Policy on Security of Data and Computer System
Thai Wacoal Public Company Limited

Introduction

Thai Wacoal Public Company Limited has established an information technology and communication system to facilitate the executives' administration and the staff's operations. This will assist the company in maintaining its efficiency, security, and reliability, as well as the continuity of its business operations.

The company recognizes the pivotal role of Artificial Intelligence (AI), a technology endowed with strategic potential and a key driving force in industrial and societal transformation worldwide. Of particular importance is Generative AI technology, which possesses the capability to create diverse types of content, such as text, images, videos, audio, or source code. This technology can assist in reducing operational time and increasing efficiency.

However, the deployment of AI and Generative AI systems (hereinafter referred to as "AI Systems") presents complex challenges and risks. These threats are not limited to traditional cyber threats but also include threats specific to AI systems themselves.

Therefore, maintaining the confidentiality, accuracy, and integrity, including the availability of business data and information technology systems, and AI systems, is vital. It also builds confidence for customers and partners, as well as complies with the requirements of relevant laws such as the Computer-related Crime Act or the personal data protection laws, etc. The company, therefore, sets a policy on the security of data and computer systems and practices for maintaining information security as a code of conduct.

1. This policy, to be strictly adhered to, is intended for employees or third parties allowed access by the company to the network system and computers, and the company's information system, and AI systems, including the Internet connection through the company's network system and computers.
2. The company operates under Thai law. Therefore, the use of the company's network system and computers, including the Internet connection, shall be in accordance with applicable computer crime laws and other related laws.

.../ 2

3. Computer systems, computers, and connecting equipment are the property of the company and are provided for services related to the company's business only.
4. The Company reserves the right to inspect, collect evidence and take proper action, if any violation of the policy on security of data and computer systems is found.

Section 1

Definitions of terms

1. **"Company"** means Thai Wacoal Public Company Limited.
2. **"Supervisor"** means the authorized person who dictates under the company's administrative structure.
3. **"Employee"** means a person who the company has hired and assigned to perform duties as specified by the company.
4. **"Data Administrator"** means an employee assigned by the company to be responsible for maintaining computer data systems, who can access the computer system program to manage the database and has been assigned to be responsible for developing, modifying, improving and maintaining data systems and various programs related to the data systems used in the company.
5. **"Network and Computer Administrator"** means an employee assigned by the company to be responsible for the maintenance and development of network system and computers, who can access computer network programs to manage databases of network systems and computers.
6. **"Software and hardware developer"** means an employee assigned by the company to be responsible for designing, creating, and planning software programs or applications or hardware development focusing on programming using any programming language.
7. **"Information Technology Center Officer"** means an employee assigned by the company to be responsible for maintaining and developing the company's information technology system, working under the departments according to the structure determined by the division director of the information technology center.
8. **"Third-party"** means a person who is not subordinate to the company, but who is entitled to access and use the company's information technology and communication systems under the specified rights nd duties.

.../3

9. **"Information Technology Center"** means a unit according to the company's structure, being in charge of information technology work, and serving as the center for study, analysis, and development of the company's information technology and communication systems.
10. **"Data"** means things that convey meanings to inform facts, matters, or whatever, notwithstanding, the meaning conveyance is done by itself or through any means, and whether it is made in the form of documents, files, reports, books, plans, maps, drawings, photographs, films, visual or audio recordings, computer recordings or any other means can make the recording appear visible.
11. **"Information system"** means the company's computer programming system, which involves storing (importing), managing (processing), and distributing (displaying) data and information to support the working mechanism of the company.
12. **"Computer system"** means a device or a set of computer equipment that connects working operations by specifying instructions, command sets, or any others, and operational guidelines for equipment or a set of devices to automatically process data.
13. **"Network and computer system"** means computers, which are an asset of the company, including peripheral devices and network equipment that interconnects various computers within the company, as well as, links remote computers together.
14. **"Assets"** means hardware, software, data, information technology, and communication systems under the supervision of the Information Technology Center.
15. **"Account"** means a list of authorized users to use the company's computer system and communication network.
16. **"Username"** means a set of letters or numbers that are assigned for logging in to use the computer system and communication network of the company for which the provisioning have been determined.
17. **"Password"** means letters, characters, or numbers put all together to use as a tool for authentication to control access to the company's information technology and communication systems.
18. **"Login"** means the process by which users access the company's computer system and communication network, which normally requires correctly entering a username and password.
19. **"Logout"** means the process that users perform to terminate the usage of the computer system and the company's communication network system.
20. **"Authentication"** means a security procedure for accessing the system. It is a step to authenticate the user's identity; normally, the proof is done by using a username and a password.
21. **"Internet"** means a communication network that connects the company's computer systems to the Internet worldwide.

