-Translation-

Data Governance Policy

Eastern Water Resources Development and Management Public Company Limited and its subsidiaries prioritize the protection and security of data, including methods for maintaining confidentiality, reliability, and availability of data. Therefore, this Data Governance Policy has been established with the following key points:

1. Definitions

The Company refers to Eastern Water Resources Development and Management Public Company Limited.

The Group refers to the Eastern Water Resources Development and Management Public Company Limited and its subsidiaries

Subsidiary refers to a company that meets one of the following criteria:

(1) A company controlled by the company.

(2) A company under the control of the company as mentioned in (1), continuing in succession.

Employee refers to permanent employees, probationary employees, contract employees, and temporary employees

Data refers to information in any form, whether in documents, electronic data, or any other format, under the possession of the group.

Confidential Data refers to data under the group's control that is ordered not to be disclosed. Disclosure of all or part of this data may impact the group's commercial interests, credibility, or other aspects.

Restricted Data refers to data known only to specific groups of people. Disclosure may affect the group's internal management.

Personal Data refers to information about individuals that can identify them directly or indirectly, excluding data of deceased persons.

Sensitive Personal Data refers to personal data classified by law as sensitive personal data under Section 26 of the Personal Data Protection Act B.E. 2019, such as race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal history, health data, disability, union membership, genetic data, biometric data, etc., or any other data that similarly affects the data subject as specified by law.

Internal Data refers to data intended for internal use within the group, including data disclosed to specific individuals such as directors, executives, employees, partners, customers, government agencies, etc.

Public Data refers to data that can be disclosed and accessed by the public, intended for external dissemination. Disclosure of such documents should not impact on the group, employees, customers, or any individuals, such as news, printed media, website information, advertisements, or job announcements of the group.

2. Objectives of the Data Governance Policy.

2.1 To provide guidelines for employees and related individuals to correctly follow the data governance policy in compliance with relevant laws, regulations, and principles of good corporate governance and business ethics, such as the Personal Data Protection Act B.E. 2019, the Public Limited Companies Act, and relevant securities and exchange laws.

2.2 To establish standards for data storage, destruction, classification, usage, request, and transfer.

2.3 To communicate the data governance policy to employees and publish it on the company's and subsidiaries' websites for external parties to be informed.

3. Data Governance Policy Practices

3.1 Data Storage and Destruction

1) Data collected must be necessary for operations, accurate, and comply with the company's and subsidiaries' personal data protection policy.

2) Classify data according to confidentiality levels: confidential, restricted, personal, internal, and public data, as outlined in **Appendix A**. Store data according to its confidentiality level, ensuring secure storage locations that consider the risks of data leakage and equipment deterioration. Data storage must comply with the guidelines specified in **Appendix B**.

3) Create a department data registry and review it at least once a year, including defining the following:

(1) Define data types according to confidentiality levels: confidential, restricted, personal, internal, and public data.

(2) Define the data storage duration, considering the necessity of data usage, legal requirements, and audit needs from internal and external agencies such as the Audit Office, Revenue Department, etc., and define data destruction methods.

(3) Define the employees responsible for data storage.

(4) Define access rights for employees who need to use the data for their duties and immediately revoke access rights when the data is no longer needed, such as when

employees resign or are transferred, or when it is necessary to revoke access rights to maintain data security.

(5) Define the authority to approve data requests.

4) When the data storage period expires, destroy the data according to the guidelines in **Appendix B.**

3.2 Data Usage

1) Employees must not use data in ways that may harm the company.

2) Employees must use data only for operational purposes and not for other purposes.

3) Personal data must be used according to the purposes specified in the privacy policy (Privacy Notice). If it is necessary to use personal data for other purposes beyond those specified in the privacy policy, seek advice from the legal and compliance department to comply with the Personal Data Protection Act B.E. 2019.

3.3 Data Request, Transfer, and Disclosure

1) Do not transfer or disclose data that violates laws, regulations, orders, policies, or practices, regardless of the format.

2) Employees must not transfer or disclose confidential, restricted, personal, or internal data unless necessary for operations or legal compliance.

3) When transferring or disclosing confidential, restricted, personal, internal, or public data, follow the guidelines in **Appendix C**.

4) Public information must be approved by the CEO or authorized personnel before being disclosed to the public.

