



Privacy Policy

Document Code PIMS-PL-001 | Version 02

Effective Date 19 October 2026

Document Code	PIMS-PL-001
Document Title	Privacy Policy
Version	02
Effective Date	19 October 2026
Prepared By	Data Protection Officer (DPO)
Reviewed By	Data Protection Officer (DPO)
Approved By	Managing Director (MD)
Classification	Public
Reference Standard	ISO/IEC 27701:2025; Personal Data Protection Act B.E. 2562 (2019)

Document Revision History

Version	Date	Description of Change	Prepared – Reviewed – Approved
01	21 September 2026	Initial release	PIMS Working Team – MD – MD



02	19 October 2026	– Corporate document format applied (TH SarabunPSK, cover metadata, revision history, table of contents, approval block); structure changed from 13 to 21 sections – Added sections: Definitions; Collection of Personal Data (notice content and groups of processing activities from the ROPA); Use and Disclosure; Quality of Personal Data; Security of Personal Data; Retention Period; Third-Party Websites and Services; Cookies; DailiTech as a PII Processor (services and controls); Sub-processors (with countries); Customer Data Ownership; PIMS Governance and Commitments, Data Protection Officer and Privacy Communication; Contact Channels; Accountability and Penalties – Lawful basis (Section 5) rebuilt from the ROPA and PDPA references corrected: legitimate interests s.24(5) (was s.24(6)), legal obligation s.24(6) (was s.24(5)), consent s.19 (was s.24(1)), pre-contractual steps under s.24(3) (was s.24(2)), social security health data s.26(5)(c); Proposal and SOW preparation changed from legitimate interests to contract; newsletters to prospects (consent) removed – Data subject rights: response time table by right added (withdrawal of consent 7 days, other rights 30 days); requests concerning customer data forwarded to the customer within 2 business days (was 3 business days, with assistance within 5) – Sub-processor list aligned with the ROPA; Anthropic (Claude Enterprise) no longer listed – Breach notification to customers: without undue delay within the time agreed in the DPA (was within 24 hours; 24 hours retained in PIMS-PD-002)	DPO – MD – MD
----	-----------------	---	---------------



		– Removed sections: The Company's Roles; Data Protection Principles; Sensitive Data; Employee Monitoring and Limits on Use; Prohibition on AI Processing of Personal Data; Roles and Responsibilities table; training requirements (within 30 days of joining, specialist course for engineers) and PDPA penalty amount – Removed references to DPIA mandatory triggers, the eight-point legal validity check and Managing Director approval of every disclosure (disclosure requests handled under PIMS-PD-005) – Document codes updated: procedures PIMS-PR → PIMS-PD – Aligned with privacy notices PIMS-AN-001 to PIMS-AN-003 (Version 02): scope and groups of processing activities extended (contract management, Finance & Accounting, partner lead sharing, payroll and welfare, work permit and visa, business travel, personnel profiles to customers, employee photographs in marketing) – Lawful basis table updated for the new activities; vital interest s.24(2) added (business travel emergency contact); explicit consent extended to race and health data in the job application form – Domestic recipients updated (payroll service provider replaced by outsourced accounting firm; banks, legal advisers, Department of Employment and Immigration Bureau, customers, technology partners, travel and event providers, acquirers and investors added) – Cross-border transfer wording aligned with PDPA Sections 28 and 29 (adequacy, safeguards such as providers' data processing	
--	--	--	--



Version	Date	Description of Change	Prepared – Reviewed – Approved
		terms with standard contractual clauses, or Section 28 exceptions) – Sub-processors added: Adobe Inc. (Adobe Acrobat Sign), DocuSign, Inc., outsourced accounting firm; Anthropic, PBC (Claude) re-added – Contact telephone changed to 02-105-3296 and added to rights requests – Criminal-record checks moved from recruitment to a post-hire check for all employees; recruitment sensitive data limited to race (statistics only), religion on the ID card copy and health (serious illness or contagious disease); insured family members added as data subjects of group health insurance; background-check providers removed from domestic recipients	



