IT Security Policy

Index

1. Objective

To establish policies and operating procedures for information and information technology systems security in accordance with both domestic and international standards, to promote awareness among employees and related parties about the importance of security, to build confidence and reliability in providing services to customers, shareholders, investors, and stakeholders, and to support compliance with the requirements of the Bank of Thailand, relevant Acts, and laws.

2. Scope of the Policy

This Information and IT System Security Policy is effective for all levels of employees and management, temporary employees, probationary employees, consultants, business partners, contractors, vendors, and other individuals who use all information and IT system resources. These resources include general data and resources, computer and network resource systems, operating systems, applications, and programs that are owned, developed, managed, or leased from other entities, including legal titles and copyrights. This Information and IT System Security Policy shall be reviewed at least once a year or when there are changes or modifications that affect the security of the information system, and/or when related regulations or laws are changed.

3. Definitions

- **Data** means anything that conveys meaning to represent a story, facts, information, or any other thing, regardless of whether the meaning is conveyed by the nature of the thing itself or through any means, and regardless of whether it has been created in the form of documents, files, reports, books, charts, maps, drawings, photographs, film, video or audio recordings, computer records, or any other method that allows the recorded material to appear.
- **Information** means facts obtained by extracting data to have meaning through processing and organizing the data, which may be in the form of numbers, text, or graphics, into a system that users can easily understand, such as reports, tables, charts, etc., and can be utilized for administration, planning, decision-making, and other purposes.
- **Information Technology** means knowledge in products or in any process or operation that relies on technology, software, hardware, communication, collection, use, or dissemination of information.
- **Information System** means an information system that utilizes computer system technology and communication system technology to assist in creating information, used for administrative planning, development, and control, which consists of the following components: Computer System, Communication System, and Information, all of which operate within the computer system.
- **Computer System** means a device or a set of computer devices connected together for operation, where commands, sets of commands, or other things, and operational guidelines have been defined for the device or set of devices to automatically process data. It consists of Hardware, Software, and Computer Personnel (Peopleware) used to process data to create information.

- **Information Technology Network** means the communication or transfer of data between information systems, such as an Intranet system, an Internet system, etc.
- **Communication System** means a system composed of a receiver, a sender, and a medium in the communication system used to transmit data (characters, numbers, images, sounds, etc.), including wired circuit systems such as Cable, Coaxial Cable, Fiber Optic, and wireless systems (Wireless) such as mobile phones, Microwave, Satellite, as well as other equipment such as Hubs, Switching, and Routers.
- **Information System Workspaces** means areas used to install computer systems, network systems, or other information systems, or for data preparation, storing computer equipment, office spaces for computer personnel, including personal computers installed at workstations.
- **Information Security** means maintaining the confidentiality of information to ensure that the information is complete, accurate, and ready for use, with the following details for information security:
    - **Confidentiality of Information** is the appropriate protection of information security to ensure that individuals accessing the systems and information are properly authorized persons.
    - **Integrity and Accuracy of Information** is the preservation of information to be complete and accurate, where all updates or changes must be authorized.
    - **Availability of Information** is the maintenance of systems and information to ensure they can be used efficiently and continuously according to the stipulated timeframe.
- **Threat** means a danger that may arise to the information system by people, things, or events, both intentional and unintentional, which causes the information of the information system to be disclosed, changed, distorted, destroyed, denied operation, or other actions according to the demand of that threat.
- **Vulnerability** means any weakness or flaw in the information system that a compatible Threat can exploit to cause harm to that information system.

4. Policy Content

4.1. Security Policy

Information Security Policy

4.1.1. The Information Security Policy shall be prepared in writing and must be approved by the senior management before implementation and disseminated to employees and relevant external parties.

4.1.2. Define the responsible unit for preparing the guidelines for the information system security policy and review the policy periodically or when there are significant changes.

4.2. Internal Organization Security

4.2.1. Internal Organization Security Structure (Internal Organization)

- Define clear measures and procedures for security management that are consistent with the structure, and establish a unit representative for management, coordination, and internal consultation.

