Information Security and Cybersecurity Management Policy

Chularat Hospital Public Company Limited

Chularat Hospital Public Company Limited and its subsidiaries (the “Company”) have implemented information technology and computer network systems to facilitate employees in performing their duties effectively. To ensure the use of information technology resources is conducted in an appropriate, efficient, and secure manner, while mitigating risks that may lead to operational disruption, data loss, or damage to the Company, the Company has adopted this Information Security Management and Cybersecurity Policy. This policy serves as a framework and standard guideline for employees and all individuals who have responsibilities or involvement in related operations. The essential principles are as follows:

<u>**Governance Structure**</u>: The Company has established a formal governance framework to clearly define the roles, responsibilities, and accountabilities in managing information security, as follows:

- **Information Security Management Committee:** The Information Security Management Committee, comprising senior executives of Chularat Hospital Public Company Limited and its subsidiaries (the “Company”), shall be vested with the authority and responsibility to:
    - **Policy Approval**: Endorse and formally promulgate the Information Security Management Policy, together with any related rules, standards, or procedures necessary to support its effective implementation.
    - **Risk Governance**: Define, approve, and periodically review the criteria for information security risk management, including acceptable levels of risk.
    - **Risk Oversight**: Review the outcomes of risk assessments and approve mitigation strategies and remediation plans for material or critical risks.
    - **Disciplinary Oversight**: Deliberate and determine appropriate disciplinary measures for violations of the Information Security Management Policy.
    - **Resource Allocation**: Ensure the allocation of sufficient resources—financial, technological, and human capital—to maintain and continually improve the effectiveness of information security management within the Company.
- **Data Protection Officer:** Employees as well as individuals formally assigned with responsibilities relating to information security and personal data management, shall undertake the following primary duties:

  - **Supervision and Guidance**: Oversee and provide direction regarding the collection, storage, and use of personal data within various systems to ensure compliance with applicable laws and policies.
  - **Monitoring and Reporting**: Conduct regular reviews of personal data management practices across systems and promptly report risks, incidents, or circumstances related to information security, together with recommended corrective actions, to the Information Security Management Committee and other designated authorities.
  - **Incident Response**: Respond effectively to information security incidents, ensuring timely management and resolution in accordance with established protocols.
  - **Training and Awareness**: Organize training programs and deliver ongoing awareness initiatives to enhance employees' understanding of personal data protection and responsible data handling practices.
  - **Information Sharing**: Proactively monitor developments, emerging threats, and industry updates related to information security and personal data protection. Communicate relevant alerts, guidance, and best practices to employees and stakeholders within the Company.
  - **Collaboration and Coordination**: Liaise with relevant internal departments and external stakeholders, including regulators, service providers, and business partners, to ensure effective coordination in the governance, protection, and lawful use of information and personal data.

- **Information Security Director:** The Company's appointed Management Representative for Information Security shall assume the following responsibilities.
  - **Policy and Strategic Advisory**: Provide guidance and recommendations to senior management on the formulation, adoption, and enhancement of policies, standards, and measures relating to information security management.
  - **Oversight of IT and Network Administration:** Supervise and advise information technology administrators and network system administrators to ensure compliance with the Company's Information Security and Cybersecurity Management Policy.
  - **Awareness and Communication**: Communicate to all employees the importance of information security and their respective responsibilities in safeguarding the Company's data.
  - **Support and Capacity Building**: Provide necessary resources, training, and knowledge to employees and relevant external parties to facilitate compliance with the Information Security and Cybersecurity Management Policy.
  - **Compliance Monitoring**: Conduct appropriate monitoring and verification of compliance with the policy by employees and relevant third parties.

- ○ **Policy Review and Improvement:** Periodically review and recommend revisions to the policy to ensure its alignment with current business conditions, emerging threats, and best practices.
- ○ **Incident Coordination**: Coordinate and implement appropriate measures to contain, mitigate, and resolve incidents of non-compliance or security breaches within the Company.
- ○ **Reporting**: Submit quarterly performance and compliance reports to the Information Security Management Committee. Report promptly on the progress, status, and resolution of security incidents or relevant developments to the Committee.
- ○ **Other Assigned Duties**: Carry out any additional responsibilities as prescribed under this Policy or as delegated by the Information Security Management Committee.

- ▪ **CHG Computer Emergency Response Team (CHG CERT)**, comprised of designated personnel from Chularat Hospital Group or assigned representatives, shall assume the following key roles and responsibilities to safeguard the Company's information assets and ensure resilience against cybersecurity threats:
  - ○ **Incident Response and Management**: Respond promptly and effectively to information security incidents, ensuring timely containment, mitigation, recovery, and documentation.
  - ○ **Threat Advisory and Remediation**: Provide recommendations and implement corrective measures to address and neutralize information security threats and vulnerabilities.
  - ○ **Monitoring and Information Sharing**: Continuously monitor developments in the cybersecurity landscape and disseminate relevant alerts, advisories, and security updates to stakeholders across the Company.
  - ○ **Research and Continuous Improvement**: Regularly study, evaluate, and update tools, methodologies, and practices to ensure the Company's information technology systems remain secure, resilient, and aligned with evolving threats and best practices.
  - ○ **Other Assigned Duties**: Undertake additional responsibilities and assignments relating to information security management as directed by senior management or the Information Security Management Committee.

Implementation Guidelines: All subsidiaries governed by this Policy shall be required to establish detailed operational procedures and contingency plans as outlined below. These documents must be developed, formally approved, and submitted to the Information Security Management Committee for endorsement within 180 days from the effective date of this Policy.

- ○ Information Resource Usage Policy - Regulations governing the appropriate and secure use of the Company's information resources.

- Personal Data Protection Policy – Guidelines to ensure the confidentiality, integrity, and reliability of personal data.
- Cybersecurity Protection Policy – Guidelines to safeguard against cyber threats and ensure appropriate incident response.
- User Account and Access Management Policy – Procedures for the creation, use, monitoring, and termination of user accounts in information systems.
- Third-Party Information Service Management Policy- Procedures and requirements for assessing, monitoring, and managing risks associated with external IT service providers.
- Information Asset Management Policy – Guidelines for the classification, protection, and proper handling of information assets.
- Data Backup and System Recovery Policy – Standards and procedures for data backup, restoration, and recovery of critical IT systems.
- Critical Incident Response Policy – Processes to address major disruptions or security incidents effectively.
- Disaster Recovery Plan (DRP) – Comprehensive strategies and plans to restore business and IT operations following catastrophic events.

Compliance, Oversight, and Disciplinary Measures:

- Compliance: All individuals who have responsibilities within, or are engaged with, the Company—including employees, contractors, service providers, counterparties, and any external parties with authorized access to the Company's information—are required to be fully aware of and comply with the provisions of this Policy.
- Oversight: The Company reserves the right to take any actions deemed necessary to manage, monitor, and safeguard the security of its information assets and information technology systems.
- Disciplinary Measures: Any violation of this Policy, whether deliberate or negligent, that causes or has the potential to cause harm to the Company, its stakeholders, or any individual, directly or indirectly, shall be treated as a serious offense. Violators shall be subject to disciplinary action in accordance with the Company's rules and regulations and may also face legal consequences where applicable.

Policy Review and Continuous Improvement

The Company shall review this Policy on a regular basis and update relevant practices to ensure that its operations remain fully aligned with the Information Security and Cybersecurity Management Policy.