



Advanced Info Service
Public Company Limited

414 AIS Tower,
Phaholyothin Rd., Samsen Nai,
Phayathai, Bangkok 10400

Data Retention and Archiving Standard (Translation)

AIS Group

Version: 1.2

Document owner: Data Protection Office

Last Updated: 1 February 2024







Document Control

Document Approval

This document was reviewed and approved by the following person

Document owner	
Name	Data Protection Office
Date	1 February 2024

Created/Modified/Cancelled by	Reviewed by	Approved by
 Weeraporn Weeratibhawom Compliance Awareness Specialist Date 1/2/24	 Montakarn Ahkuputra Head of Data Protection Office Unit Date 2/2/24	 Mark Chong Chin Kok Acting Chief Information Officer Date 6/2/24
	 Pepijn Kok Head of Cyber Security Section Date 5/2/24	



Revision History

This document has the following modification record.

Version	Date	Author	Detail	Reviewer	Approval
1.0	9 August 2022	Cyber Security	Initial release	Head of Data Protection Office Unit, Head of Cyber Security Section	Chief Information Officer
1.1	2 August 2023	Cyber Security	<ul style="list-style-type: none"> - Edited the details of topic 1.4 Consequence for Non-Compliance - Edited the refer document name from Data Classification and Handling Framework to Data Classification and Handling Standard - Edited 1.5 Definitions, 13) Physical Format to Publishing Format - Delete the definition of “Cyber Security Deviation Control Working Group (CSDC)” in Clause 1.5 Definitions because CSDC member is rotate quarterly - Edited details of 3.2. (Retention and Archiving Period) 	Head of Data Protection Office Unit, Head of Cyber Security Section	Chief Information Officer



Version	Date	Author	Detail	Reviewer	Approval
			<ul style="list-style-type: none"> - 2.1 deleted text Change SIM card, - 3.1 Edited from "New Register (new customers, old customers, make new eKYC, apply for GobalPay service, activate PromptPay service, start mPay wallet, apply for mPay agent, shop apply for payment service)" to "Service registration data, including detailed information about identification and mPay transaction data (apply for GobalPay service, activate PromptPay service, start mPay wallet)" and edit the data owner from CFO to MD- MPAY - Edited text from "Register for a new agent (ROM WebMA, Mobile App, Web Agent, 		



Version	Date	Author	Detail	Reviewer	Approval
			<p>Web Call Center)" to "Service registration mPay Agent data, including detailed information about identification and mPay transaction data (ROM WebMA, Mobile App, Web Agent, Web Call Center)", edited the data owner from CCBO/CEBO to MD-MPAY, and added picture format</p> <ul style="list-style-type: none"> - Deleted Clause 3.3 Detailed information about identification (KYC) - Edited 3.4 the data owner from CFO to MD-MPAY and deleted picture format - Added text in 6.1, retention period At least 90 days - Edited text in 6.2 retention period from "More than 90 days but not more than two years can 		



Version	Date	Author	Detail	Reviewer	Approval
			<p>be a particular case for an individual or occasionally" to "Upon request from the competent official before the expiration of the 90-day period under Clause 6.1, for a further period of not more than 6 consecutive months, but not more than 2 years"</p> <ul style="list-style-type: none"> - Edited text in 3.3.2 from physical format to publishing format - Added Cyber Security and Data Protection for Employee Procedure to 4. Reference 		
1.2	1 February 2024	Cyber Security	<ul style="list-style-type: none"> - Added text in topic 1.5 Definitions, 15) Customer Profile and 16) Customer Order History - Updated content in topic 3.2 Retention and Archiving Period, in the section of 2. Customer Record and 	Head of Data Protection Office Unit, Head of Cyber Security Section	Act. Chief Information Officer



Advanced Info Service
Public Company Limited

414 AIS Tower,
Phaholyothin Rd., Samsen Nai,
Phayathai, Bangkok 10400

Version	Date	Author	Detail	Reviewer	Approval
			6. Computer Traffic Data Record		



Table of Contents

1. Introduction	9
1.1. Objective	9
1.2. Scope	9
1.3. Exceptions.....	9
1.4. Penalties for Non-compliance with the Standard.....	9
1.5. Definition	9
2. Roles and Responsibilities	12
3. Standard.....	13
3.1. Data Asset Inventory Management.....	13
3.2. Retention and Archiving Period.....	14
3.3. Safeguarding of Data during Retention and Archiving	22
3.4. Secure data destruction.....	24
4. Reference.....	25
Annex A: Data Asset Inventory Form.....	26



1. Introduction

1.1. Objective

To set standards for securely retaining important company information and comply with applicable legal requirements and regulations by keeping the information for business purposes and complying with the laws as necessary.

