Bangkok Lab and Cosmetic Public Company Limited
48/1 Moo 5, Nongshaesao Road, Tumbon Namphu, Ampur Meung,
Ratchaburi 70000, Thailand

(Translation)
Management Document of Bangkok Lab Cosmetic BLCP 10-053

Information Security Policy

Revision No. 0 Effective Date: 02/07/2025

(Translation)

Bangkok Lab and Cosmetic Public Company Limited

Information Security Policy

Approved by *Assist. Prof. Dr. Wanchai Sutananta*
(Chairman of the Board of Directors)
Based on the Resolution of the Board of Directors Meeting
No. 5/2025 on June 20, 2025

Revision No. 1/2025

Table of Contents

(Translation)

Information Security Policy

Bangkok Lab and Cosmetic Group (the "Company") recognizes the importance of information as the organization's most valuable asset. Therefore, it has established an information security policy to ensure that the entire information system is managed effectively and serves as a framework and practice for protecting and maintaining information assets from all types of threats, whether intentional or unintentional, originating both within and outside the organization. This policy covers the confidentiality, accuracy, integrity, and availability of information. Thus, the information security policy is announced, and its content is continuously updated.

Objectives

1. To establish guidelines for effectively securing information systems according to the information technology security standards, ISO/IEC 27001.
2. To enhance customer confidence in the Company's ability to provide services and maintain the confidentiality of information and information technology systems.
3. To provide guidelines for determining the Company's information technology operations to align with good internal controls over information, comply with relevant laws, regulations, and requirements, and prevent any violations related to the use of the Company's information systems.

Information Security Practices

Section 1: Organizational Controls

1.1 The information security policy is approved by management and communicated to internal personnel and relevant external parties, as well as reviewed at specified intervals or when significant changes occur.

1.2 Roles, duties, and responsibilities regarding information security are defined and responsibilities are divided according to the organizational structure.

1.3 Regarding the separation of duties and responsibilities, any duty or its performance that would create a conflict of interest for the Company must be separated.

1.4 Regarding the responsibilities of management, management must ensure that all personnel adhere to and maintain the security of information by following the information security policy and the established procedures or work processes.

1.5 Regarding communication with authorities, the Company establishes and updates information for contact with the authorities.

1.6 In contacting specialized groups with shared interests, it requires establishing contact information for these groups and those with expertise in information security.

1.7 For information or intelligence regarding security, information related to threats to information security is collected and analyzed to prepare security-related information or intelligence.

1.8 For information security and project management, information security must be integrated with project management.

1.9 Lists of information and other related assets, including property owners, must be prepared and updated to ensure the information is up-to-date and accurate.

1.10 Regarding the proper use of assets, the Company has established procedures for managing data and related assets in writing and put them into practice.

1.11 For return of assets, personnel and those involved from external agencies must return all assets they hold upon termination or change of employment or employment contract.

1.12 For data confidentiality levels, data is categorized according to the Company's information security

requirements, considering confidentiality, integrity, and availability from relevant departments.

1.13 Regarding data identification, the Company has established procedures for data identification as appropriate and put them into practice in accordance with the established data confidentiality levels.

1.14 In terms of data transfer, the Company has established regulations/procedures for transferring data of all types of devices or equipment, both internal and external data transfers.

1.15 Regarding access control, the Company has established criteria for accessing data and assets, both physical access and remote system access, and put them into practice.

1.16 For identity management (used for system authentication), the entire life cycle of identity data, which is part of the authentication process for system access, must be managed throughout the data life cycle.

1.17 In terms of data related to authentication, the allocation and management of data related to authentication must be properly controlled.

1.18 Access rights to data and assets must be reviewed, updated, and revoked in accordance with the organization's access control policy.

1.19 The information security and relationships with external service providers must be implemented to manage risks to information security related to the use of products or services from external service providers.

1.20 Information security requirements must be specified in the service agreement with the external service provider. Relevant information security requirements must be defined and agreed upon with each external service provider, depending on the type and relationship with that service provider.

