ORNSIRIN

Information Security Incident Reporting and Management Policy

1. Objective

This Information Security Incident Reporting and Management Policy (the "Policy") is established to provide guidelines for handling incidents related to information security within Ornsirin Holding Public Company Limited and its subsidiaries (collectively referred to as the "Ornsirin Group"). The Policy applies to incidents that have occurred, are likely to occur, or are suspected to occur, which may result in personal data breaches, in accordance with the definitions set forth below.

2. Scope of the Policy

This Policy applies to all employees, contractors, agents, representatives, interns, and other personnel of Ornsirin Holding Public Company Limited and its subsidiaries (collectively, the "Ornsirin Group"). In addition, the Ornsirin Group requires its business partners, vendors, and service providers—including their respective employees, workers, contractors, agents, representatives, and other personnel who collect, access, store, or otherwise process personal data on behalf of the Ornsirin Group (collectively referred to as "Personnel/Contractors") to comply with this Policy. This Policy does not create any rights for Personnel/Contractors nor impose any obligations on the Ornsirin Group beyond those required under applicable laws. It is an internal document of the Ornsirin Group and does not grant any rights or privileges to external parties.

Any violation of this Policy may result in disciplinary action, including termination of employment, or termination of contracts with business partners, vendors, or service providers, as applicable.

The Ornsirin Group reserves the right to amend or update this Policy from time to time and will notify Personnel/Contractors as appropriate.

3. Information Security Incident Reporting Requirements

3.1 Any employee or contractor who identifies, suspects, or becomes aware of an information security incident—whether it has occurred, is likely to occur, or is suspected to occur—must report the matter immediately to the Information Security Incident Management Team (contact details are provided in Clause 3.4 of this Policy). The report must be submitted using the Information Security Incident Reporting Form as specified in Appendix 1.

3.2 An information security incident refers to any actual, potential, or suspected event, action, failure, or circumstance that results in the destruction, loss, alteration, or compromise of data owned, controlled, or maintained by Ornsirin Holding Public Company Limited and its group companies, whether directly or indirectly (including data managed by business partners, vendors, or external service providers). Such incidents may occur accidentally, intentionally, or unlawfully, and may result in unauthorized access, disclosure, or acquisition of paper-based or electronic information, regardless of whether such data constitutes personal data or confidential information. This includes, but is not limited to, data stored in physical files, emails, spreadsheets, personnel records, payroll records, servers, portable storage devices (e.g., computers, laptops, or smartphones), and IT databases.

The following are illustrative examples of incidents that must be reported to the Information Security Incident Management Team

• Theft or loss of computers, laptops, smartphones, USB drives, external hard drives, or any other data storage devices belonging to Ornsirin Holding Public Company Limited or used by employees/contractors to store Company-related data

• Unauthorized intrusion or theft occurring within the Company's premises

• Cyberattacks or any unauthorized activities that pose risks to the Company's systems, including databases, computers, or communication networks

• Situations where employees/contractors access, view, or disclose data, files, or databases beyond their assigned responsibilities

• Breach of non-disclosure agreements (NDA) or confidentiality obligations by external parties.

• Any of the above incidents occurring in connection with business partners, vendors, or service providers of the Ornsirin Group

3.3 Cooperation, Employees/Contractors are required to fully cooperate with Ornsirin Holding Public Company Limited and the Information Security Incident Management Team in the investigation of any information security incidents.

3.4 Information Security Incident Management Team

Information Security Incident Management Team	
Contact Information	Email : PDPA@ornsiril.co.th Telephone : 053-295709
Team Members	
Incident Manager (Primary Contact)	Data Protection Officer (DPO) Nongnuch Kesorn Tel: 085-7047235
Information Technology Department	Kanjana Sriwichai Tel: 094-6344490
Legal Department	
Human Resources Department	Channarong Toonkaew Tel: 085-9519995
Accounting Department	Chatchaiyong Boonkwang Tel: 087-7270324

3.5 The Information Security Incident Management Team shall maintain continuous monitoring on a 24-hour basis. The primary Incident Manager can be contacted immediately via: Email : Nongnuch.t@ornsirin.co.th Telephone: 097-9695164 This ensures that incidents can be reported and responded to without delay.

4. Information Security Incident Management Procedures

Phase 1: Internal Reporting and Incident Confirmation

The objective of Phase 1 is to promptly identify and confirm whether an information security incident has actually occurred and to ensure timely reporting to the Information Security Incident Management Team.