.../4

22. **"Download"** means bringing a file or data from another computer to the computer we use via the Internet.
23. **"Upload"** means transferring a file or data from the employee's computer to the Internet or transferring the file to other computers that have been connected.
24. **"Log file"** means information regarding communications of a computer system, which represents the source, origin, destination, route, date, quantity, duration, and other types of services involved in the communication of a computer system.
25. **"Hardware"** means a set of components that make up a computer system. Computer hardware includes physical components such as a monitor, mouse, keyboard, computer storage, hard disk, VGA card, sound card, RAM, motherboard, etc., which are all tangible.
26. **"Software**" means a set of commands or programs directing a computer to run in the sequences of the specified steps to get the results that computer users want. The software handles and controls computer processing from powering on until powering off.
27. **"Application"** means a program or a set of commands used to control the operation of a computer and various peripheral devices to work according to the command and meet the needs of users.
28. **"Electronic mail" (e-mail)** means a system that personnel uses to send and receive messages between linked computers and communication networks. The information sent can be text, photographs, graphics, animations, sounds, etc., and the sender can send the message to one or more recipients. The standards used in this type of data transmission are, for example, SMTP, POP3, and IMAP.
29. **"Malware"** means computer programs, a set of commands, and/or electronic data designed to directly or indirectly disrupt or damage the company's information technology and communication systems. It causes a malfunction or works not per the specified commands, such as computer viruses, Spyware, Worms, Phishing, Trojan Horse, Mass Mailing, etc.
30. **"Artificial Intelligence (AI)"** means the technology developed to enable the processing systems of computers, robots, machinery, or electronic devices to possess attributes or behaviors that are similar to humans, in accordance with objectives defined by humans, such as learning, perception and response to environmental stimuli, reasoning, and problem-solving.
31. "**Generative AI**" means a type of AI technology capable of creating new content in various formats based on text or commands (prompts) provided by humans. This includes, but is not limited to, text, images, videos, source codes, or other formats.
32. **"Personal Data"** means information related to an individual that can directly or indirectly identify that person, excluding data of deceased individuals in particular.

.../ 5

33. **"Sensitive Personal Data"** means the personal data as defined under Section 26 of the Personal Data Protection Act B.E. 2562 (2019), including race, ethnicity, political opinions, religious beliefs or philosophies, sexual behavior, criminal history, health information, disabilities, union membership, genetic information, biometric data, or any other data that impacts the data subject in a similar manner, as stipulated by the Personal Data Protection Committee.

Section 2

Practices for system use

1. Practices for the use of network and computer systems

1.1 The company has operated in accordance with applicable laws. Therefore, the company's use of the network and computer systems, including data systems and the Internet, must comply with the laws on computer-related crime and other relevant laws.

1.2 The company does not support or allow employees or third parties to violate computer-related crime laws and other related laws.

1.3 The company's network system and computers are available to provide services related to the Company's operations only and is not allowed to be used in other businesses irrelevant to the Company's operations.

1.4 Access to the company's network system and computers shall follow the procedures determined by the company for obtaining access permission through the required registration.

1.5 Requesting access permission requires approval by the employee's direct supervisor and following the procedures set by the company.

1.6 The use of the company's network system and computers must be done only through the company's computer.

1.7 The use of the company's network system and computers from a computer that does not belong to the company requires prior permission from the network and computer system administrator and if any unauthorized use is found, the network and computer system administrator may immediately eliminate the use from the company's network system and computers.

.../6

1.8 The company reserves the right to withdraw the company's network system and computers services without prior notice.

2. Practices for the use of information systems

2.1 Upon any data system development or revision, data administrators shall have collaborative testing with employees before implementation.