- Clearly define and separate the duties and responsibilities of employees, and arrange for periodic inspections to be consistent with and in compliance with the security policy.
- Define measures for the approval of new system usage and/or information processing equipment, and control compliance.
- Arrange for the signing of non-disclosure agreements between employees and concerning confidentiality, and regularly update related terms or conditions. Implement control measures for the exchange of security system-related information, where the implemented measures must be stringent enough to ensure that critical information is not disclosed to unauthorized persons.
- Prepare a list and contact information for security coordination with internal units, government agencies, and various organizations related to information security.
- Mandate an independent auditor to inspect the management, operation, and practice related to information security periodically or whenever there are significant changes.

4.2.2. Internal Organization Security Related to Customers or External Parties

- Define measures for accessing information by external parties, by conducting a risk assessment arising from accessing information or the equipment used to access the information.
- In cases where customers, service users, or external parties need to access the information or information assets of the company, an agreement/contract related to security must be specified and prepared, along with a clear statement of the necessity for access. Furthermore, the use by external parties must be strictly controlled.

4.3. Asset Management

4.3.1. Responsibility for Assets

- Create and constantly update the inventory of information assets to be accurate, specifying the responsible person, the unit that owns the information, and the assets related to information processing, as well as periodically inspecting the information asset inventory.
- Establish rules, regulations, or procedures for using information assets to prevent damage from misuse.

4.3.2. Information Classification

- Classify information according to the importance of the data and information assets, and define appropriate control and protection measures in compliance with legal requirements.

4.4. Human Resources Security

4.4.1. Security Prior to Employment

- Define employment conditions, job responsibilities, qualifications check, and arrange for the signing of an employment contract/agreement between the prospective personnel, those working from external entities, and the organization. Compliance with the employment contract and the organization's information security policy and procedures must be strictly controlled.

4.4.2. Security During Employment

- Regularly organize training and publicize the security policy to ensure that employees and external parties are informed and comply correctly. Relevant units must always create/update operating manuals and procedures to be current.
- Define disciplinary measures to punish employees who violate or breach the security policy and/or procedures.

4.4.3. Termination or Change of Employment

- Define procedures for terminated employees or those whose employment status has changed, requiring the responsible unit to strictly control compliance.
- Terminated employees or those with a change in employment status are not allowed to access, modify, or perform any actions on the organization's information system data. The responsible unit is required to promptly remove their rights to access the organization's data and information systems across all systems and must return all assets under their responsibility during their employment.

4.5. Physical and Environmental Security

4.5.1. Secure Areas

- Define controlled areas to prevent unauthorized access. Strictly control entry and exit in such areas to prevent potential damage to the information system, equipment, and information processing.
- Control and monitor the work of external parties operating in controlled areas by the employee responsible for that area throughout the period of work.
- Provide physical protection and procedures for maintaining security in offices, workplaces, and other assets to protect them from risks arising from accidents and external events such as accidents, fire, flood, earthquake, terrorism, etc.

4.5.2. Securing Data Center

- Operational procedures and a security system for entering and exiting the data center should be established. Sufficient equipment or systems for protection and warning in the data center should be provided to prevent threats, and the operation of such procedures and systems should be regularly inspected.
- Entry and exit from the data center must be controlled, inspected, and authorized only for employees with rights or external individuals approved by the data center administrator.
- Operations within the data center should have operational documentation, and adherence to the manual or operational documentation is required. Documentation must be up-to-date and usable.
- Install monitoring and damage prevention systems as appropriate, such as closed-circuit television (CCTV), uninterruptible power supply (UPS) systems, fire protection systems, and humidity and smoke detection systems.
- There should be a system to prevent computer systems from being damaged by power instability.

- Uninterruptible Power Supply (UPS) systems must be installed to ensure the system can provide services in case of power shortage or failure.
- Backup power systems (Grid) are provided as necessary to ensure adequate system services in case of power failure or shortage.
- Regularly inspect and test the operation of various damage prevention systems within the data center, according to the timeframe specified in the requirements for maintaining each piece of equipment or system.

4.5.3. Equipment Security

- The placement of office equipment must consider the risk of unauthorized access and environmental threats and various hazards that may occur. Measures must be defined to ensure the safe placement of office equipment.
- Critical support systems and equipment, including backup power systems, backup communication systems, temperature control systems, air conditioning systems, ventilation systems, etc., must have defined protection methods to ensure continuous use and prevent problems for the information system.
- Power cables, communication cables, and other cables must be appropriately protected and maintained, and prevented from unauthorized access, obstruction, or damage.
- Define methods and responsible persons for regular maintenance of various equipment to ensure continuous operation and that the equipment is in complete working order and ready for use.
- All types of information assets taken outside the organization must be authorized beforehand and strictly controlled. Procedures must be defined by considering various environmental conditions and risks that could cause damage to those assets.