4.1 Initial Assessment: The Information Security Incident Management Team shall designate an assigned individual to conduct preliminary investigation and assessment for each reported incident (the "Primary Incident Manager").

The **Primary Incident Manager** shall coordinate with the employee/contractor who reported the incident and gather as much relevant information as available at that time. Where the incident relates to information technology or other computer security matters, the Primary Incident Manager must coordinate with the Information Technology Department and the Information Security Incident Management Team accordingly. In addition, the Primary Incident Manager shall conduct an initial assessment as soon as possible, and within the first 24 hours, to determine whether there are reasonable grounds to believe that the incident has actually occurred. If there are no reasonable grounds at that time, the Primary Incident Manager shall prepare an internal report, including the following details:

- Name of the employee/contractor who reported the incident
- Description of the reported information security incident
- Explanation of the reasons why the Primary Incident Manager has determined that there are no reasonable grounds to believe that the incident has occurred or may occur

The Primary Incident Manager shall prepare a written report and submit it to other members of the Information Security Incident Management Team immediately upon obtaining sufficient information.

4.2 If the Primary Incident Manager determines that there are reasonable grounds to believe that an information security incident has actually occurred, the Primary Incident Manager must immediately notify other members of the Information Security Incident Management Team in order to proceed to Phase 2 without delay.

Phase 2: Information Security Incident Management

The objective of Phase 2 is to manage information security incidents both internally and externally. During this phase, the incident must be assessed as quickly as possible to enable the Ornsirin Group to make timely notifications where required, including reporting to government authorities, individuals, or other relevant parties in accordance with applicable laws.

At the same time, the Information Security Incident Management Team shall take all necessary actions to control the incident, mitigate risks, and minimize potential damage.

4.3. Threat Containment: Where the incident constitutes a persistent or ongoing threat (e.g., cyberattacks, hacking, or malware affecting the Company's information systems), the Information Security Incident Management Team shall ensure that appropriate security measures are implemented by relevant personnel, including the Information Technology Department, to isolate and contain the threat and prevent further impact on the Company's technical environment.

4.4 Incident Documentation: The Information Security Incident Management Team shall maintain detailed records of all actions taken from the detection of the incident through investigation, clarification, and resolution.

4.5 Evidence Preservation: During the investigation, the Information Security Incident Management Team shall implement appropriate measures to preserve relevant data and evidence, including

- Preventing deletion, alteration, or destruction of data (including system logs, backup overwrites, or data reuse)
- Instructing employees/contractors with system access to exercise caution to avoid modifying or damaging relevant data and evidence

- Securing suspicious codes or malware
- Taking legal actions in accordance with applicable laws and the policies of Ornsirin Holding Public Company Limited, where applicable

4.6 Digital Forensics: The Information Security Incident Management Team shall assess, on a case-by-case basis, whether it is necessary to engage forensic examiners or external forensic service providers to document affected equipment, conduct forensic analysis on computers, or perform other related services. Such forensic activities shall be supervised and controlled by the Legal Department or external legal counsel providing legal advice to the Ornsirin Group, particularly in cases where legal proceedings, investigations, or internal inquiries are anticipated.

4.7 Confidentiality: The Information Security Incident Management Team shall coordinate with relevant departments to ensure that all information security incidents are treated as confidential until a decision has been made regarding disclosure or communication. Access to incident-related information shall be strictly limited to only those employees/contractors who have a need to know, in order to prevent unauthorized disclosure or data leakage.

4.8 Assessment of Incident Scope: The Information Security Incident Management Team shall assess and gather relevant information regarding the scope of the information security incident, including, where appropriate:

- Date, time, and nature of the incident
- Categories of personal data potentially affected
- Risks of damage, misuse, or unauthorized use
- List of individuals who are aware of the incident, whether internal or external to Ornsirin Holding Public Company Limited

The Information Security Incident Management Team may use the following checklist to support the assessment

- What is the nature of the incident (e.g., data breach, loss of devices, insider theft, or similar events), and how was it detected?
- What type of data is affected, and what is the scope of the affected data? Does it trigger any legal or contractual notification obligations?
- Who are the affected individuals (e.g., customers, employees, or other parties)?
- Where are the affected individuals located (e.g., within Thailand only or also in other jurisdictions)?
- Can the Company estimate the type and volume of personal data affected?
- What is the extent of the incident? In cases of unauthorized system access, which hosts were accessed, what data was involved, and what methods were used by the intruder?
- Has the incident been disclosed to the media?
- What measures have been taken to secure the systems without compromising critical electronic evidence (e.g., disconnecting affected servers from the internet, capturing forensic images of impacted devices)?
- Who is responsible for managing the technical and security aspects of the incident, and has the Company engaged external IT or forensic service providers?
- Are there any additional internal stakeholders who should be informed (e.g., senior management, corporate communications)?