2.2 The use of the data system shall comply with the provisioning that the data administrator has agreed upon with the employees according to the established provisioning table approved by the supervisors in the administrative line and the division director of the information technology center.

3. Guidelines for Using AI Systems.

3.1 **Acceptable Usage of AI Systems:**

Users must study and understand the information, capabilities, benefits, risks, and limitations of each type of AI system. They should apply these systems appropriately to support the company's operations within the specified context, which includes but is not limited to:

1. Data analysis and report generation.
2. Writing commands or programs.
3. Drafting letters or documents, such as memos, policies, etc.
4. Providing preliminary advice or guidance for problem-solving.
5. Creating content for internal communication or promotional materials.
6. Performing other tasks assigned by supervisors.

3.2 **Prohibited Usage of AI Systems:**

AI systems must not be used in a manner that could cause harm to individuals, the company, society, or the nation, particularly in the following cases:

1. Replacing human judgment in high-risk decisions, such as legal, financial, or decisions affecting life, property, or individual rights.
2. Creating false information or content that could harm individuals, the company, or society.
3. Disclosing or using confidential company information, internal documents, or data that could impact operations.

.../7

4. Using personal data without the owner's consent, or data that may be non-compliant with the Personal Data Protection Act B.E. 2562 (2019) or other relevant laws.
5. Creating intellectual property infringement content (copyrights, patents, trademarks), including unauthorized copying, replication, or modification.
6. Developing tools or content that are directly harmful, such as creating deepfake materials for malicious attacks or writing code to develop malware or computer viruses.

3.3 **Data Confidentiality and Security in Using AI Systems:**

1. Prohibits using internal company data or confidential information (e.g., passwords, contract documents, sensitive memos) in AI systems, especially in public or free services where data may be recorded and used to train AI models.
2. If necessary to use AI with confidential or sensitive personal data, users must employ only AI systems authorized by the company, with consent from data owners and approval from the relevant department director.
3. Refrain from using data that could threaten the security of information systems, such as passwords or API keys, in conjunction with AI systems.
4. All source code generated by AI systems must be thoroughly checked for correctness and vulnerabilities before deployment.
5. In the event of security breaches involving AI systems, immediate reporting to supervisory authorities and following incident management procedures are required.

3.4 **Roles and Responsibilities in Using AI Systems:**

Users and individuals involved in applying AI systems bear important responsibilities, including:

1. Users must verify and take responsibility for final decisions and outcomes based on AI-generated data, particularly concerning accuracy, legal impact, and confidentiality before use or dissemination.
2. Immediately report any errors or potentially negative results from the AI system to supervisors.
3. Clearly specify when using content generated by AI, such as noting "This content was created or assisted by AI technology," to ensure transparency.

.../8

Section 3

Practices for Employees

1. This policy on the security of data and computer systems is deemed to be part of the operational requirements. Employees who access the company's network system and computers must accept and acknowledge the policies or regulations set up by the company, without any excuses for non-acknowledgment of those policies or regulations. Furthermore, employees must comply with the policies, requirements, provisions, and instructions set by the company, including those that will be set in the future, and in case of non-compliance, it shall be deemed a violation of the company's regulations.
2. All employees have the right to use the network system and computers, as well as the information system. Any violation that causes or may cause damage to the company or any person will be considered by the company as appropriate for taking disciplinary and legal action against the employees who cause such violations.
3. The company provides the registration of user accounts, composed of individual usernames and passwords, to employees whose duties involve the use of networks and computers, information systems, and the Internet system, with rules for using passwords such as the number of characters must be no less than 8 characters and should not be easy-to-guess words, and the password changing period is every 90 days or as deemed appropriate for such a system. Employees who access the network system and computer must log in for their own authentication, and when they finish working, they must always log out of the system for the sake of the safety of the whole system and the preservation of rights to use the domain and employee data documentation.
4. The passwords of employees are deemed assets of the company. It is prohibited to disclose passwords, which are considered personal information, to others as well as to jointly use a common username and password. However, in cases of necessity, it is required to obtain approval in writing from the supervisor. Meanwhile, all employees have a duty to strictly protect their passwords.
5. Employees may be assigned to access other systems specified by the company. They must comply with the system usage rules and keep their username and password confidential, not disclosing them to others unless written approval from the supervisor is given.
6. If any user account is canceled, the employee shall notify the supervisor and apply to cancel the user account immediately after the termination of use.