1.2. Scope

This standard covers the protection and security of company information, personal data, and traffic logs, which refers to the Computer Crime Acts, inside and outside the company's workplace. The standards include:

- 1) All employees and departments of the company
- 2) External parties who granted access to assets related to sensitive corporate data.

1.3. Exceptions

Any other form of action where this standard is not applicable must ask for approval from the Cyber Security Deviation Control Working Group (CSDC) by proceeding:

- 1) Analyze risks arising from non-compliance with the documentation. However, compensation control must be considered to reduce potential risks as well.
- 2) Make a written record of accepting the risks that may arise from non-compliance through the head of the section or above to request approval from CSDC.

1.4. Penalties for Non-compliance with the Standard

- 1) Refer to the current version of the employee handbook. "Staffs' Rules of Advanced Info Service Plc. and Subsidiaries"
- 2) Refer to the Cyber Security and Data Protection for Employee Procedure

1.5. Definition

The definitions in this standard are based on the "Customer Information Protection Standard for Employee and Third Party" and "Data Classification and Handling Framework" The definitions include:

- 1) **"Company"** means Advance Info Service Public Company Limited and companies in the AIS business line.
- 2) **"Employee"** means an employee hired to work as a probationary employee, permanent employee, contract employee, and executive at all levels under the company's employment.



Advanced Info Service
Public Company Limited

414 AIS Tower,
Phaholyothin Rd., Samsen Nai,
Phayathai, Bangkok 10400

- 3) **"Customer"** means a person who purchases products or uses services of Advanced Info Service Public Company Limited and companies in the business line.
- 4) **"Third Party"** means a person, a juristic person, or a legal entity that can request personal information from the company.
- 5) **"External Party"** means personnel or external entities operating business or providing services that may be entitled to access to the company's information and information processing equipment, such as
 - Business Partner
 - Outsource
 - Supplier
 - Service Provider
 - Consultant
- 6) **"Company's Sensitive Data"** means six domains: customer, employee, partner, financial, network, and strategic data. This definition refers to the document "Data Classification and Handling Standard" Appendix B.
- 7) **"Data Asset"** means a set of data elements, which can be in physical and electronic formats such as forms, and document files.
- 8) **"Data Owner"** means a person or entity responsible for business use or business results of that information system. The data owner is assigned to manage, control, and protect the company's sensitive data assets throughout the life cycle. The data owner must be a person or entity appointed by the company.
- 9) **"Data Steward"** means a person responsible for supervising each data domain and has a strong understanding of business needs and data security in the organization. The data steward acts as a mediator between business and information technology departments to discuss the logic, communication, and data domain usage the data steward must specify in each data domain.
- 10) **"Company's Laptop/PC"** means computer equipment that is the company's property, including the company's desktop equipment and portable devices, such as a laptop, notebook, smartphone, and tablet computer.
- 11) **"Company's storage"** means the storage facility provided by the company. The users can retrieve, import, and export the company's data from electronic media such as the company's Network Attached Storage (NAS) and OneDrive.
- 12) **"Electronic Format"** means data in various formats such as e-Document files, emails, images, and texts stored in electronic forms such as hard drives, clouds, databases, portable computers, or the company's desktop computer or company data storage.
- 13) **"Publishing Format"** means data in various formats such as text and images printed on printed media such as paper.



