BDMS
Bangkok Dusit Medical Services
ทะเบียนเลขที่ 0107537000025

บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน)
2 ซอยศูนย์วิจัย 7 ถนนเพชรบุรีตัดใหม่
กรุงเทพฯ 10310
เลขประจำตัวผู้เสียภาษี 0107537000025

Bangkok Dusit Medical Services PLC.
2 Soi Soonvijai 7, New Petchburi Rd.,
Bangkok 10310 Thailand
Tax ID: 0107537000025

Tel +66(0)2310-3000 Fax +66(0)2310-3115
Contact Center Tel 1719
www.bdms.co.th

Information Security Management Policy

Bangkok Dusit Medical Services Public Company Limited and its Subsidiaries

Policy Statement

Bangkok Dusit Medical Services Public Company Limited (BDMS) and its subsidiaries have provided Information Technology System to facilitate the staffs to work for the organization, In order to ensure the consistency of the information security operations with the organization's policies and relevant laws BDMS has established an Information Security Management Policy to provide guidelines and standard regulations for employees and persons who duties are involved in the work to be able to perform tasks correctly.

Objective

To ensure that the information security operations of Bangkok Dusit Medical Services Public Company Limited and its subsidiaries standards are well defined and maintained accordingly to three following principles.

1) Confidentiality: To protect sensitive and private information from unauthorized access.
2) Integrity: To ensure the data are protected from modification by an unauthorized party.
3) Availability: To ensure the systems, applications and data are available and accessible to authorized users when needed.

Scope

All organization information users and organization information system users without exception.

Definitions

No.	Vocabulary	Definition
1.	Organization	Bangkok Dusit Medical Services Public Company Limited (BDMS) and its subsidiaries (BDMS plc). holding more than 50% of the shares.

No.	Vocabulary	Definition
2.	Information Security Management Committee: ISMC)	The group of persons officially appointed by the President
3.	Privacy & Information Security Working Group: PSWG	A working group appointed by the Chief Operating Officer (COO), consisting of representatives of Privacy and Information Security from each group or each subsidiary.
4.	Staff	Employees, Contractors, and other persons entrusted by the organization to perform the work under the terms or contracts.

<u>Roles and Responsibilities</u>

The organization has defined the roles, duties, and responsibilities of information security management through the organizational structure as follows:

- ➢ Approve and enforce policies or procedures related to the Information Security Management Policy.
- ➢ Define and approve criteria for risks and acceptable risk levels.
- ➢ Review the results of the risk assessment and remedial plans for important risks of the organization.
- ➢ Consider penalizing those who violate the information security management policy.
- ➢ Provide support for the resources needed to operate.
- ➢ Approve and promulgate policies or procedures related to personal data protection operations in accordance with the Data Security and Privacy Act.
- ➢ Approve the principles and practices of personal data protection to beas guidelines for data controllers and data processors.
- ➢ Appoint a working group to determine the guidelines of personal data management in accordance with the Act.
- ➢ Review the operation of personal data protection to ensure that the processing of personal data is in accordance with the Personal Data Protection Act other relevant laws.

Procedure

All companies covered by this policy are required to develop the procedures and plan detailed below and submit them for approval–by the Information Security Management Policy Committee and all the following procedures are defined to review in every 2 years or when there are significant changes, e.g., changes in law & regulations, the BDMS policies, etc.

- Information Asset Management
- Risk Assessment & Risk Treatment
- Information Classification & Handling
- Acceptable Use
- User Access Control
- Cyber Security Protection
- Physical Security
- 3rd Party Management
- Backup & Restore
- Cyber Security Incident Management
- Business Continuity Management

Workflow

- None

Communication Channel & Training

1. Notification via electronic mail (e-mail)
2. Post an announcement on the company's board.
3. Self-study in the e-document system

Monitoring and Measuring

The Information Security Management Policy Committee can assign the Privacy & Information Security Working Group (PSWG) to monitor and present the performance measurement of each group according to policies and procedures at least once a year

Related Documents

- None

- **References**

1. Cybersecurity Act: 2019
2. Personal Data Protection Act: 2019
3. Information Security Management System - ISO/IEC 27001: 2013
4. Information Security Management in Health - ISO/IEC 27799: 2016