Table of Contents

1. Introduction	6
2. Scope	6
3. Definitions.....	7
4. Collection of Personal Data	8
5. Lawful Basis for Processing.....	9
6. Use and Disclosure of Personal Data.....	11
7. Quality of Personal Data.....	11
8. Security of Personal Data	11
9. Cross-Border Transfer of Personal Data	12
10. Rights of Data Subjects	12
10.1 Channels and response times.....	13
11. Retention Period	14
12. Third-Party Websites and Services	14
13. Cookies	14
14. DailiTech as a PII Processor	15
15. Sub-processors	16
16. Customer Data Ownership.....	17
17. Personal Data Breach Notification.....	17
18. PIMS Governance and Commitments.....	18
18.1 Data Protection Officer	18
18.2 Privacy Communication.....	18
19. Contact Channels	19
20. Accountability and Penalties.....	19
21. Review of this Policy	19
Document Approval	20



1. Introduction

To ensure that the organization is managed in accordance with the principles of good governance, DailiTech Co., Ltd. ("DailiTech" or the "Company") recognises the importance of personal data protection. The Company respects the rights of individuals over their personal data, which is a fundamental privacy right protected under the Constitution of the Kingdom of Thailand and the Personal Data Protection Act B.E. 2562 (2019) ("PDPA"). The Company therefore issues this Policy as the principal framework for the protection of personal data.

This Policy is the top-level privacy policy of the DailiTech Privacy Information Management System (PIMS) established in accordance with ISO/IEC 27701:2025. It applies to processing in which DailiTech acts as a **PII controller** and to processing in which DailiTech acts as a **PII processor** on behalf of its customers.

Its objectives are to ensure that personal data is processed lawfully, fairly and transparently; that processing is limited to specified purposes and to the minimum necessary; that personal data is accurate, retained no longer than necessary and kept secure; and that DailiTech can demonstrate accountability through the ROPA, DPIAs and the PIMS.

2. Scope

This Policy applies to the Board, directors, executives and employees at all levels of the Company, as well as contractors, suppliers, service providers and other stakeholders who process personal data for or on behalf of the Company. It covers every processing activity recorded in the Record of Processing Activities (PIMS-RG-001 Record of Processing Activities (ROPA)), including collection channels, types and formats of personal data, purposes, disclosure, cross-border transfer, retention and the security measures applied.

The processing activities in scope are grouped into the following business functions, as recorded in the ROPA:

- **Consulting & Implementation** – solution design, proposals and SOW, AWS project delivery, contract management
- **Managed Services** – incident and ticket management, change management, monitoring and alerting, LINE OA communication
- **IT / Internal Operations** – identity and access management, device management, meeting recording, AWS access control, vendor register, corporate email



- **Human Resources** – recruitment, tax withholding, social security, group health insurance, personnel administration, payroll and welfare benefits, work permits and visas, business travel, submission of personnel profiles to customers, use of employee photographs and videos in marketing
- **Customer Success** – events and seminars, marketing communication, office CCTV, partner lead sharing and opportunity registration
- **Finance & Accounting** – billing, invoicing and collection, supplier selection, contracts and payments
- **PII processing on behalf of customers** – AWS Infrastructure Managed Service

3. Definitions

Term	Definition
Personal data / PII	Any information relating to a person which enables the identification of that person, directly or indirectly, but not including information of deceased persons.
Sensitive personal data	Personal data under PDPA Section 26: racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic data, biometric data, or other data prescribed by the PDPC.
Data subject / PII principal	The natural person to whom the personal data relates.
Data controller / PII controller	A person or juristic person having the power and duty to make decisions regarding the collection, use or disclosure of personal data.
Data processor / PII processor	A person or juristic person who collects, uses or discloses personal data pursuant to the orders or on behalf of a data controller.
Sub-processor	A processor engaged by DailiTech that processes personal data for which DailiTech is a controller or processor.
ROPA	The Record of Processing Activities maintained under PDPA Sections 39 and 40 (PIMS-RG-001).
DPO	The Data Protection Officer of DailiTech, contactable at privacy@dailitech.com .
PDPC	The Personal Data Protection Committee and its Office (the Thai supervisory authority).