Advanced Info Service
Public Company Limited

414 AIS Tower,
Phaholyothin Rd., Samsen Nai,
Phayathai, Bangkok 10400

- 14) **"Warehouse"** means an external company that operates a business of storing documents or assets of various organizations which the company hires to keep essential documents of the company such as customer information documents and accounting documents.
- 15) **"Customer profile"** means data that indicates or identifies the customer's identity and is used to provide customer service, such as Mobile Number, Name-Surname, Address, Birthdate, ID Card Number.
- 16) **"Customer Order History"** means transaction history data of Change Promotion, Reconnect - Credit Limit, Reconnect - Customer Request, Reconnect - Debt, Reconnect – Fraud, Suspend - Credit Limit, Suspend - Customer Request, Change Account Promotion, Change Billing Account, Change SIM, Change Service, Suspend - Customer Request



2. Roles and Responsibilities

1) Data Owner and Data Steward Roles

- Provide data asset inventory under the scope of responsible data.
- Review the data asset inventory at least once a year or when data has been changed.
- Protect stored data recorded in electronic or print media securely accord to the standards.
- Consider destroying stored data that exceed the requirements.

2) Employee Roles

- Learn, understand and follow this standard.
- Employees involved in or taking care of external parties must have that external party comply with this standard.

3) Data Protection Office Roles

- Provide some advice on data retention and safeguard to the data owner, data steward, or related agencies.

4) External Party Roles

- Learn, understand and follow this standard document.

5) Warehouse Roles

- Store customer data documents and company's sensitive data with a high level of security to ensure integrity and availability.
- Deliver customer data documents and company's sensitive data to the company when requested by the data owner or data steward.
- Destroy stored data documents as requested by the data owner or data steward following the Information Disposal Standard.



3. Standard

3.1. Data Asset Inventory Management

- 1) The data steward or asset owner must provide a data asset inventory for documents or records that contain the company's sensitive data. The inventory should specify the data owner, the purpose of usage data, storage location, retention period, and storage formats/types, lawful basis of processing to facilitate systematic and standardized management of data governance practices. The practice refers to Data Classification and Handling Framework document, for example:
 - Record or electronic format shall store in the company's archive in the form of the company's OneDrive/NAS Storage/Cloud Object Storage or database or the company's electronic information system.
 - Documents or physical format shall store in a secure location with access or the company's warehouse.
- 2) The data steward or asset owner must ensure that the data asset inventory is reviewed at least once a year and updated when there is a significant change to the data asset.
- 3) Each item is subject to a retention period under the law or business suitability that demonstrates the necessity and data usage.

3.2. Retention and Archiving Period

The details of Important data that must be archived for a specified period are as follows:

	Category	Retention Period		Data Owner	Lawful Basis / Company Data Management	Format			
		In-System	Archiving			Paper	E-Document	Database/NAS/Server	Picture
1	Human Resources Record								
1.1	Applicant data, only for unsuccessful applicants (Job applicant)	4 years	N/A	CHRO	1. For the company's human resource management 2. (HRM 120) Personnel Management Regulations on Recruitment and Hiring Employees B.E. 2565				
1.2	Employee records for current employees.	Retained all time of the contract	N/A	CHRO					
1.3	Employee resignation records or contract discharge records	10 years following the separation of employment	N/A	CHRO		✓	✓	✓	-
1.4	Separation records for employees fired for misconduct, corruption, committing illegal actions, or violating the company's standard policy.	1 - 40 years	N/A	CHRO					
2	Customer Record								
2.1	Data of customer under contract (Customer Profile)	Retain throughout the period of contract	N/A	H-CSM	Contract Basis	✓	✓	✓	✓
2.2	Customer Profile, when the customer cancels the service (Prepaid, Postpaid), general customers refer to customers with no balance in the system or no overpayment.	2 years after the date cancel the service	N/A	H-CSM	The Notification of the National Broadcasting and Telecommunications Commission regarding the Protection Measure for	✓	✓	✓	✓



	Category	Retention Period		Data Owner	Lawful Basis / Company Data Management	Format			
		In-System	Archiving			Paper	E-Document	Database/NAS/Server	Picture
					Telecommunications Subscriber concerning Privacy Right and Freedom to Communicate by Telecommunications, Article 11 Paragraph 2				
2.3	Customer Profile, when the customer cancels the service (Prepaid, Postpaid), in the case of general customers, this refers to the customer with a balance in the system or has an overpayment	Retain all the time of outstanding balance or overpayment and continue for 2 years from the date of no balance or overpayment (inactive)	N/A	H-CSM	1. Contract Basis 2. The Notification of the National Broadcasting and Telecommunications Commission regarding the Standard for Telecommunications Service Contract, Article 34 3. The Notification of the National Broadcasting and Telecommunications Commission regarding the Protection Measure for Telecommunications Subscriber	✓	✓	✓	✓



