BTS
GROUP

Information Security Policy (Public Version)

Table of Contents

1. Principles

The company has implemented information technology systems in its business operations for both management and internal services. Therefore, information technology systems and information are crucial. If there is insufficient care, protection, and control over the use of information, it could lead to damages related to Confidentiality, Integrity, Availability, and the provision of The company's information technology services. Thus, The company has established this Information Technology Policy to govern, control, maintain, and develop the security for information and the management system for The company's IT services to ensure they are appropriate and continuous.

2. Objectives

1) To establish guidelines for maintaining the security of The company's information technology systems.
2) To establish guidelines for the management of The company's information technology services.
3) To ensure that The company's information technology operations are efficient, appropriate, sufficient, and achieve The company's stated objectives.
4) To serve as a guideline and requirement for The company's information technology operations to be in accordance with internal controls for information technology and to comply with relevant laws, regulations, and requirements, as well as to prevent illegal acts and violations of laws, rules, and company policies.
5) To maintain the security of information in terms of Data Confidentiality, Data Integrity, Availability, and Non-Repudiation, including the prevention of Information Leakage to outside The company.

3. Definitions

No.	Term	Definition
1	Company	BTS Group Holdings PCL (BTSG)
2	Employee	Employees, hired staff, probationary employees
3	User	Employees, hired staff, probationary employees, external parties, and external service providers authorized to access information
4	Digital Solutions Department	The department responsible for overseeing The company's information technology
5	External Service Provider	A company that provides various services to support The company's operations
6	Data Center	The server and network room, primary data center, and backup data center of The company
7	Asset	Anything of value to The company that is a tangible object
8	Information	Data that is valuable to The company and must be controlled and managed
9	Information Security	The maintenance of Confidentiality, Integrity, and Availability of information, as well as other properties such as Authenticity, Accountability, Non-Repudiation, and Reliability
10	Information Technology System	The company's operational systems that utilize information technology, computer systems, and network systems to create IT systems for planning, management, and service support

No.	Term	Definition
11	Mobile Device	Laptop Computer, Smartphone, Tablet. Mobile devices are used to access, use, and store The company's information
12	Removable Storage Media	Various forms of data storage media, such as Flash Drives, External Hard Disks
13	Malicious Software	Also known as "Malware," short for Malicious Software, which refers to programs designed to attack systems, cause damage, and steal data, such as Viruses, Worms, Trojan Horses, Spyware, Keyloggers, data theft programs, and the embedding of Malicious Mobile Code (MMC)
14	Open Design	Design using a language or source code that is commonly understood and can be further developed by others, while also supporting future functionality
15	Data Masking	A measure to protect important data in a database system that is needed for testing. The database structure will resemble the production system, but the data used will be replaced with other data or characters, substituted with NULL values, or shuffled, so that it does not resemble the original data, allowing for the use of partial, non-real data
16	Social Media	A group of internet-based applications built on the ideological and technological foundations of society, allowing people to exchange user-generated content. This refers to existing market services such as Facebook, Twitter, LinkedIn, etc

4. Information Technology Policies

This Information Technology Policy covers both information technology security and the management system for information technology services, comprising the following policy points.

(1) Information Technology Policy

The company establishes, documents, and annually reviews a comprehensive set of information security policies and procedures, ensuring they are communicated to all relevant personnel and stakeholders.

(2) Organization of Information Security Policy

The company define and enforce clear roles and responsibilities for information security across the organization, including the segregation of duties to mitigate risks of unauthorized access or misuse.

(3) Human Resource Security Policy

Security responsibilities are integrated into the entire employee lifecycle, from defining roles and providing security awareness training to implementing formal processes for managing access rights during onboarding, transfers, and termination.

(4) Mobile Device Policy

Policy governs the secure use of all mobile devices, including company-provided and personal (BYOD) assets, to protect corporate data. This includes setting standards for device configuration, software, and physical security.

(5) Teleworking Policy

The company facilitate secure remote work through a formal Teleworking Policy, which mandates the use of secure connection methods, such as VPNs, and enforces access controls to protect company systems and data.

(6) Asset Management Policy

The company maintains a comprehensive inventory of all information assets, which are classified and managed according to their value and sensitivity throughout their lifecycle.

(7) Access Control Policy

Access to company networks and systems is strictly controlled based on the principle of least privilege and business necessity. This is managed through a formal user registration, review, and de-registration process.

(8) Cryptography Policy

The company implement cryptographic controls to protect the confidentiality and integrity of sensitive company data, both at rest and in transit, in line with data classification levels.

(9) Physical and Environmental Security Policy

The company implement stringent physical and environmental security controls for secure areas, such as data centers and server rooms, to protect critical IT infrastructure from unauthorized access, damage, or interference.

(10) Clear Desk and Clear Screen Policy

Employees are required to protect sensitive information in their workspace by securing documents and removable media and by logging out of systems when unattended.

