Berli Jucker Public Company Limited
บริษัท เบอร์ลี่ ยุคเกอร์ จำกัด (มหาชน)

Information and Cyber Security Policy	**Reference number : SRMD 03/ 2020**
	Review date : 31 July 2025
	Approval date : 31 July 2025
	(Executive Board Meeting No.4/2025)
	Effective date : 31 July 2025
	Supersede date : 29 June 2022

Berli Jucker Public Company Limited Group and the group company (hereinafter referred to as "BJC Group") places importance on the development of digital technology and use of information in conducting business. BJC Group realizes the importance of information security, including prevention of cyber threats so this policy has been established to create operational guidelines for data security and the use of information technology in BJC Group. In addition, BJC Group places great importance on data integrity ensuring the accuracy and completeness of information as well as protecting data from unauthorized access, alteration or use across all related processes.

Policy Scope

This policy applies to the business operations under Berli Jucker Public Company Limited and its subsidiaries.

Guidelines

1. Providing various measures to ensure that information security is sufficient and appropriate consistent with business operations, level of importance of data, including internal and external factors that affect information security. BJC Group pays attention to the confidentiality of information, data availability, completeness and accuracy to complying with the laws, rules and regulations of related external parties.
2. Setting guidelines for all executives, directors and employees to follow information security/cybersecurity policy / company secrets as specified in the code of conduct of BJC Group strictly as follows;

    2.1 During the employment period, employees will aware of company information known as "trade secrets", means trade information which has not yet widely known or not yet accessible among the persons who are related to such information. It is the information which is useful commercially as it is a secret and it is the information which a commercially trade secret controller uses appropriate measure to maintain its secrecy so this information may be stated in contract or any other agreement of the company or specified in the trade secrets act, B.E 2545 (2002). Employees agree to keep "trade secrets" of the company that have known or given because of working for the company and do not send or copied to recipient without permission, including disclose and / or do or refrain from any action that damage to the company's reputation or the company's business.

2.2 Maintaining confidentiality with customers, contractors or business partners or any other person of BJC Group.

2.3 Shall not reveal any confidential information, documents or trade secret for 1 year after leaving their duties.

2.4 All Employees shall strictly adhere to and comply with BJC Group's information security policy without interfere in other's privacy. Do not use confidential information that not authorized, including accessing data and files of other users without permission in accordance with rules, regulations, and company regulations about using of equipment and tools in computer systems.

2.5 Shall not bring assets or use the internet of BJC Group with commercial purpose or personal benefit except for directly benefit to the company, including avoid using the website or electronic mail that is vulnerable to cyber-attack.

2.6 Shall not install software or record any information in the company's computer without permission.

2.7 Shall not bring the company's software to other persons which includes suppliers, contractors, customers of the company and personal agenda.

Furthermore, the use of the internet or connect to the internet by employees to transferring data, dissemination of pornography, sending and receiving information via electronic mail (e-mail) that violates the law or copyright law or the intent or the purpose of the policy or regulations for information security policy of the company or Computer-related Crime Act B.E 2550 (2007) or other related laws.

2.8 No copyrights infringement of the company and / or of other companies that allow the company to use computer software regardless of the contract and / or any methods and / or whether the action is repeated or modify or distribute to the public or rent or copy whether for profit or not.

3. Providing Information security and cyber security awareness training as well as communicating related to information technology, information security and cyber threats to all employees regularly.

4. Defining roles, responsibilities and duties appropriately for operation about information systems and information security, including setting authorization and control for accessing important information. Moreover, the equipment or space used to store important data both is protected appropriately through physical storage and information systems to prevent any access to sensitive information without permission.

5. Password policy is set to be in line with business operations and current situation as well as communicated to all employees that they must keep their password and any other

codes specified by the company to access the computer system or company information or personal information confidentially. Password must be kept so that others do not know, and do not share with other people to comply with the password policy strictly.