4. Collection of Personal Data

The Company collects personal data only to the extent necessary for lawful purposes that are directly related to its business. Before or at the time of collection, the Company informs data subjects of the following (PDPA Section 23), through the privacy notices issued under PIMS-AN-001 to PIMS-AN-003:

- (a) the purposes of collection, use or disclosure;
- (b) where collection is required to comply with law or a contract, or is necessary to enter into a contract, the possible consequences of not providing the personal data;
- (c) the personal data to be collected and the retention period;
- (d) the categories of persons or entities to whom the personal data may be disclosed;
- (e) the identity and contact details of the data controller and the DPO;
- (f) the rights of the data subject; and
- (g) any other information required by law.

The Company collects personal data for the following groups of processing activities. Full details are maintained in PIMS-RG-001.

Group of activities	Categories of personal data
Consulting & Implementation – solution design, proposals/SOW and AWS project delivery, contract management	Customer and prospect contacts: name, position, company, email, telephone; authorised signatories: signature, copy of ID card or passport, company affidavit, power of attorney
Managed Services – incident and ticket management, change management, monitoring and alerting, LINE OA communication	Customer contacts and users: name, email, telephone, incident details, system logs, IP address, user agent, user/account ID, LINE user ID and display name, LINE profile picture, messages, images and files
IT / Internal Operations – identity and access management, device management, meeting recording, AWS access control, vendor register, corporate email	Employees, meeting participants, vendor and business contacts: name, email, device association, image and voice (recordings)



Group of activities	Categories of personal data
Human Resources – recruitment, tax withholding, social security, group health insurance, personnel administration, payroll and welfare benefits, work permit and visa, business travel, personnel profiles to customers, employee photographs in marketing	Job applicants, employees and insured family members: identification and contact data, national ID, taxpayer ID, social security number, education and employment history, salary, leave, appraisal, bank account, family and emergency contact details, passport, visa and work permit, photographs and videos; sensitive data – criminal record (post-hire check for all employees; work permit and visa), health data (including insured family members), race and religion (job application form)
Customer Success – events and seminars, marketing communication to existing customers, office CCTV, partner lead sharing	Attendees, customer contacts, employees and visitors: name, company, position, email, telephone, dietary restrictions, photographs/video, CCTV images; contact and opportunity details shared with technology partners
Finance & Accounting – billing, invoicing and collection, supplier selection, contracts and payments	Customer billing contacts and supplier contacts: name, position, email, telephone, billing address, tax ID or national ID (individuals), bank account details, invoices and withholding tax certificates; authorised signatories' signature and ID documents

5. Lawful Basis for Processing

Every processing activity must have at least one lawful basis identified and documented in the ROPA before processing begins. The lawful bases used by DailiTech are:

Lawful basis (PDPA)	Description	ROPA activities relying on it
Contract – s.24(3)	Necessary for the performance of a contract to which the data subject is a party, or to take steps at the data subject's request before entering into a contract.	Consulting and project delivery, incident/change management, monitoring, identity and access management, AWS access control, corporate email, recruitment, group health insurance, personnel administration, payroll and welfare benefits, business travel, contract management, billing and collection, supplier payment