	Category	Retention Period		Data Owner	Lawful Basis / Company Data Management	Format			
		In-System	Archiving			Paper	E-Document	Database/NAS/Server	Picture
					concerning Privacy Right and Freedom to Communicate by Telecommunications, Article 11 Paragraph 2				
2.4	Customer Profile, when the customer cancels the service (Prepaid, Postpaid) due to a dispute with the company or a lawsuit.	Retain the data until the case is over.	N/A	H-CSM	The Notification of the National Broadcasting and Telecommunications Commission regarding the Protection Measure for Telecommunication Subscriber concerning Privacy Right and Freedom to Communicate by Telecommunications, Article 11 Paragraph 2	✓	✓	✓	✓
2.5	Customer Order History of customer under contract	Retain throughout the period of contract	N/A	H-CSM	Contract Basis	✓	✓	✓	✓
2.6	Customer Order History, when the customer cancels the service (Prepaid, Postpaid), in the case of general customers, this refers to the customer with a	2 years after the date cancel the service	N/A	H-CSM	The Notification of the National Broadcasting and Telecommunications Commission regarding the Protection Measure for	✓	✓	✓	✓



	Category	Retention Period		Data Owner	Lawful Basis / Company Data Management	Format			
		In-System	Archiving			Paper	E-Document	Database/NAS/Server	Picture
	balance in the system or has an overpayment				Telecommunications Subscriber concerning Privacy Right and Freedom to Communicate by Telecommunications, Article 11 Paragraph 2				
2.7	Customer Order History, when the customer cancels the service (Prepaid, Postpaid), in the case of general customers, this refers to the customer with a balance in the system or has an overpayment	Retain all the time of outstanding balance or overpayment and continue for 2 years from the date of no balance or overpayment (inactive)	N/A	H-CSM	1. Contract Basis 2. The Notification of the National Broadcasting and Telecommunications Commission regarding the Standard for Telecommunications Service Contract, Article 34 3. The Notification of the National Broadcasting and Telecommunications Commission regarding the Protection Measure for Telecommunications Subscriber	✓	✓	✓	✓



	Category	Retention Period		Data Owner	Lawful Basis / Company Data Management	Format			
		In-System	Archiving			Paper	E-Document	Database/NAS/Server	Picture
					concerning Privacy Right and Freedom to Communicate by Telecommunications, Article 11 Paragraph 2				
2.8	Customer Order History, when the customer cancels the service (Prepaid, Postpaid) due to a dispute with the company or a lawsuit.	Retain the data until the case is over.	N/A	H-CSM	The Notification of the National Broadcasting and Telecommunications Commission regarding the Protection Measure for Telecommunication Subscriber concerning Privacy Right and Freedom to Communicate by Telecommunications, Article 11 Paragraph 2 (In cases where it is necessary, according to other laws)	✓	✓	✓	✓
2.9	Retention of user usage details (CDR) when telecommunication services are terminated	The last 6 months of service usage after the current service date.	N/A	H-CSM	1. The Notification of the National Broadcasting and Telecommunications Commission regarding the Protection	✓	✓	✓	-



	Category	Retention Period		Data Owner	Lawful Basis / Company Data Management	Format			
		In-System	Archiving			Paper	E-Document	Database/NAS/Server	Picture
					Measure for Telecommunication Subscriber concerning Privacy Right and Freedom to Communicate by Telecommunications, Article 11 Paragraph 2 2. Emergency Decree on Public Administration in Emergency Situations B.E. 2548				
2.10	Report on VAT Receipt, tax invoice, copy of tax invoice (Tax Invoice/Receipt)	Not less than <u>5 years</u> - but not more than <u>7 years</u>	<u>10 years</u>	CFO	1. Section 87/3 Provisions of the Revenue Code 2. Section 193/31 of the Civil and Commercial Code: The net claim for taxes has a statute of limitations of ten years.	✓	✓	✓	-
2.11	Accounting Records sent to the Revenue Department	<u>5 calendar years</u> following the year of the transaction	<u>10 calendar years</u> following the year of the transaction	CFO	1. Section 13 Accounting Act B.E. 2543 2. Section 193/31 of the Civil and	✓	✓	✓	-