6. Employees shall use the assets of the company with care, responsibility for the equipment. Any received equipment from the company should be always in good condition by contacting repair department when damage occurs. The company's assets must not be lost or destroyed, even if equipment are not their responsibility directly. Do not bring any property to use for other purposes except for company's benefits. Any equipment that has important information or able to access the information system of the company must be prevented from being used by people who are not authorized, such as setting a password or screen saver of the computer when not in use. If the device is lost or stolen, notify the management Information System Division as soon as possible to consider the appropriate actions for information security.
7. Using of personal equipment to connect with the company information system must comply with rules and regulations set by person in charge of information systems.
8. Sending, using, processing, storing and destroying important information and equipment that has important data must be an appropriate process to ensure that adequate information security for preventing disclosure of information without permission or accessed by unauthorized people.
9. Information system development shall have accurate and reliable process which covers the process of system design, development, testing and implementation. There is a separate system for development and the system that actually works, including places importance to designing systems with sufficient security and have security checks before actual use.
10. Any amendment to information systems or related equipment must have appropriate procedures and processes. There is impact assessment for relevant parties and communicate to them, including sufficient testing and updated relevant documents.
11. There are adequate and appropriate network security measures. Protection programs have to be installed to prevent external threats on main and client's server, and the program shall be updated at an appropriate time.
12. There is storage of important information systems (Log) and set the appropriate storage period. Log will be used in the inspection and trace back to usage history that comply with the laws, rules and regulations of related external parties.
13. There is a process in place to prevent information system interruptions and cyber-attacks within a timely manner, in addition consideration of action for preventing recurrence of situation and report to the management board.

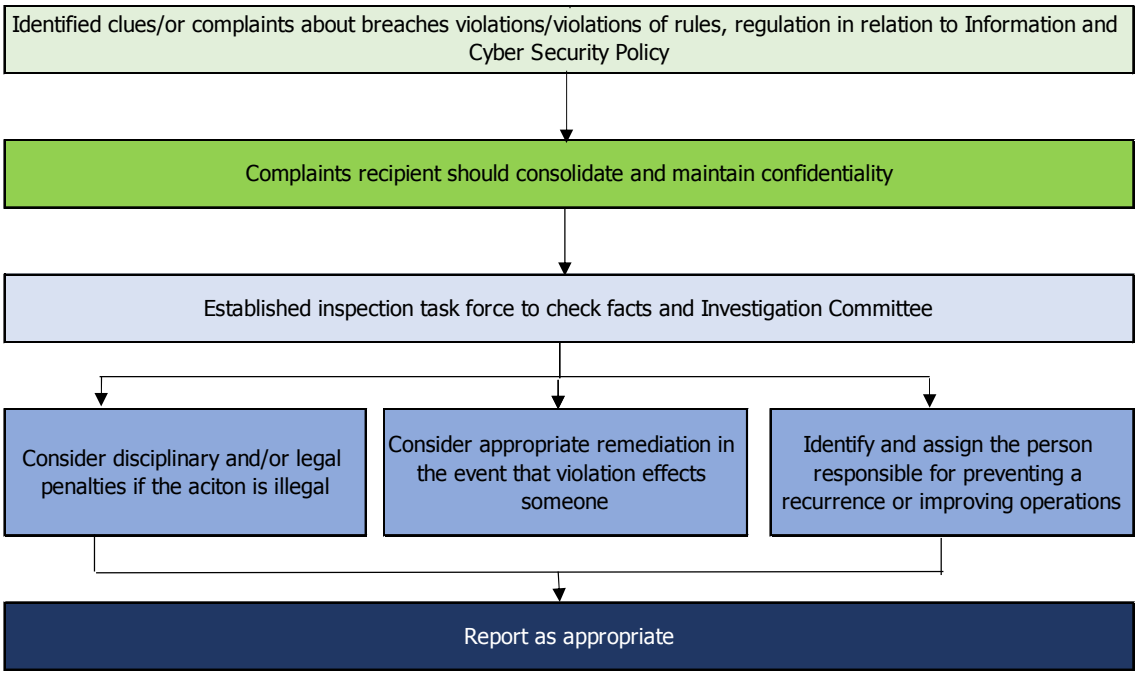
14. Critical data is securely stored, including the determination of business continuity plans and incident response procedures in place with regular test of Disaster Recovery Planning.
15. There is a centralized maintenance of information technology equipment for maintaining equipment in good condition and continuous usage.
16. Using of information technology services from outsource must have sufficient security in accordance with the company policy. There is selection, monitoring and evaluation of services appropriately.
17. There is a risk assessment of the organization and related parties regarding of information security and cyber threats by setting the risk management guidelines appropriately.
18. There is a clear escalation process which employees and stakeholders can make complaint or report something suspicious related to information security and cyber-attacks so the company have appropriate corrective and preventive communication procedures to manage about the issue. All employees are responsible for reporting information immediately about suspicious events that bring to infringement of policies and measures, data theft, intervention, invasion, or destruction of information systems that affect information security or cause damage to the company.
19. Employees shall acknowledge and follow the guidelines of using computer and network systems appropriately, including information security procedure to prevent confidential information from being unintentionally disclosed. The company supports information security is a part of employee performance evaluation for the development of human resource appropriately.
20. During the employment period, employees shall not do anything and / or refrain from any actions that cause damage to the company as a result of false information and / or reports or records or communications whether by any means. If there is intentionally violation of policies or measures related to information security that cause damage to the company, the person who violate the rules will be punished according to the regulations of the company, and prosecuted if the operation is against the law.
21. The company is committed to continuously enhancing its information security systems through regular reviews of security processes, measures, and technologies to ensure alignment with technological advancements, international standards, and the evolving risk landscape. Improvements and updates are guided by test results and recommendations from both internal and external audits, as well as lessons learned from real incidents. The company places strong emphasis on maintaining data integrity in addition to ensuring data protection, in accordance with international standards.