Lawful basis (PDPA)	Description	ROPA activities relying on it
Legitimate interest – s.24(5)	Necessary for the legitimate interests of the Company or of another person, except where such interests are overridden by the fundamental rights of the data subject. A legitimate interest assessment (LIA) is recorded for each activity.	LINE OA communication, device management, meeting recording, marketing communication, office CCTV, partner lead sharing, IT resources monitoring, submission of personnel profiles to customers, incidental appearance in event photographs
Legal obligation – s.24(6)	Necessary for compliance with a law to which the Company is subject (e.g. Revenue Code, Social Security Act, PDPA s.40 record-keeping).	Tax withholding, social security, sub-processor register, work permit and visa, accounting and tax records (billing, supplier payment)
Consent – s.19	Freely given, specific, informed and unambiguous consent, obtained in accordance with PIMS-PD-006. Used only where no other lawful basis applies.	Events and seminars, use of employee photographs and videos in social media and marketing
Explicit consent – s.26 para 1	Required for sensitive personal data unless a Section 26 exception applies.	Recruitment (race, religion and health data in the application form), post-hire criminal-record check (all employees), group health insurance (health data of employees and insured family members), events (dietary restrictions), work permit and visa (criminal record)
Section 26(5)(c) – compliance with law (social security)	Sensitive data necessary for compliance with employment-protection and social security law.	Social security (sickness/maternity data)
Vital interest – s.24(2)	Necessary to prevent or suppress a danger to a person's life, body or health.	Business travel (contacting the emergency contact)

Consent is considered only where the processing cannot rely on the bases in PDPA Section 24(1)–(6). Where consent is used, the Company informs the data subject of the right and the channel to withdraw consent (Email privacy@dailitech.com or Form PIMS-FM-002 in accordance with PIMS-PD-001).



6. Use and Disclosure of Personal Data

Personal data is used or disclosed only for the purposes notified to the data subject, for purposes to which the data subject has consented, or for purposes directly related to the original purpose of collection. Consent is not required for use or disclosure in the following cases:

- (a) to prevent or suppress a danger to a person's life, body or health;
- (b) where the personal data has been lawfully disclosed to the public;
- (c) where necessary for the establishment, compliance with, exercise or defence of legal claims;
- (d) to comply with a law or a court order; and
- (e) any other case permitted by law.

Personal data is disclosed within Thailand only to the recipients recorded in the ROPA, including the Revenue Department, the Social Security Office, the partner insurer and partner hospitals, the outsourced accounting firm (bookkeeping, payroll and tax filings), banks and the provident fund manager, legal advisers, the Department of Employment and the Immigration Bureau, recruitment agencies (where used), customers and prospective customers (personnel profiles), technology partners and vendors (lead sharing and opportunity registration), travel and event service providers, event organisers and photographers under NDA and DPA, and the CCTV service provider/building management, and, in a restructuring, merger or sale of business, prospective acquirers, investors and their advisers. Disclosures to third parties are recorded in accordance with PIMS-PD-005.

7. Quality of Personal Data

The Company ensures that personal data is accurate, complete, up to date and not misleading, and gives data subjects the opportunity to request correction of their personal data.

8. Security of Personal Data

The Company implements appropriate technical and organisational measures, aligned with the DailiTech ISMS (ISO/IEC 27001:2022) and ISO/IEC 27701:2025, to prevent loss, unauthorised access, destruction, use, alteration or disclosure of personal data. The baseline controls recorded in the ROPA are:

- Single sign-on and multi-factor authentication through Microsoft Entra ID with Conditional Access;



- Role-based access control and least privilege, with annual access reviews (ISMS-PD-001);
- Encryption at rest (AES-256) and in transit (TLS 1.2/1.3);
- CrowdStrike Falcon EDR and Microsoft Intune MDM with FileVault disk encryption;
- Microsoft Purview data loss prevention (DLP) and sensitivity labels;
- Audit logging, and privileged access to customer environments through Keeper Connection Manager, IAM AssumeRole and NAT IP whitelisting; and
- Activity-specific measures recorded against each ROPA activity (e.g. WorkSpaces session recording, separate storage of health documents, CCTV review approval).

The Company is not liable for damage arising from the use or disclosure of personal data to third parties caused by the data subject's own actions or omissions, or by persons acting with the data subject's consent, such as failing to log out of the Company's systems.