.../9

7. Employees should use the company's network system and computer resources effectively, not causing network and computer density, not downloading or uploading data or anything else irrelevant to the work, or not using any website irrelevant to the work or operations of the company.
8. Employees shall use polite messages, and/or use messages in a way that a reasonable man should use in messages sent to others, including performing properly according to the practice of network system and computer usage at the company.
9. Employees are responsible for exercising caution when using the company's network system and computers; specifically, third parties are not permitted to access the network system and computers through their own user accounts.
10. For preventive purposes, in case other people, know and misuse the password of employees and cause damage to the company, employees shall keep the password confidential, not write down the passwords where they can be easily seen, and not use a computer program to save the password for the personal computer that the employee possesses.
11. Computers and peripheral equipment are deemed the asset of the company. Employees are responsible for maintaining them in perfect condition and making them normally usable, and shall refrain from any acts that could cause damage or unsure of safety.
12. Employees are prohibited from installing or modifying computers and computer network equipment, or developing software programs and hardware, including system resources, for use in reducing the capacity of the system, breaking security mechanisms, or to gain more resources, or to attempt changing the limitation of access rights to system resources from those permitted.
13. For the safety of computer network system usage, if any employee encounters a computer virus, it shall be notified to the information technology center staff to remove the computer virus as soon as possible.
14. Employees should delete unnecessary data from their personal computers in order to save the memory on the storage media.
15. Employees should cooperate and facilitate network and computer administrators to check the security of the network system and computers as well as complying with the recommendations related to the security of the company’s network system and computers.
16. Employees are prohibited from using the company's network system and computers for the following;

.../10

16.1 Acts for any purpose other than the operational objectives or as permitted by the company, such as benefiting one's own or others' businesses.

16.2 Breaking the law or causing harm to others.

16.3 Acts that are detrimental to public order or morals.

16.4 Trading or profiting or for personal benefit.

16.5 Disclosure of Confidential Information derived from working for the company, whether it is the information of the company, employees or third parties.

16.6 Acts of infringement or unauthorized access to other people's computer resources connected to a network system, computers, or the Internet.

16.7 Acts that infringe on the intellectual property of the company or others.

16.8 Acts to obtain another person's information without permission from the proprietor of the information or the person who has the right to such information.

16.9 Receiving or transmitting information that causes or may cause harm to the company or others, such as importing or forwarding false information, receiving or transmitting information in the form of a chain letter, receiving or transmitting information in a manner that violates the law or violates the rights of others, and so on.

16.10 Acts for dissemination, editing, or alteration by electronic means or any other means that cause damage, disrepute, or humiliation to the company or other persons.

16.11 Interfering with the use of other employees' network system and computers or causing the company's network system and computers to be unusable normally.

16.12 Expressing personal opinions about the company's operations on any website in a way that may lead to misunderstandings or cause harm to the company or other people.

16.13 Any other acts that may be contrary to the company's interests or that may cause conflict with or damage to the company.

17. Access to software, programs, or applications must be authorized and approved by the employee's supervisor, and the software, program, or application must have legitimate copyright.

18. Employees are prohibited from installing any software, programs, or applications on the computer, including other peripheral devices other than those provided by the company. In cases of necessity, for additional use, it should be notified to the staff of the information technology center to operate with the permission and approval of the employee's direct supervisor.

.../11

19. Emails of the company (@wacoal.co.th) shall be used only for the business of the company. Employees are prohibited from sending e-mail that causes spam or junk against other people's networks and computers or attaching a file that contains a computer virus, unnecessarily disguising or spreading it to other people, which may cause damage to the recipient or affect the overall network and computer system. If any employee violates the use of e-mail in an improper way other than for the working operation of the company, if the action is contrary to the applicable laws and there is an offense according to the regulations of the company, such employee shall be responsible for any damage incurred.
20. The rights to search and retrieve resources from the company's data system, network system, and computers are provided only for employees. Such rights may be granted to third parties only at the discretion of the supervisor.
21. Use of the company's network system and computers must be in accordance with the company's policy on data and computer system security and computer crime laws, as well as other related laws.
22. All employees who have access to the company's network system and computers, are required to strictly adhere to the requirements, procedures, and practices for using the network system and computers.
23. If any transmission of information that violates the Computer Crime Act and other related law it is found, it shall be notified to the supervisor and network and computer administrators, or staff at the information technology center.