4.6. Communication and Operation Management

4.6.1. Operational Procedures and Responsibilities

- Implement controls for changes, updates, and modifications to the information processing systems and/or equipment, and ensure that relevant units are informed and comply.
- Separate duties, operating procedures, and procedures for abnormal events or security breaches related to information systems and networks, to prevent or reduce the opportunity for unauthorized changes, modifications, or misuse of the organization's information assets.
- Keep development, testing, and production systems separate, and isolate computers used for information system development from those used for actual service provision to reduce the risk of unauthorized access or modification to the production system.

4.6.2. Third Party Service Delivery Management

- When using services from external parties, the service provider must comply with security measures, service characteristics, and service level requirements in the contract and/or agreement, including controlling usage and system access based on granted rights.

- Service conditions must be updated when there are significant changes in the service provider's organization that may affect the systems or processes related to the external service.

4.6.3. System Planning and Acceptance

- Require units to plan for additional information resource requirements to ensure the system is efficient and can support future increases in usage.
- Define criteria for testing and acceptance of new, updated, upgraded, and other information systems before they are put into actual use.

4.6.4. Protection against Malicious Software

- Define measures and procedures for detection, prevention, recovery, and continuous updates.
- Regularly raise user awareness to be careful and avoid using computers and equipment that may pose a risk of infection and spread of malicious software.

4.6.5. Back-up

- Regularly back up and test back-up data, including off-site back-ups, in accordance with the organization's back-up standards.

4.6.6. Network Security Management

- Define measures and responsibilities for managing operating systems, network-based applications, and information transmitted over the network to reduce risks and prevent various network threats.
- Define security attributes, service levels, management requirements for network services, internal network services, and services received from external parties for all network service agreements utilized.

4.6.7. Media Handling

- Define operational procedures and rights for managing removable media.
- Define procedures for destroying data on equipment or storage media to ensure that all sensitive information and licensed software stored on those devices or media are completely destroyed before disposal or reuse, to prevent information disclosure.
- Define operational procedures for managing, storing information, and protecting documents and applications to prevent unauthorized access, misuse, unauthorized disclosure, or leakage of critical data.

4.6.8. Exchange of Information

- Establish policies, procedures, and measures to control and prevent issues with automated office systems and the exchange of information through all communication channels, preventing unauthorized access, misuse, and data corruption during transmission outside the organization.
- The exchange of information and software with external entities must be documented in writing.
- Establish regulations for email usage to protect information transmitted electronically.

- Define policies, procedures, and methods to control the connection of the information system to external individuals or entities.

4.6.9. Monitoring

- Regularly record information usage events (Audit log), user activity, system service denial, and various error events related to information usage and/or security-related events according to the defined timeframe, and analyze them to find appropriate solutions.
- Define operational procedures to regularly check recorded access activity (Monitoring System Use) according to the defined timeframe, and establish measures to prevent unauthorized modification or destruction of recorded activity or events related to information usage.
- System administrator or related personnel work must be logged and regularly reviewed.
- All computers in the organization must have synchronized time, referenced from a correct time source, to be used as evidence for time verification.

4.7. Access Control

4.7.1. Business Requirements for Access Control

- Establish policies and procedures to control access to organizational information based on business necessity and the risks associated with accessing information assets.

4.7.2. User Access Management

- Define operational procedures and responsible units for granting various rights to new employees, as well as procedures for revoking usage rights upon resignation or internal job change.
- Define, control, and restrict system usage rights for each information system based on the job function and necessity of use, and establish a formal process for periodically reviewing user access rights.
- Implement a password management process for users to securely control password allocation.

4.7.3. User Responsibilities

- Define procedures for setting and selecting passwords, protecting unsupervised information equipment from unauthorized access, and controlling the storage of critical information assets in secure locations.

4.7.4. Network Access Control

- Define procedures and control access to company network services, specifying which services users are permitted and not permitted to use.
- External service users must be required to authenticate their identity before being allowed to access the network and information systems.
- Require network devices to have identification and authentication processes to demonstrate that the connection originates from an authorized device or location, including authenticating computers before network access.