(11) Operations Security Policy

The company implements formal procedures for managing IT operations securely, including change management, separation of environments (development, testing, production), and regular system monitoring and maintenance.

(12) Protection from Malware Policy

The company deploy comprehensive anti-malware solutions across our network and servers and have established procedures for employees to report and respond to suspected malware infections.

(13) Backup Policy

The company maintains a formal data backup strategy to ensure the availability of information in line with business continuity requirements, with secure storage of backup media.

(14) Communications Security Policy

Network is segmented and protected by security systems to control information flow and safeguard data during transmission.

(15) Internet Use Policy and Social Media Use Policy

Acceptable use policies are in place to ensure that internet and social media are used responsibly, securely, and in a manner that protects The company's reputation and assets.

(16) E-mail Policy

The use of The company email system is governed by a policy that outlines acceptable use, security measures against threats, and proper handling of company information.

(17) System Acquisition, Development and Maintenance Policy

Security is a core requirement throughout the system development lifecycle (SDLC). The company follows principles like Defense-in-Depth, Privacy by Design, and secure coding standards for all in-house and third-party developed systems.

(18) Information Technology Incident Management Policy

The company has a formal incident management process to ensure timely and effective detection, response, and resolution of information security incidents to minimize business impact.

(19) Supplier Relationships Policy

The company manages security risks associated with third-party suppliers by defining security requirements in contracts, controlling their access to company information, and regularly monitoring their performance.

(20) Change Management Policy

A formal change management process is implemented to ensure that all changes to IT systems are assessed, approved, and deployed in a controlled manner to prevent adverse impacts on security and services.

(21) Information Security of Business Continuity Management Policy

Information security requirements are integrated into our business continuity management to ensure that information assets remain protected and available during and after a disruption.

(22) Compliance Policy

The company is committed to complying with all applicable legal, statutory, regulatory, and contractual requirements related to information security. The company conducts regular risk assessments and audits to ensure ongoing compliance.

(23) Media Handling Policy

The company has established measures for the secure handling, storage, and transport of all types of media containing company information to prevent data loss or unauthorized disclosure.

(24) Media Disposal Policy

When media is no longer required, it is securely disposed of using methods that ensure the stored data is irrecoverable.

(25) User Registration and De-Registration Policy

A formal procedure governs the entire lifecycle of user access, from registration and granting of privileges to the timely revocation of access upon termination or change of role.

(26) Password Management Policy

The company enforces a robust password management policy that mandates strong complexity, regular changes, and account protection mechanisms to secure user access to all information systems.

(27) Capacity and Performance Policy

The company continuously monitors and manages the capacity and performance of our IT services to ensure they consistently meet current and future business demands.

(28) Clock Synchronization Policy

All company servers and systems are synchronized to an authoritative time source to ensure the accuracy and integrity of time-stamped records for security and operational purposes.

(29) Technical Vulnerabilities Management Policy

The company proactively manages technical vulnerabilities through a defined process of regular monitoring, assessment, and remediation to protect systems from emerging threats.

(30) Information Transfer and Exchange Policy

Procedures are in place to govern the secure transfer of information, both internally and with external parties, ensuring that data is protected in accordance with its classification.

(31) Information Retention Policy

The company defines and implements controls for the secure retention of data and documents in compliance with legal, regulatory, and business requirements.

(32) Threat Intelligence Policy

The company collects and analyzes threat intelligence to proactively identify and understand potential security threats, enabling us to enhance our defensive posture and mitigate risks.

(33) Information Security for Use of Cloud Services Policy

The use of cloud services is governed by a policy that includes a due diligence process for selecting providers and ensures compliance with our security standards.

(34) Data Masking Policy

Where appropriate, data masking techniques are used to protect sensitive data in non-production environments, such as testing and development.

(35) Data Leakage Prevention Policy

The company implements technical and procedural controls to identify, monitor, and prevent the unauthorized disclosure or leakage of sensitive company data.

(36) Configuration Management Policy

The company maintains secure baseline configurations for critical hardware, software, and network devices, and manages changes through a formal process to prevent unauthorized modifications.

5. Risk Management Policy

The company has established a formal information security risk management framework. The company conducts regular risk assessments and implements appropriate treatment plans to manage risks to an acceptable level.

6. Internal Audit Policy

An internal audit program is in place to independently assess the effectiveness and compliance of our information security controls and management system on an annual basis.

7. Criteria for Exemption from Information Technology Security Policy and Standards

A formal process exists for requesting temporary, risk-assessed exemptions from security policies. All exemptions require justification, are granted for a defined period, and must be approved by authorized management.

Reviewed By	Reviewed By	Approved By
....	....	....
(Chirawadi Wisetcharoen)	(Veerapa Rodjanapiyavong)	(Rangsin Kritalug)
Digital Solutions Department Manager	Assistant to Chief Operating Officer	Chief Operating Officer