	Category	Retention Period		Data Owner	Lawful Basis / Company Data Management	Format			
		In-System	Archiving			Paper	E-Document	Database/NAS/Server	Picture
					Commercial Code: The net claim for taxes has a statute of limitations of ten years.				
2.12	Fraud customer data	Retain the data until the dispute or issue is over.	N/A	H-CSM / CFO	To use in the company's lawsuit.	✓	✓	✓	-
3	mPay Details Record								
3.1	Service registration data, including detailed information about identification and mPay transaction data (apply for GobaIPay service, activate PromptPay service, start mPay wallet)	10 years when terminated the relationship and no balance in wallet	N/A	MD-MPAY	Anti-Money Laundering Act, B.E. 2542	✓	✓	✓	✓
3.2	Service registration mPay Agent data, including detailed information about identification and mPay transaction data (ROM WebMA, Mobile App, Web Agent, Web Call Center)			MD-MPAY		✓	✓	✓	✓
3.3	mPay Wallet in case there is an outstanding balance in the wallet after the			Retain all the time the customer has a due		MD-MPAY	✓	✓	✓



	Category	Retention Period		Data Owner	Lawful Basis / Company Data Management	Format			
		In-System	Archiving			Paper	E-Document	Database/NAS/Server	Picture
	document storage period is exceeded	credit in the wallet.							
4	eBusiness Portal Record								
4.1	New Register prospect, New Register	<u>10 years</u> after the end of the service contract (inactive)	N/A	H-CSM	Section 193/30 of the Civil and Commercial Code for use in the company's lawsuit.	✓	✓	✓	-
5	AIS Playground Marketplace Record								
5.1	New Register applies for AIS Partner management Platform service for a juristic person.	<u>10 years</u> after the end of the service contract (inactive)	N/A	CCBO/ CEBO	Section 193/30 of the Civil and Commercial Code for use in the company's lawsuit.	✓	✓	✓	-
6	Computer Traffic Data Record								
6.1	Computer traffic data, Log files storage (log file)	<u>At least 90 days</u> from the date that information enters the computer system	N/A	CTO	Section 26 Computer Crime Act	-	✓	✓	-
6.2	In case of necessity, the officer will order the service provider to maintain computer traffic data.	Upon request from the competent official before the expiration of the <u>90 days</u> period under Clause 6.1, for a further		CTO		-	✓	✓	-



	Category	Retention Period		Data Owner	Lawful Basis / Company Data Management	Format			
		In-System	Archiving			Paper	E-Document	Database/NAS/Server	Picture
		period of not more than 6 consecutive months , but not more than 2 years							
7	Partner (WDS, Telewiz, AIS Buddy, ROM, Client store) Record								
7.1	Partnership registration record (AIS Partner Management)	Retained all time during the partnership period	N/A	CCBO/CEBO	Section 193/30 of the Civil and Commercial Code for the company's defending	✓	✓	✓	-
7.2	Partner records when ended the service.	10 years after the expiry of the service contract (inactive)		CCBO/CEBO	✓	✓	✓	-	

Note: Data retention and archiving periods may be longer than those shown in the above table, for the law allows more extended retention periods.

3.3. Safeguarding of Data during Retention and Archiving

3.3.1. Protection of retained/stored in electronic format

Store and back up crucial electronic format data in a secure location designated by the company using the following secure storage and backup method.



Types of archives	Practices
Company's server	<ul style="list-style-type: none"> • Store and backup data only in secure storage within the AIS network • Use authentication to control access to data • Restrict access to authorized users only. • Store the server in a secure computer room. • Encrypt data following IT Security Standards. • Regularly back up the data in the system according to the IT Security Standard Module 15: Backup.
Company's workstations such as laptops, tablet	<ul style="list-style-type: none"> • Always lock the screen when away from the computer. • Keep the portable computer in a cabinet. Locks off when not in use. • Set a strong password and store it in a safe place according to the IT Security Standard. • Scan for malicious software regularly.
Company's storage, such as NAS Storage	<ul style="list-style-type: none"> • Restrict access to data for authorized users only. • Use a user id and password that can identify the user to authorize and verify the identity to access the data.
Office 365 (OneDrive) provided by the company/Company's share point/ Cloud object storage provided by the company	<ul style="list-style-type: none"> • Enable Multi-Factor Authentication. • Choose the individual format for file sharing or share only with specific people. • Set the default sharing format as private every time.
Storage media such as tape, hard disk, object storage other storage	<ul style="list-style-type: none"> • Store in a safe and secure place. to prevent unauthorized access • Storage from external sources or that has been used outside the company must always be checked for viruses before they can be used in-house. If the files on the recording media are encrypted, users must decrypt data before starting the virus scan.