- Define measures to prevent access to ports used for monitoring and system configuration, covering both physical protection and prevention of access via the information network.
- Define types of organizational network access, such as separating the network by groups of information services used, groups of users, and groups of information systems.
- Define network connection restrictions between the organization and external parties, considering access control and system requirements based on business needs.
- Define network routes to control connectivity and information flow on the network in accordance with the access control policy, covering shared networks and connections from client machines to server machines, to prevent the use of alternative routes.

4.7.5. Operating System Access Control

- Define operational procedures and secure controls for accessing or using the operating system.
- Require authentication before use, where users must have unique identification information for system access.
- Password management must have operational procedures and effective methods for controlling password setting.
- The use of utility programs must be appropriate, with restrictions and controls to prevent security violations or circumvention.
- Require a system to disconnect users after a specified period of inactivity or to limit usage time and connection duration for critical/high-risk information systems, including client machines that have been inactive for a period.

4.7.6. Application and Information Access Control

- Restrict access to information and various functions of the application system by separating access according to user type.
- Critical/high-risk information systems must be isolated in specifically designated areas or boundaries.

4.8. Information Systems Acquisition, Development and Maintenance

4.8.1. Security Requirements of Information Systems

- Analyze and specify security requirements or needs for new information systems or systems modified from existing ones.
- Require systems to be Straight through processing systems that avoid re-keying data or manual intervention.

4.8.2. Correct Processing in Applications. To prevent errors, loss, unauthorized changes, or misuse of information during processing, the following data correctness verification processes must be defined:

- Input Data Validation
- Control of Internal Processing
- Message Integrity

- Output data Validation
- Prohibit the export of data for external processing and re-entry into the system via manual intervention. If manual intervention is necessary due to system limitations, a regulation must be established that specifies control processes for accuracy, completeness, processing speed as required for use, preservation, confidentiality, and availability.

4.8.3. Cryptographic Controls

- Establish a policy and procedure for using cryptographic processes and programs. Critical information systems and data of the organization must be encrypted, and encryption must be strictly controlled in accordance with the procedure.
- Define encryption method standards that allow for the management of keys used to encrypt or decrypt data, and require the update of key length and character standards to be appropriate for the organization's operation and technology.

4.8.4. Security of System Files

- Define operational procedures to control the installation of various software on production systems to reduce the risk of system malfunction, by testing the software's functionality prior to installation.
- Prohibit the use of actual production data for system testing. If necessary, approval procedures, protective measures, and strict control of usage must be established.
- Control the use of libraries and restrict access to source code for production or live systems to prevent unauthorized or accidental changes.

4.8.5. Security in Development and Support Processes

- Define procedures to control changes and modifications to information systems and perform technical checks after changes to reduce the risk of system damage or unavailability. Each modification must consider measures to prevent leakage or reduce the opportunity for information to be leaked.
- If software from a vendor needs to be corrected or changed, changes must be limited to only what is necessary, and the correction must be strictly controlled.
- Define measures to control and monitor software development by external parties. Specifically, outsourcing contracts for system development must cover essential content, including agreements on copyright, system usage, system inspection, and system quality assurance.

4.8.6. Technical Vulnerability Management

- Define measures for vulnerability management and ensure that vulnerabilities are reduced appropriately and promptly to mitigate risks arising from flaws in various systems.

4.9. Information Security Incident Management

4.9.1. Reporting Information Security Events and Weakness

- Define procedures and operational methods for reporting information security events and weaknesses in the organization. Employees, contractors, or external staff must strictly follow these procedures to resolve problems quickly.

4.9.2. Management of Information Security Incidents and Improvements

- Define responsibilities and operational procedures to systematically manage information security incidents.
- Define details for incident recording, such as event type, quantity, and cost of damage, to be used as evidence and supporting data for resolving future issues.
- Collect evidence of incidents that occur to support legal proceedings, both civil and/or criminal.

4.10. Business Continuity Management

4.10.1. Information Security Aspects of Business Continuity Management

- Define necessary security details for establishing business continuity, including planning and risk analysis for operational disruption that is consistent with and comprehensive of the Information Security Policy. The plan must be tested and updated regularly to remain appropriate and current.
- Business continuity management and IT disaster recovery must comply with the organization's BCP (Business Continuity Plan) and IT Disaster Recovery Plan documents.

