

# Information Security Management System Policy

## Scope

This policy covers all IT operations of Bumrungrad Hospital Public Company Limited and its subsidiaries (the "**Company**"), including all types of Company assets (regardless of location), such as:

- Data (databases, documents, emails, etc.), including personal data;
- Licensed software or internally developed programs;
- Physical assets (computer rooms, computer equipment, laptops, tablets, printers, workspaces, etc.);
- Employees and personnel hired by the Company; and
- Various services (power backup systems, communications, network systems, etc.).

## Definitions

- **Information Security:** Maintaining confidentiality, integrity, and availability of information to prevent unauthorized access, alteration, or loss of data; and
- **Information Security Control:** The process of identifying information risk context (**Identify**), protecting information assets (**Protect**), detecting abnormal events (**Detect**), responding to incidents (**Response**), and recovering information assets to ensure business continuity (**Recovery**).

## Details

The Company establishes an overall policy for managing information security, divided into 13 key areas:

1. **Information Security Policy:** The Company has a written information security policy, communicated to all employees and relevant departments, reviewed periodically or when significant organizational changes occur;
2. **Human Resources Security:** The Company has established measures to control security in personnel management and to provide appropriate security awareness training for personnel. This is to ensure that Company employees and other personnel hired by the Company are aware of and comply with the Company's policies. It also includes revoking system access rights and returning Company assets upon termination of employment;

3. **Asset Management:** The Company maintains an asset inventory that specifies the owner or custodian of each asset, establishes guidelines for asset usage and return, and includes appropriate procedures for the destruction of data storage media;
4. **Access Control:** The Company has implemented secure access control for internal and external information systems, password policies, access rights assignment and review, and authorization as per Company regulations;
5. **Encryption:** The Company has implemented appropriate encryption measures to protect confidential information, ensuring that such information can only be accessed or used by authorized individuals;
6. **Physical and Environmental Security:** The Company has established measures to control the security of physical locations and environments, including access control to areas where computer systems are installed, backup power systems, air conditioning systems, and other protective systems (such as fingerprint scanners, CCTV, and automatic fire suppression systems). These measures are intended to prevent unauthorized individuals from accessing and causing damage to information assets. The Company also ensures that all equipment is properly maintained and kept in optimal and ready-to-use condition;
7. **Operations Security:** The Company has planned for information resources to be readily available, with appropriate protection systems, event logging, system usage monitoring, data backup systems, and secure data transmission or exchange (such as email and internet). This also includes change management controls to ensure the security of the Company's information systems;
8. **Network Communications Security:** The Company has established measures to control secure access to network systems, including the segmentation of networks between internal users and external users who interact with the Company;
9. **Systems Acquisition, Development, and Maintenance:** The Company has established information security measures at every stage of the system development lifecycle, covering development, testing, and test data processes, as well as security checks for data being imported or exported. These measures are also considered as part of the evaluation or contracting process with external service providers;
10. **Supplier Relationships:** The Company must establish protective measures for information assets that may be accessed by external service providers. There must be written agreements, service contracts, confidentiality agreements, and personal data processing agreements with external service providers who can access, process, store, or communicate information. These providers must comply with such agreements, and any changes in the services provided by external providers must be properly managed;
11. **Information Security Incident Management:** The Company has designated responsible personnel and established procedures to handle incidents affecting

information system security and violations of the Company's personal data protection measures. This includes reporting abnormal events and security weaknesses, as well as personal data breaches, to IT management and relevant regulatory authorities;

12. **IT Disaster Recovery Plan:** The Company has established IT business continuity plans to address situations where a crisis or disaster causes the information systems or network to become unavailable. The plan is tested at least once a year, or as appropriate, in order to use the results to improve the plan and ensure it aligns with business operations; and
13. **Compliance:** The Company ensures compliance with laws, regulations, and requirements set by government agencies and regulatory bodies, as well as all contractual obligations binding the Company.

## **Roles and Responsibilities**

- **Chief Information Security Officer:** Oversees compliance with the information security policy;
- **Department Heads:** Responsible for the security of assets and information under their supervision, coordinating with IT for audits and evaluation of security measures; and
- **Employees, Vendors, Contractors, and Consultants:** Must comply with the security policy, standards, procedures, and guidelines to ensure information security in their work.

## **Enforcement and Penalties**

This policy is part of the Company's regulations. Employees who violate or fail to comply may be subject to disciplinary action as specified in the Company's work regulations, at the Company's discretion.