9. Cross-Border Transfer of Personal Data

Personal data is transferred outside Thailand only to the recipients and countries listed in the Cross-Border Transfer Register (PIMS-RG-003), which is maintained consistently with the ROPA. Each transfer is made only where (a) the destination country has adequate data protection standards under PDPA Section 28, (b) appropriate safeguards are in place under Section 29, such as the provider's data processing terms incorporating standard contractual clauses, or (c) an exception under Section 28 applies, such as consent, performance of a contract with the data subject, compliance with law or protection of life or health, in accordance with the PDPC Notifications on cross-border transfer. Destination countries currently include Singapore, the United States, Australia, Japan, Canada and the European Union (Czech Republic, Germany), and, for business travel, the destination country of the trip. The procedure is set out in PIMS-PD-005.

Tax withholding, social security, group health insurance and office CCTV data are processed and stored in Thailand only.

10. Rights of Data Subjects

Data subjects may exercise the following rights under the PDPA, subject to the conditions and exceptions provided by law. Where the data subject is under 20 years of age or legally incapacitated, the request may be made by the parent, guardian or authorised representative.



- **Right to withdraw consent** – where processing is based on consent, the data subject may withdraw consent at any time, unless restricted by law or by a contract that benefits the data subject. Withdrawal does not affect processing carried out before the withdrawal.
- **Right of access** – to access and obtain a copy of their personal data and to request disclosure of how the data was obtained where it was collected without consent.
- **Right to data portability** – to receive their personal data in a structured, commonly used, machine-readable format and to request its transfer to another controller where technically feasible.
- **Right to object** – to object to processing based on legitimate interest or public task, and to processing for direct marketing. Objections to direct marketing are always honoured.
- **Right to erasure** – to request deletion, destruction or anonymisation where the data is no longer necessary, consent has been withdrawn, an objection has been upheld, or the processing is unlawful.
- **Right to restriction** – to request restriction of use while a correction or objection request is being verified, or instead of erasure.
- **Right to rectification** – to request that their personal data be corrected, updated and completed.
- **Right to lodge a complaint** – with the PDPC if they believe the Company has infringed the PDPA.

The Company may refuse a request where permitted by law (e.g. compliance with a law or court order, or where the request would adversely affect the rights and freedoms of others) and will inform the data subject of the reasons for refusal. Requests are handled in accordance with the Data Subject Rights Request Procedure (PIMS-PD-001). Requests may also be made by telephone at 02-105-3296.

10.1 Channels and response times

Right	Channel	Response time*
Withdraw consent	Email privacy@dailitech.com or Form PIMS-FM-002	Within 7 days
Access / obtain a copy	Email privacy@dailitech.com or Form PIMS-FM-002	Within 30 days
Data portability	Email privacy@dailitech.com or Form PIMS-FM-002	Within 30 days



Right	Channel	Response time*
Object (including direct-marketing opt-out)	Email privacy@dailitech.com , Form PIMS-FM-002 or unsubscribe link	Within 30 days (marketing opt-out: immediately, at most 7 days)
Erasure	Email privacy@dailitech.com or Form PIMS-FM-002	Within 30 days
Restriction of processing	Email privacy@dailitech.com or Form PIMS-FM-002	Within 30 days
Rectification	Email privacy@dailitech.com or Form PIMS-FM-002	Within 30 days

* Counted from the date the identity of the requester has been verified. Where DailiTech acts as a PII processor, requests are forwarded to the relevant customer (PII controller) in accordance with PIMS-PD-009.

11. Retention Period

The Company retains personal data only for as long as necessary to fulfil the purposes for which it was collected, or for longer where retention is required or permitted by law (e.g. the Revenue Code, the Labour Protection Act, the Civil and Commercial Code limitation periods and the Computer Crime Act). Retention periods for each ROPA activity are defined in the Data Retention and Disposal Policy (PIMS-PL-002). At the end of the retention period, personal data is deleted, destroyed or anonymised in accordance with the Data Retention and Disposal Procedure (PIMS-PD-007).

12. Third-Party Websites and Services

The Company may provide links to websites and services of third parties for convenience and information. Such websites and services operate independently of the Company and have their own privacy notices and policies, which data subjects are strongly advised to review. To the extent that the Company does not own or control those websites, the Company is not responsible for their content, privacy practices or quality of service.