4.11. Compliance

4.11.1. Compliance with legal requirements

- Legal requirements, operational procedures stated in contracts (between the organization and individuals or other external parties) must be specified in writing, kept up-to-date, and consistent with the requirements. Strict control must be implemented to ensure compliance.
- Define methods to protect personal information, information related to legal requirements, operational regulations, contractual requirements, and business requirements from loss, damage, forgery, misuse of information processing equipment, or unauthorized use.
- Cryptographic control measures must be consistent with the organization's security policy and not conflict with legal requirements.

4.11.2. Compliance with Security Policies, Standards and Technical Compliance

- Define measures for supervisors to oversee and control the compliance of subordinate employees with the organization's Information Security Policy.
- Require regular auditing of information systems and technical details of systems already in use or providing services to ensure compliance with the information security policy and standards.

4.11.3. Information Systems Audit Consideration

- The information system audit must define a comprehensive and complete audit approach. The defined approach should not affect business systems and processes, or affect them as little as possible.

- The use of various tools for auditing information systems must comply with access procedures and be controlled to prevent misuse or disclosure of information to unauthorized persons.

4.11.4. Compliance with the Computer-Related Crime Act, B.E. 2550 (2007)

- Specify the requirements of the Computer-Related Crime Act, B.E. 2550 (2007), and establish related operational procedures for business operations, updating them to align with the Act.
- Provide support to protect computer systems in the organization to prevent employees from using them to cause damage, and clarify employees' responsibilities under the Act. Any violation is the direct responsibility of the employee.
- Cooperate with officials in inspecting data from computer systems and information of individuals who commit offenses under the Act.

4.12 Personal Data Controller Security Measures

Principles and Rationale

Personal Data Security means maintaining the Confidentiality, Integrity, and Availability of personal data, in order to prevent loss, unauthorized access, use, alteration, correction, or disclosure of data without authority or unlawfully. The Personal Data Protection Act B.E. 2562 (2019), the Ministry of Digital Economy and Society Announcement Re: Personal Data Security Standards B.E. 2563 (2020), and the Personal Data Protection Committee Announcement Re: Personal Data Controller Security Measures B.E. 2565 (2022) require the Data Controller to establish security measures.

The objective of security is to protect the personal data subject's right to privacy and their legally recognized power to control their personal data. For this reason, personal data security is a legal duty that requires the Data Controller to perform in order to prevent loss, unauthorized access, use, alteration, correction, or unlawful disclosure of personal data, which would lead to a personal data breach.

Personal Data Security

The Company shall implement personal data security measures covering the collection, use, and disclosure of personal data as required by law, including Administrative Safeguards, Technical Safeguards, and Physical Safeguards, as follows:

1. **Administrative Safeguards**
   1.1 Inform the Company's board of directors, executives, employees, or all levels of personnel and all types of Company temporary staff, as well as business partners, alliances, and/or Company stakeholders of the personal data security measures, and raise awareness of the importance of personal data protection for these groups to strictly comply with the established measures.
   1.2 Identify potential risks to information assets, prevent potential risks, audit and monitor threats, and personal data breach incidents, in line with the Information Security Policy. Define responsibilities for handling breach incidents and for remedying and recovering damages caused by threats and personal data breach incidents.

1.2.1 Clearly define the responsible employee and methods for reporting breach incidents to the Company's representative, such as sending an email and notifying via mobile phone in case of severe and urgent breaches.

1.2.2 Define operational methods for the Company's representative, who is responsible for notifying the Personal Data Protection Committee of personal data breaches within 72 hours of becoming aware of the incident.

1.2.3 Notification of a personal data breach under Clause 1.2.2 may be exempted if there is no risk of impact on the rights and freedoms of individuals, and a risk assessment of the impact on the rights and freedoms of individuals will be conducted.

1.3 Define user authorization or rights for accessing personal data (User Responsibilities), by defining rights in various forms such as the right to view, the right to modify/add, the right to disclose and disseminate, the right to data quality inspection, and the right to delete/destroy.

1.4 User Access Management is implemented to control access to personal data, restricting it only to authorized persons.

1.5 Provide a method for auditing historical access, changes, deletion, or transfer of personal data to be consistent and appropriate with the methods and media used for collecting, using, or disclosing personal data.