Types of archives	Practices
	<ul style="list-style-type: none"> The storage media sent by the company to a third party must never be used before or have to be fully formatted before saving the data file to be transmitted. Refer to the data destruction standards document.
Portable media (e.g., USB, memory card)	<ul style="list-style-type: none"> Data storage is prohibited.
Personal computer	<ul style="list-style-type: none"> Customer data and the company's sensitive data storage are prohibited.
Private email or public storage	<ul style="list-style-type: none"> Data storage is prohibited.

3.3.2. Protection of retained/stored in publishing format

Sensitive data in a physical format such as paper or memo must be stored safely in the following ways:

Type of archives	Practices
Warehouse	<ul style="list-style-type: none"> Store paper in a securely locked cabinet or shelf. Lock the cabinet or filing room when not in use. Data owner or data steward who is a manager or at a higher level than the manager shall authorize access or copy of documents that contain sensitive information. Data access control officers shall verify access authorization and control the access to the data, such as the name of the data, date and time of access, and purpose of access. Do not remove documents from the storage area without permission.

3.4 Secure data destruction

Information that is unnecessary for business or legal use must be destroyed by a safe method. The data owner or data steward must consider eliminating the stored data beyond the required requirements.

Regarding secure data destruction, refer to the 'Information Disposal Standard' document to prevent data recovery or reconstruction, which will lead to a data breach.



4. Reference

- 1) Customer Information Protection Standard for Employee and Third Party
- 2) Data Classification and Handling Standard
- 3) Information Disposal Standard
- 4) IT Security Standard
- 5) (HRM 120) Personnel Management Regulations on Recruitment and Hiring Employees B.E. 2565
- 6) Cyber Security and Data Protection for Employee Procedure
- 7) Civil and Commercial Code
- 8) Provisions of the Revenue Code
- 9) Accounting Act B.E. 2543
- 10) The Notification of the National Broadcasting and Telecommunications Commission regarding the Standard for Telecommunications Service Contract
- 11) The Notification of the National Broadcasting and Telecommunications Commission regarding the Protection Measure for Telecommunication Subscriber concerning Privacy Right and Freedom to Communicate by Telecommunications
- 12) Emergency Decree on Public Administration, B.E. 2548 (2005)
- 13) Anti-Money Laundering Act, B.E. 2542
- 14) Computer Crime Act

Effective date: from 9 February 2024



Advanced Info Service
Public Company Limited

414 AIS Tower,
Phaholyothin Rd., Samsen Nai,
Phayathai, Bangkok 10400

Annex A: Data Asset Inventory Form

Data Asset Inventory consist of at least the data as following:

Data Owner	Application Owner	Service Name/ Application Name/ System Name	Purpose of Data Usage	Format	Storage Location	Lawful Basis	Retention Period	Reviewed Date	Reviewed by
<i>Refers to company's sensitive data announcement</i>	<i>Define the application owner</i>	<i>Define service name / application name / system name</i>	<i>Define the purpose of data usage</i>	<i>Ex. Paper / e-Document / Database/NA S/Server/ Picture</i>	Paper: <i>define storage location</i> e-Document: <i>define storage location path</i> Database/NAS/Server: <i>define storage location details</i> Picture: <i>define storage location path</i>	<i>Ex. Section 87/3 Provisions of the Revenue Code</i> <i>*Refers to the Lawful Basis column at the table of topics 3.2</i>	<i>Ex. 10 Years</i> <i>Refers to Retention period from table of topics 3.2</i>	<i>Ex. 08/08/2022</i>	<i>Define reviewer's name</i>

* In case of data collection purpose in Lawful Basis column does not match in the table of topics 3.2, please contact Data Protection Office unit