22. The company places strong emphasis on monitoring and responding to information security threats. This includes continuous anomaly detection, comprehensive risk analysis, and the deployment of real-time alert systems designed to identify intrusions or unusual activities. A dedicated Cybersecurity Operations team is tasked with promptly analyzing and addressing threats to ensure swift and effective incident response.
23. Clear roles and responsibilities regarding data security are defined for employees at all levels. Specialized training is provided to personnel responsible for managing or accessing critical data to ensure they understand their individual responsibilities and are equipped with appropriate practices aligned with their roles.
24. Information security requirements are established for relevant external parties, such as IT service providers, suppliers, or business partners, through contracts and/or agreements that include provisions on confidentiality, data access control, and more. In addition, appropriate assessments or audits are conducted to ensure that external parties comply with adequate and appropriate security standards.

Any violation of the laws, rules, regulations, ethics, or this policy, or permitting subordinates to violate them, executives, committees, and employees must report directly to the company's given channels. The company has clearly defined policies, processes, and measures to protect whistleblowers. When internal or external parties suspect or believe that laws, regulations, or ethics are being violated, they can report through the channels provided. The Investigation Committee and/or Inspection Taskforce, comprised of representatives from Human Resources, Group Audit Department, Legal, and the relevant Head of Business Unit where the incident occurred, will then carry out the procedures in accordance with Corporate's Whistleblowing Policy and the BJC Code of Conduct. BJC's corporate-wide whistle blowing system are shown as illustrated below.

Berli Jucker Public Company Limited
บริษัท เบอร์ลี่ ยุคเกอร์ จำกัด (มหาชน)

Information and Cyber Security Policy	Reference number : SRMD 03/ 2020
	Review date : 31 July 2025
	Approval date : 31 July 2025
	(Executive Board Meeting No.4/2025)
	Effective date : 31 July 2025
	Supersede date : 29 June 2022



The Information and Cyber Security Policy will be effective from 31 July 2025 onwards.