Section 4

Practices for information technology center staff

1. Practices for network and computer administrators

1.1 Being in charge of supervising, maintaining, and improving the network system and computers of the company to be always functional. In case of any malfunction in the system, the network and computer administrators are entitled to suspend the use of the network system and computers to prevent damage.

.../12

1.2 Being in charge of inspecting the use of the company's network system and computers to comply with the security policy of information and computer systems, or the order of the division director of the information technology center to suspend the use of the network system and computers of employees, in the event that may cause damage to the company.

1.3 Refraining from exercising their authority to access, receive, or send data transmitted through the company's network system and computers, not having their own right to access such information, and refraining from disclosing information that they have obtained from or due to the duty of network and computer system administrators, which is not allowed to be disclosed to any person.

1.4 Storing and maintaining computer traffic data (Log) in compliance with the computer crime law and other related laws.

1.5 Calibrating the Universal Standard time for the computer system in accordance with the applicable law.

1.6 Supervising software and various programs installed on employees' computers to be in accordance with the copyright of the software or installed programs.

1.7 Performing other duties related to the company's network system and computers as assigned by the Director of Information Technology Center.

1.8 The company respects the privacy rights of all employees and reserves the right for the assigned network and computer system administrators to inspect the use of the network system and computers of employees in accordance with this policy.

2. Practices for Data Administrators

2.1 Developing, improving, and maintaining information systems, including specifying safety requirements.

2.2 Determining the provision of the information system prior to usage.

2.3 Controlling software installations into the information system or on employees' computers without affecting the main system or causing damage to the overall system.

2.4 Suspending the use of the employee's information system, when any improper use, violation of the terms of use, or illegal use is found.

2.5 Performing other duties related to information systems as assigned by the division director of the information technology center.

.../13

3. **Practices for Software and Hardware Developers**

3.1 The company supports research to enhance academic knowledge on software and hardware for software and hardware developers, provided that the software and hardware do not affect or cause problems with the network system or computers, and the company shall own the copyright in any program, command set, software, or hardware developed by the software and hardware developer while working as an employee of the company.

3.2 Do not develop any program, command set, software, or hardware to destroy the security system for the company's network system and computers, causing it impossible to use normally, including not acting in a manner of secretly using a password, stealthily copying others' data, cracking others' passwords, or generating authority and priority to possess resources in the network system and computers, including control of screens, keyboards, mice, and data stored on computers of other companies.

3.3 It is prohibited to develop any program, command set, software, or hardware that will duplicate the program or disguise the program with other programs, in the same manner as malware or computer viruses, or programs that will destroy information systems, network systems, and computers, or restrict the right to use the company's software.

3.4 Information Technology Center staff, who are in charge of website development, shall not present illegal information, infringe copyright and intellectual property rights, or show inappropriate messages or images, or those contrary to good morals and traditions.

3.5 The Information Technology Center staff, in charge of developing websites related to Web boards or Web blogs, shall inspect, access, and store the computer traffic data (Logs) as required by applicable law.

This Security Policy for Data and Computer System shall be deemed as part of the work regulations of Thai Wacoal Public Company Limited and shall announce to employees for acknowledgment and compliance, including for inspection and control for strict compliance with this policy. If there is any violation, ignorance, nor uncompliance, such acts shall be subjected under disciplinary measures in accordance with the work regulations.

.../14

This Security Policy for Data and Computer System has been approved by the resolution of the Board of Directors' Meeting No. 1/2026 on January 28, 2026 and effective from February 1, 2026 onwards, thus, the policy and regulations for the use of computer systems, dated January 1, 2025 shall be cancelled.

Thamarat Chokwatana

(Mr. Thamarat Chokwatana)

Chairman