- Have law enforcement authorities been contacted? If so, which authorities and by whom?

4.9 Reporting to Law Enforcement Authorities: As part of the investigation process, in cases where there is unauthorized access to the data or information systems of Ornsirin Holding Public Company Limited, the Information Security Incident Management Team shall assess whether it is necessary or appropriate to report the incident to relevant law enforcement authorities.

4.10 The Legal Department shall apply the analytical framework set out in Appendix 3 to advise the Information Security Incident Management Team on applicable data breach notification laws (the "Summary of Data Breach Notification Laws") (see Appendix 2), and determine whether the incident constitutes a reportable data breach. The Legal Department shall further advise whether notification is required to affected individuals, government authorities/regulators, or any other relevant parties.

The Information Security Incident Management Team shall provide accurate and complete information as requested by the Legal Department to enable proper legal assessment and advice.

4.11 Consideration of Other Requirements

In addition, the Legal Department may advise the Information Security Incident Management Team on other applicable requirements beyond data breach notification laws that may necessitate reporting of information security incidents. These may include:

- Applicable laws and industry-specific regulations relevant to the incident
- Contractual obligations with business partners or other third parties
- Personal data protection policies, notices, or other internal and external communication documents
- Public commitments or non-binding policies of Ornsirin Holding Public Company Limited that have been disclosed to the public.

4.12 Reporting to Government Authorities, Individuals, or Other Parties

(a) Content of Reports, Statements, and Q&A Scripts : The Information Security Incident Management Team shall coordinate with the Legal Department to determine the appropriate wording and communication approach for reports, statements, and Q&A scripts, ensuring compliance with applicable requirements.

Where the Information Security Incident Management Team decides to assign Company personnel or engage external call center services to respond to inquiries from affected individuals, the team must prepare standardized scripts. These scripts shall be used by call center personnel or designated Company representatives to ensure accurate, consistent, and appropriate communication regarding the information security incident and related matters.

(b) Form of Notification, Where applicable laws do not prescribe a specific form of notification to affected individuals, the Ornsirin Group may consider the following approaches:

- For individuals who have provided an email address, the Information Security Incident Management Team shall send notification via email to all affected individuals and request acknowledgment of receipt
- For individuals who have provided a postal address but no email address, the Information Security Incident Management Team shall send notification via registered mail with acknowledgment of receipt

The Information Security Incident Management Team shall coordinate with the Legal Department to determine the most appropriate method of notification, taking into account applicable legal requirements and associated costs. This Policy does not require public disclosure through other channels (such as the Company's website or national media), unless required by applicable data breach notification laws or where the Ornsirin Group determines that such disclosure is appropriate for customer relations or other purposes on a case-by-case basis. If notification cannot be made in accordance with the above, the Information Security Incident Management Team shall consult the Legal Department immediately to determine alternative notification methods.

Notwithstanding the above, notification may be delayed if law enforcement authorities determine that such disclosure could impede an ongoing investigation.

4.13 Handling of Inquiries: The Information Security Incident Management Team shall establish a clear approach for responding to inquiries from the media, government authorities, or other parties. In most cases, such inquiries should be referred directly to the Legal Department or the Corporate Communications/Public Relations function for assessment and preparation of appropriate responses, ensuring consistency, accuracy, and compliance with applicable requirements.

Phase 3: Post-Incident Measures

4.14 Documentation Requirements: Regardless of whether data breach notification laws are deemed applicable to the information security incident, the Primary Incident Manager shall prepare formal documentation of the incident. In particular, the documentation should include the assessment results supporting the decision not to apply data breach notification laws, where applicable.

4.15 Remedial Measures: The Information Security Incident Management Team shall coordinate with the Legal Department and the Information Technology Department to establish necessary technical and organizational measures to prevent recurrence of similar incidents. Such measures may include: Review and update of policies and proceduresU ,Training and awareness programs for employees/contractors, Enhancement of internal processes and controls.

In addition, the Information Security Incident Management Team shall assess relationships with external parties involved in the incident and take appropriate actions, such as: Contract amendments, Process improvements, Additional training, Strengthening of security measures, Selection of alternative vendors and where appropriate. External parties shall be contractually obligated to notify the Ornsirin Group immediately upon becoming aware of any actual or suspected information security incident. Furthermore, such external parties should provide recommendations to the Legal Department and the Information Technology Department where adjustments to incident management processes are required.