1.21 Procedures for information security management in the ICT service and product supply chain must be established for ICT.

1.22 There must be regular monitoring, reviewing, evaluating, and managing changes in information security practices and the delivery of services from external service providers.

1.23 The information security must be established for the use of services. The management and use of Cloud services must be defined according to information security requirements.

1.24 There is planning and preparation for managing information security incidents.

1.25 There is assessment and decision-making for incidents related to information security.

1.26 Handling information security incidents is conducted according to the established written procedures.

1.27 Knowledge gained from information security incidents must be used to strengthen and improve information security measures.

1.28 The Company has established procedures to identify, collect, and maintain evidence of incidents related to information security.

1.29 The Company has planned to maintain information security at an appropriate and sufficient level to meet the needs during disruptions.

1.30 The availability of ICT for business continuity must be planned and ensured at all times, in accordance with the objectives and requirements for business continuity and the related ICT systems.

1.31 Requirements related to laws, regulations, and employment contracts must be documented in writing and kept up to date.

1.32 Intellectual property rights require appropriate procedures to protect intellectual property rights and prevent infringement of both the Company's and others' intellectual property.

1.33 Regarding data protection, the organization's data must be protected from loss, destruction, falsification, unauthorized access, and unauthorized dissemination.

1.34 Privacy and personal data protection must be identified and implemented in accordance with the requirements mandated by laws and regulations.

1.35 Independent reviews of information security must be conducted independently at specified intervals or when significant changes occur.

1.36 Compliance with policies, rules, and standards for information security must be reviewed regularly.

1.37 Written operational procedures must be available for personnel who need to use them.

Section 2: People Controls

2.1 Selection and background checks of job applicants must be conducted at an appropriate level to business needs, the confidentiality level of the data to be accessed, and the associated risks.

2.2 Employment agreements and conditions must address the information security responsibilities of personnel and the Company.

2.3 Awareness, education, and training in information security must be appropriately provided to personnel.

2.4 Disciplinary processes must be formally defined and communicated to personnel regularly.

2.5 Responsibilities after the termination or change of employment must be mandated as specified and communicated to personnel and relevant departments.

2.6 Confidentiality or non-disclosure agreements must be clearly identified, documented in writing, regularly reviewed, and signed by personnel and relevant parties from various departments.

2.7 When personnel work remotely, security measures must be implemented to protect data that is accessed, processed, or stored outside the organization.

2.8 Reporting information security-related incidents requires a mechanism for personnel to report observed or suspected information security incidents through appropriate and timely reporting channels.

Section 3: Physical Controls

3.1 A physical boundary or perimeter must be established to protect the area with related information and assets.

3.2 For physical access control, areas requiring security must have appropriate access control and controlled access points.

3.3 Maintaining security for the office, workspaces, and equipment requires a design and implementation to provide tangible protection.

3.4 For physical security monitoring, it requires continuous monitoring and surveillance to prevent unauthorized physical access.

3.5 Protection against physical threats and environmental hazards, such as natural disasters and both intentional and unintentional physical threats, must be designed and implemented.

3.6 Operations in areas requiring security must be designed and implemented.

3.7 Document-free workspaces and computer screen protection must be established and enforced to prevent physical access to critical documents and data of the organization.

3.8 Regarding equipment placement and protection, equipment must be placed and protected to ensure its safety.

3.9 Regarding the security of assets used off-site, such assets must be protected.

3.10 Data storage media must be managed throughout their lifecycle in accordance with confidentiality classification methods and the management of related data and assets.

3.11 Supporting utility systems must be protected from power failures and other disruptions.

3.12 The security of the signal line must be protected from disruption, signal interference, or damage.

3.13 Equipment maintenance is required to ensure readiness for use and the maintenance of data accuracy

and confidentiality.

3.14 Security for the disposal or destruction of equipment or other use of equipment must be verified to ensure that critical data and licensed software are securely erased or overwritten before they are disposed of or used in any other way.

