as the follows:
  - ➢ Approve and enforce policies or other procedures related to the Information Security Management Policy
  - ➢ Define and approve criteria for risks and acceptable risk levels
  - ➢ Review the result of the risk assessment and important risk mitigation plan of the organization
  - ➢ Consider a punishment for a person who commits a breach of the Information Security Management Policy
  - ➢ Support all necessary resources used in the information security operations

- Data Protection Officer: employees from Company or any persons, who are assigned to have roles and responsibilities as follows
  - ➢ Supervise and advise the work related to store and use the private data in the systems

- Inspect the files and the usage of private data in the systems and report risks, incidents or situations related to the information security as well as the solution to the Management and related persons
- Respond and cope with incident related to the information security occurred in the company
- Provide training programs and knowledge to the company's employees on the use and protection of the private data
- Monitor and report incidents related to the information security to all related persons in the company
- Coordinate with other departments on the data management for both inside and outside the company

- Information Security Director: a representative of management from Greenline Synergy Co., Ltd. has roles and responsibilities as the follows:
  - Provide advice and recommendation to the management for establishing policy and regulations related to the information security management
  - Supervise and advice works related to the operations of the information technology and computer network administrators to follow the regulations
  - Communicate with employees to have them recognize the importance of the information security
  - Provide knowledge to employees and related third party on the compliance with the Information Security Management Policy
  - Properly monitor the compliance of employees and related third party with the policy
  - Review and improve the policy in order to appropriately respond to the current situation
  - Coordinate and determine the management solution in case of a violation of the security of the organization's information
  - Provide a quarterly report of the operations to the Information Security Management Committee
  - Provide a progress report of incident or situation to the committee
  - Perform other duties assigned in this policy

- BDMS Computer Emergency Response Team (BDMS CERT): consists of staffs from Greenline Synergy Co., Ltd. or assigned persons having roles and responsibilities as follows:
  - Respond and cope with the incidents of the information security
  - Provide advices on and solutions for the cyber threats
  - Monitor and report incidents related to the information security to all related persons in the company

- Regularly study, improve and update tools and practices to increase the level of information security protection.
- Perform other duties related to the Information Security management as assigned by the Management

Practice Guidelines: All companies under this policy shall establish procedures and processes in accordance with the details provided below and submit for approval from Information Security Management Committee within 180 days after this policy is effective.

- Information Resource Usage Procedure
- Data Protection Procedure
- Cybersecurity Protection Procedure
- User Account Management Procedure
- Thirty-party Service Delivery Management Procedure
- Information Assets Management Procedure
- Information Security Operation Management Procedure
- Information Security Incident Management Procedure
- Disaster Recovery Plan

Practice, Audit and Discipline:

- Practice: Persons with responsibilities related to the company such as employees, employees of the contracting company, service providers as well as third party who uses the data of the company are required to recognize and comply with all the details of the policy.
- Audit: The company reserves the right in any circumstance to manage and protect the information and information technology system of the organization.
- Discipline: Any person who directly and indirectly commits a breach of the company's regulations or a potential damage to the company or anyone will be subject to both disciplinary and legal actions.