4.16 Review of Insurance Obligations: The Information Security Incident Management Team shall review relevant insurance policies of Ornsirin Holding Public Company Limited to determine whether notification to the insurer is required in accordance with the terms and conditions of the applicable policies. This includes consideration of requirements relating to timing, content, and the form of notification as stipulated under the insurance coverage.

ORNSIRIN

Appendix 1

Information Security Incident Reporting Form

Please complete the details below and submit the form via email to the Information Security Incident Management Team at PDPA@ornsirin.co.th

Description of Information Security Incident	
Date and Time of Detection	
Person Identifying the Incident	Name: Position: Department: Country: Email Address: Telephone Number:
Reporting Employee / Contractor	☐ Same as the person identifying the incident Name: Position: Department: Country: Email Address: Telephone Number:
Systems Potentially or Actually Affected	
Categories of Affected Individuals (e.g., customers, business partners, employees/contractors, emergency contacts, minors, persons with disabilities)	
Categories of Personal Data Affected	
List of Persons Notified of the Incident	

ORNSIRIN

Appendix 2

Summary of Data Breach Notification Laws

<table>
<tr><th>No.</th><th>Data Breach Notification Law</th><th>Key Details</th></tr>
<tr><td>1.</td><td>Personal Data Protection Act B.E. 2562 (2019) (“PDPA”)</td><td>
• There are two types of notification obligations:
<table>
<tr><th>1. Notification to the Personal Data Protection Committee Office (PDPC)</th><th>2. Notification to data subjects</th></tr>
<tr><td>Without undue delay, and where feasible, within 72 hours from the time the Primary Incident Manager becomes aware of the information security incident.</td><td>Without undue delay</td></tr>
<tr><td>Notification of a Personal Data Breach</td><td>Notification of a Personal Data Breach, including remedial measures</td></tr>
<tr><td>Where the incident is likely to result in a risk to the rights and freedoms of individuals.</td><td>Where the incident is likely to result in a high risk to the rights and freedoms of individuals</td></tr>
<tr><td>Exceptions to the obligation to notify a personal data breach, as well as the applicable notification procedures, shall be prescribed in subordinate regulations.</td><td>Exceptions to data breach notification obligations and the applicable notification procedures shall be prescribed in subordinate regulations.</td></tr>
</table>
• “The data controller shall have the following duties
…(4) Notify the personal data breach to the Office without undue delay and, where feasible, within seventy-two (72) hours from the time of becoming aware of the breach, unless such breach is unlikely to result in a risk to the rights and freedoms of individuals. Where the breach is likely to result in a high risk to the rights and freedoms of individuals, the data controller shall also notify the data subjects of the breach and the remedial measures without undue delay. Such notification and any applicable exemptions shall be in accordance with the criteria and procedures prescribed by the Committee.” (Section 37)
• “ Any data controller who violates or fails to comply with Section 21, Section 22, Section 24, Section 25 paragraph one, Section 27 paragraph one or paragraph two, Section 28, Section 32 paragraph two, or Section 37, or obtains consent by deception or by misleading the data subject as to the
</td></tr>
</table>

No.	Data Breach Notification Law	Key Details
		purpose, or fails to comply with Section 21 as applied mutatis mutandis under Section 25 paragraph two, or transfers personal data in violation of Section 29 paragraph one or paragraph three, shall be subject to an administrative fine not exceeding Baht 3,000,000." (Section 83) • "The data processor shall have the following duties:: ...(2)Implement appropriate security measures to prevent loss, unauthorized access, use, alteration, modification, or disclosure of personal data, and notify the data controller of any personal data breach that has occurred." (Section 40) • " Any data processor who fails to comply with Section 40 without reasonable cause, or transfers personal data in violation of Section 29 paragraph one or paragraph three, or fails to comply with Section 37 (5) as applied mutatis mutandis under Section 38 paragraph two, shall be subject to an administrative fine not exceeding Baht 3,000,000." (Section 86)
3.	Cybersecurity Act B.E. 2562 (2019) ("Cybersecurity Act")	• The Cybersecurity Act requires reporting to competent authorities. Such notification obligations apply to organizations designated as Critical Information Infrastructure (CII) under subordinate regulations issued pursuant to Section 49 of the Cybersecurity Act, particularly in cases involving significant cyber threats. • " Where a significant cyber threat occurs affecting the systems of a Critical Information Infrastructure organization, such organization shall report the incident to the Office and the relevant supervisory or regulatory authority, and take response actions in accordance with the measures prescribed under Chapter 4 . The Cybersecurity Committee may also prescribe criteria and procedures for such reporting." (Section 57) • " Any Critical Information Infrastructure organization that fails to report a cyber threat in accordance with Section 57 without reasonable cause shall be subject to a fine not exceeding Baht 200,000." (Section 73)