1.6 In case of non-compliance with these security measures, leading to a breach or leakage of personal data due to the Company's deficiency, the Company will notify the personal data subject of the details of the incident and a remediation plan (if any). However, the Company will not be responsible for any damages resulting from the use, disclosure, or negligence of the personal data subject or other persons with the data subject's consent.

1.7 When the period for personal data use expires or when there is no longer a necessity to retain the personal data, the Company will proceed to delete or destroy the personal data from the storage system, unless the personal data must be retained as required by law.

1.8 The Company will arrange for internal audit units to review and evaluate the effectiveness of the personal data security system.

2. Technical Safeguards

2.1 Implement a method to allow for the historical review of access, modification, deletion, or transfer of personal data, consistent and appropriate with the methods and media used for transfer of personal data, consistent and appropriate with the methods and media used for collecting, using, or disclosing personal data.

- Regularly monitor whether any items or datasets of personal data under the Company's care (as the Data Controller) have passed their retention period. This is to ensure the data

is deleted, destroyed, or rendered unidentifiable to the personal data subject, as the case may be.

2.2 Control access to personal data only for authorized persons, according to the data management rights, which include import, modification, correction, disclosure, and deletion/destruction.

2.3 Implement a data backup and recovery system to ensure continuous operation of the systems and/or various services, in accordance with the Company's information criteria and procedures.

3. Physical Safeguards

3.1 Control physical access to personal data and the equipment used for storing and processing personal data, considering usage and security. Examples include having security officers for the area, installing a CCTV system, and locking personal data filing cabinets.

3.2 Define authorized persons to access equipment used for storing or processing personal data according to their responsibilities, in order to prevent unauthorized access, disclosure, knowledge, or unauthorized copying of personal data, or the theft of storage or processing equipment.

4. Agreements between the Company and Personal Data Processors

In the event of an agreement between the Company and a Personal Data Processor, the Company will require the Personal Data Processor to implement measures in accordance with this policy to prevent the loss, unauthorized access, use, modification, or unlawful disclosure of personal data or any action performed without legal authority, and to notify the Company of any personal data breach incidents. The stringency of the measures must correspond to the level of risk or potential damage that may occur if personal data is leaked, modified, copied, or unlawfully destroyed, by implementing the following:

4.1 Assessment Before Data Delivery

4.1.1 Verify the rights, authority, and legal basis used by the individual and/or other legal entity to request the personal data.

4.1.2 Inquire about the purpose of using the data to assess the necessary level of detail for the copy (e.g., whether it is necessary to know the date of birth or house number, or if only the birth year and zip code are sufficient), and whether it is necessary to know personally identifiable data (e.g., full name, 13-digit identification number). Also, assess whether converting personally identifiable data into a new, anonymous code would be sufficient for the intended use.

4.2 Upon Data Delivery

4.2.1 Prepare new data from the raw data with only the level of detail necessary for the purpose of use.

4.2.2 Deliver the data and record the name of the data requester, contact information, date of data provision, legal basis used to access the personal data, and the purpose of use.

4.2.3 Inform the individual or legal entity that upon receipt of the data, the recipient must also perform the duties of a Personal Data Controller for the requested data, in accordance with the scope and purpose of use that was stated.

4.3 After Data Delivery

4.3.1 Periodically monitor usage to record the latest status of that data's usage. If the data is no longer necessary for the originally stated purpose, the individual or legal entity should be notified to delete or destroy the data.

4.3.2 Define methods for continuously updating the data to ensure it is current for the user's needs.

5. Sending and Transferring Personal Data Abroad

Sending or transferring personal data abroad, including storing personal data on databases in any other system where the data transferee or storage service provider is located abroad, requires that the destination country for data storage must have personal data protection standards equivalent to or better than the measures outlined in this policy.

6. Violation of the Company's Security Measures

In the event of a violation of the Company's security measures that results in a personal data breach to the public, the Company will notify the data subject promptly, as well as communicate the remediation plan for damages resulting from the breach or leakage of personal data to the public in cases caused by the Company's deficiency.

Review of Measures

The Company will arrange for a review of these Personal Data Controller Security Measures when necessary and/or when technology changes.

Disclaimer

The Company shall not be responsible for any damages resulting from the use or disclosure of personal data by a third party, including the neglect or failure to log out of the Company's database or social media system by the data subject or any other person with the data subject's consent.