13. Cookies

The Company's website may use cookies and similar technologies (e.g. web analytics) to enable the website to function, to remember preferences and to understand how visitors use the website.



Cookies are small text files stored on the visitor's device. Non-essential cookies are used only with the visitor's consent, which may be changed at any time through the cookie settings on the website or the browser.

Cookie category	Description	Status
Strictly necessary	Required to provide the website and its security, e.g. session identifiers.	Always active
Functional	Improve functionality, e.g. remembering preferences. Some functions may not work without them.	Consent required
Analytics	Collect usage information to help the Company understand and improve the website and its communications.	Consent required

14. DailiTech as a PII Processor

In addition to acting as a PII controller for the activities recorded in the ROPA, DailiTech acts as a **PII processor** when it accesses or processes personal data held in customers' AWS environments while providing Implementation and Managed Services. In that role DailiTech:

- processes personal data only on the documented instructions of the customer and for the purposes of the service, as set out in the customer agreement and data processing agreement (DPA);
- does not use customer personal data for its own purposes, including marketing or advertising;
- informs the customer if an instruction infringes applicable law;
- assists the customer in responding to data subject requests and in meeting its obligations;
- returns or disposes of personal data at the end of the service as agreed in the DPA; and
- engages sub-processors only with the customer's general or specific authorisation.

Data location: DailiTech's own controller data is stored in the cloud services listed in PIMS-RG-003. Customer data processed by DailiTech as processor remains in the AWS account and Region selected by the customer (e.g. Thailand ap-southeast-7 or Singapore ap-southeast-1). The customer determines and is informed of that location.



DailiTech service	Personal data that may be processed	Controls
AWS Infrastructure Managed Service	Database query results that may contain customers' end-user PII	Customer request required before any query; SELECT-only; no export; results deleted immediately after troubleshooting; IAM role + MFA; session logged
AWS Implementation / Migration projects (e.g. MGN, DMS)	Customer data sets in transit during migration (content determined by the customer)	Work performed inside the customer account through AWS WorkSpaces; clipboard/download blocked; no copies retained
Managed Services – monitoring, backup configuration and incident response	System logs and technical identifiers held in the customer's environment	Access through IAM AssumeRole and Keeper Connection Manager; log retention per DPA

15. Sub-processors

The Company may disclose or transfer personal data to service providers acting as processors or sub-processors, only to the extent necessary for the purposes notified and under appropriate data protection agreements. Sub-processors process personal data only on the Company's instructions and do not use it for their own purposes, including marketing or advertising. The current sub-processors are:

Sub-processor	Country	Service
Amazon Web Services (AWS)	USA (Singapore, Thailand regions)	Cloud infrastructure (IaaS)
Microsoft Corporation (M365)	USA (global cloud)	SaaS – Exchange, Teams, SharePoint, OneDrive, Purview, Entra ID
CrowdStrike, Inc.	USA	Endpoint security
Atlassian Pty Ltd	Australia (global cloud)	ITSM – JIRA SM, JIRA Software, Confluence
GitLab Inc.	USA	Version control, CI/CD, Terraform state
Make (Celonis SE)	EU (Czech Republic)	Workflow automation



Sub-processor	Country	Service
Airtable Inc.	USA	Operational database / logs
1Password (AgileBits Inc.)	Canada	Secrets management
LINE Corporation	Japan	Messaging – LINE OA webhook
Notion Labs, Inc.	USA	Workspace – documentation, approvals, contact lists
tl;dv GmbH	Germany (EU)	Meeting recording / transcription
Adobe Inc. (Adobe Acrobat Sign)	Singapore	Electronic signature – job application forms
DocuSign, Inc.	EU (DocuSign EU data centres)	Electronic signature – contracts and employee documents (integrated with Make)
Outsourced accounting firm	Thailand	Bookkeeping, payroll and tax filings
Anthropic, PBC	USA	AI assistant (Claude) – drafting, analysis and workflow automation

16. Customer Data Ownership

All data and content that customers store or process in their own environments remain the property of the customer. DailiTech does not claim ownership of such data and accesses it only as necessary to provide the service, maintain systems or comply with law. At the end of the service, customer data is returned or securely deleted, and a certificate of deletion is issued where required by the DPA.