ORNSIRIN

Appendix 3

Guidelines on Data Breach Notification Laws

1. Guidelines for Assessment – Personal Data Protection Act (PDPA)

The Information Security Incident Management Team shall assess the nature, scope, and severity of the information security incident in accordance with the direction and guidance of the Legal Department. Such assessment should be conducted on a case-by-case basis, taking into consideration the following set of questions.

Note: The Legal Department shall verify whether competent authorities have issued any subordinate regulations or guidelines relating to personal data breach incidents and risk assessment. Where such regulations or guidelines exist, Ornsirin Holding Public Company Limited shall take them into account together with the following assessment criteria.

Question 1:

Does the information security incident involve "personal data" as defined under the Personal Data Protection Act (PDPA)? *(If yes, proceed to the next question)*

Question 2:

Does the incident involve destruction, loss, or alteration—whether accidental or unlawful—or unauthorized disclosure or access to personal data that is transmitted, stored, or processed (i.e., a "personal data breach")? *(If yes, proceed to the next question)*

Question 3:

Is the personal data breach likely to result in a risk to the rights and freedoms of individuals, based on applicable guidelines?

(Note: Risk assessment should be conducted in accordance with subordinate laws/guidelines, where available) (If yes, proceed to the next question)

Question 4:

Are there any subordinate laws or guidelines that provide exemptions from the obligation to notify the Personal Data Protection Committee Office (PDPC)? If so, are such exemptions applicable?

If **no**, the Information Security Incident Management Team should consider whether notification to the PDPC is required and proceed to the next question

Question 5:

Is it likely that the risk can be classified as a high risk to the rights and freedoms of individuals?

Risk Assessment Guidelines – In determining whether an incident presents a risk or a high risk, the assessment shall be conducted on a case-by-case basis, taking into account the following factors:

- Type and sensitivity of the personal data involved in the incident
- Volume of personal data affected
- Number of data subjects impacted
- Nature of the personal data breach (e.g., loss of a computer device vs. theft of a company database)
- The ease with which the affected data can be used to identify individuals.

- Special characteristics of affected individuals (e.g., vulnerable groups such as minors or persons with disabilities)
- Special characteristics of the data controller (e.g., organizations that process large volumes of sensitive personal data, such as hospitals or insurance companies)

Note: Risk assessment should be conducted in accordance with applicable subordinate laws or guidelines, where such regulations or guidance have been issued.

Question 6:

Are there any subordinate laws or guidelines that provide exemptions from the obligation to notify data subjects? If so, are such exemptions applicable?

If **no**, the Information Security Incident Management Team should assess whether it is required to:

(1) Notify the Personal Data Protection Committee Office (PDPC), and

(2) Notify the data subjects.

2. Guidelines for Assessment – Cybersecurity Act

The Information Security Incident Management Team shall assess the nature, scope, and severity of the information security incident in accordance with the direction and guidance of the Legal Department. Such assessment should be conducted on a case-by-case basis, taking into consideration the following set of questions.

Note: The Legal Department shall verify whether competent authorities have issued any subordinate regulations or guidelines relating to Critical Information Infrastructure (CII), data breaches, and risk assessment. Where such regulations or guidelines exist, the Ornsirin Group shall consider them together with the following assessment criteria.

Question 1:

Are there any subordinate laws or guidelines that define criteria for Critical Information Infrastructure (CII)? If so, does the Ornsirin Group fall within such criteria? *(If yes, proceed to the next question)*

Question 2:

Does the information security incident constitute a "cyber threat" as defined under the Cybersecurity Act? *(If yes, proceed to the next question)*

Question 3:

Are there any subordinate laws or guidelines that define criteria for "significant" cyber threats? If so, does the incident meet such criteria?

If **yes**, the Information Security Incident Management Team shall assess whether the Ornsirin Group is required to report the incident to the National Cybersecurity Committee (NCSC) and the Cybersecurity Regulatory Committee (CRC), as applicable.

Effective from 15 November 2024 onwards