Section 4: Technological Controls

4.1 End-user devices must be protected. This typically encompasses notebooks, computers, mobile phones, and other data-processing devices that users commonly utilize or that have the capability to transmit data over a network.

4.2 For exclusive access rights, the allocation and granting of exclusive access rights, such as administrator level or managerial level, must be limited and managed.

4.3 Restrictions on access to information and related assets must be implemented according to specific policies tailored to the access control guidelines established.

4.4 Restricting access to source code, system development tools, and software that can be read and overwritten must be properly managed.

4.5 For secure authentication, technologies and procedures for secure authentication must be implemented based on specific policies tailored to matters related to access control.

4.6 For system capacity management, the use of system resources must be monitored, tracked, and adjusted to meet current and projected resource requirements.

4.7 Protection against malicious programs must be implemented and supported by appropriately raising awareness of users.

4.8 Technical vulnerability management requires monitoring to obtain information on vulnerability risks, assessing them, and defining appropriate measures to implement.

4.9 For system configuration management, security settings for hardware, software, services, and networks must be defined, documented, implemented, monitored, and reviewed to ensure compliance with the defined settings.

4.10 Regarding data deletion, data stored in information systems, devices, or other data storage media must be deleted or destroyed when it is no longer needed.

4.11 Data concealment measures must be implemented to prevent unauthorized viewing or misuse of data stored in the system. These measures should adhere to specific policies that address relevant issues and business needs, while also considering applicable laws.

4.12 Data leakage prevention must be applied to systems, networks, and devices that process, store, or transmit critical data.

4.13 Regarding data backup, copies of software and system data must be regularly stored and tested in accordance with specific policies tailored to each data backup matter.

4.14 Data-processing equipment backup requires adequate backup arrangements to meet the availability requirements of those devices.

4.15 Logging requires a system arrangement for log data to create, store, protect, and analyze data.

4.16 System and equipment monitoring activities must be carried out to detect abnormal behavior and assess the likelihood of potential information security incidents.

4.17 In setting the clock correctly, it must be set accurately against an authorized time reference source.

4.18 The use of utility programs with privileges allows for the breach of application control measures, and the system must be strictly restricted and controlled for use.

4.19 Regarding software installation on service systems, necessary procedures and measures must be implemented to manage software installation on service systems securely. Once development and testing are complete, the software will be installed on the service system to provide services to users.

4.20 For network security, security, safety, and controls must be maintained to protect data in systems and applications running through the organization's network and network devices.

4.21 The security of network services must be defined, implemented, tracked, and maintained to ensure compliance with established mechanisms, service level, and requirements.

4.22 The segmentation of networks, groups of information services, users, and information systems must be separated within the organization's network according to the organization's needs.

4.23 For web filtering, access to external websites must be managed to reduce the likelihood of accessing harmful content.

4.24 The use of data encryption and rules for the use of data encryption, including the management of encryption keys, must be defined and implemented.

4.25 The security development lifecycle and rules for developing secure software and systems must be defined and implemented.

4.26 Application security requirements must be defined and approved during the development or provision of the application.

4.27 The secure system architecture and system engineering principles must be defined, documented in writing, updated, and implemented in information system development activities.

4.28 For secure programming, the principles of secure programming must be applied to software development.

4.29 Security testing in system development and certification must be defined and implemented throughout the system development lifecycle.

4.30 Regarding system development by external agencies, the organization must oversee, monitor, track, and review the activities related to system development undertaken by external agencies.

4.31 The separation of the environment for testing, development, and provision of services is required and must have security measures.

4.32 Change management must include controls through established procedures for change management.

4.33 Data for testing must be properly selected, protected, and managed.

4.34 Protecting information systems during system testing by assessors requires planning and agreement between the testing operators and relevant executives to prevent potential problems with the service system, such as system disruptions during testing or unauthorized access to critical data in the system.

Policy Review

The information security policy will be reviewed and assessed for its adequacy and appropriateness annually.

This information security policy was approved by the Executive Committee Meeting No. 5/2025 on June 20, 2025, and was effective from June 21, 2025, onward.