17. Personal Data Breach Notification

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the Company notifies the PDPC without delay and, where feasible, within 72 hours of becoming aware of it, and notifies the affected data subjects without delay where the risk is high (PDPA Section 37(4)). As a PII processor, the Company notifies the customer (PII controller) without undue delay after becoming aware of the breach, within the time agreed in the DPA (PDPA Section 40(2)). Breaches are managed in accordance with PIMS-PD-002.



18. PIMS Governance and Commitments

Top management of DailiTech commits to:

- satisfy applicable requirements related to the protection of personal data, including the PDPA, contractual requirements with customers and the requirements of ISO/IEC 27701:2025;
- provide a framework for setting privacy objectives (PIMS-RG-006);
- continually improve the PIMS;
- appoint a Data Protection Officer and assign PIMS roles and responsibilities (IMS Manual IMS-MN-001);
- assess and treat privacy risks, including through DPIAs where required (IMS Manual IMS-MN-001; PIMS-PD-003); and
- communicate this Policy within the Company and make it available to interested parties.

18.1 Data Protection Officer

- The DPO is appointed in writing by the Managing Director and reports directly to the Managing Director.
- The DPO performs the duties in PDPA Section 42: advising DailiTech, its employees and processors on PDPA compliance; monitoring compliance; coordinating and cooperating with the PDPC; and keeping confidential the information obtained in performing their duties.
- DailiTech supports the DPO with adequate tools, resources and access to personal data and processing operations. The DPO must not be dismissed or have their employment terminated for performing their DPO duties, and must have no conflicting duties.
- Other PIMS roles and responsibilities are defined in the IMS Manual and its roles and responsibilities document.

18.2 Privacy Communication

What	When	With whom	How	Who communicates
Privacy Policy and privacy notices	On issue / change	Employees, public	Intranet, website	DPO
Privacy objectives and KPI results	Quarterly	Information Security Committee (ISC), MD	ISC meeting	DPO
Sub-processor changes	30 days before change	Customers	Email / customer portal	DPO / MS Lead



What	When	With whom	How	Who communicates
Personal data breach	Per PIMS-PD-002	PDPC, customers, data subjects	Official notification	DPO with MD approval
DSR responses	Per PIMS-PD-001	Data subjects	Email	DPO

19. Contact Channels

For suggestions or questions about the collection, use or disclosure of personal data, or to exercise rights under this Policy, please contact the Data Protection Officer:

Data Protection Officer	DailiTech Co., Ltd.
Address	The Parq, 6th Floor Unit, East Wing, 88 Ratchadaphisek Road, Klongtoey, Bangkok 10110, Thailand
Email	privacy@dailitech.com
Telephone	02-105-3296
General enquiries	contact@dailitech.com

20. Accountability and Penalties

Employees and units involved in processing personal data must comply strictly with this Policy and its supporting procedures. Any person responsible for an activity who neglects, omits or acts in breach of this Policy, resulting in an offence under the law or damage, is subject to disciplinary action in accordance with the Company's regulations, without prejudice to any civil, criminal or administrative liability under the law.

21. Review of this Policy

The DPO reviews this Policy at least annually, and whenever there is a significant change in the ROPA, the law or the Company's services. Changes are approved by the Managing Director. The current version is published on the Company's website and communicated to employees.



Document Approval

Prepared by	Reviewed by	Approved by
Signature  (Sura Rodpongpan) PIMS Working Team and DPO Date 19 / 10 / 2026	Signature  (Vit Niennattrakul) Managing Director Date 19 / 10 / 2026	Signature  (Vit Niennattrakul) Managing Director Date 19 / 10 / 2026