3.4 Responsibilities for Data Security

1) Employees must prevent data from being damaged, lost, altered, accessed, or disclosed without authorization.

2) Employees must monitor and report any abnormalities that may affect data security to their supervisors immediately upon noticing such abnormalities.

3) In case of data leakage or any other incidents related to data that may cause damage to the group, employees must report to their supervisors immediately upon discovering such incidents for corrective actions.

Announced on 24 October 2024.

-Signed-

.....

President & CEO

Appendix A: Guidelines for Data Classification by Confidentiality Levels.

Confidentiality Levels of Data				
Confidential Data	**Restricted Data**	**Personal Data**	**Internal Data**	**Public Data**
Data under the group's control that is ordered not to be disclosed. Disclosure of all or part of this data may impact the group's commercial interests, credibility, or other aspects. This data must be strictly secured, and access must be limited. Examples: Unpublished financial statements, important contract documents, proprietary R&D information, proprietary production processes, project bidding information, and any critical trade secrets that could impact the	**Data is known only to specific groups of people. Disclosure may affect the group's internal management. This data must be strictly secured, and access must be limited.** Examples: Meeting agendas on confidential matters such as director appointments, employee salary adjustments, and CEO performance evaluations.	**Information about individuals that can identify them directly or indirectly, excluding data of deceased person. Unauthorized disclosure or use of this data may impact or harm the group according to the Personal Data Protection Act B.E. 2019. This data must be strictly secured, and access must be limited** Examples: Names, contact information, birth dates, photos, nationalities, religions of directors, shareholders, customers, partners who are individuals, representatives of corporate partners, employees	**Data intended for internal use within the company, including data disclosed to specific groups such as directors, executives, employees, partners, customers, government agencies, etc. This data must be secured, and access must be limited appropriately. Unauthorized external disclosure may impact the company** Examples: Company regulations, work rules, training documents, group insurance benefits, personal income tax submission documents, provident fund	**Data that can be disclosed and accessed by the public, intended for external dissemination** Examples: Annual reports, Form 56-1 One Report, sustainability reports (SD Report), information on the company's website, disclosed financial statements.

Confidentiality Levels of Data				
Confidential Data	**Restricted Data**	**Personal Data**	**Internal Data**	**Public Data**
company's commercial interests or credibility.		of partners, tenants, employees of tenants, visitors, and users of the building or operational areas.	documents, documents used for communication with government agencies.	

Appendix B: Guidelines for Data Storage, Maintenance, and Destruction

1. Hard Copy Documents (Both Originals and Copies).

Data Management	Confidentiality Levels of Data				
	Confidential Data	**Restricted Data**	**Personal Data**	**Internal Data**	**Public Data**
Hard Copy Document Storage	1. Documents should be stored in an appropriate area in a locked cabinet. 2. In cases where documents are stored outside the company, they must be contained in a secure package	1.Documents should be stored in an appropriate area in a locked cabinet. 2. In cases where documents are stored outside the company, they must be contained in a secure package.	1.Documents should be stored in an appropriate area in a locked cabinet. 2. In cases where documents are stored outside the company, they must be contained in a secure package.	1. Documents should be stored in an appropriate area. 2. In cases where documents are stored outside the company, they must be contained in a secure package.	Consider as appropriate.
Hard Copy Document Duplication	Copying hard copy documents must be authorized by the person	Copying hard copy documents must be authorized by the person	Copying hard copy documents must be authorized by the person	Consider as appropriate.	Consider as appropriate.

Data Management	Confidentiality Levels of Data				
	Confidential Data	Restricted Data	Personal Data	Internal Data	Public Data
	with authority according to clause 1.3(5).	with authority according to clause 1.3(5).	with authority according to clause 1.3(5).		
Hard Copy Document Destruction	When the data storage period expires, destroy the documents using a shredder.	When the data storage period expires, destroy the documents using a shredder.	When the data storage period expires, destroy the documents using a shredder and record the destruction details.	When the data storage period expires, destroy the documents using a shredder.	When the data storage period expires, destroy the documents using a shredder.

Appendix B: Guidelines for Storage, Retention, and Disposal of Data

2. Electronic File Data.

Data Management	Confidentiality Levels of Data				
	Confidential Data	Restricted Data	Personal Data	Internal Data	Public Data
Electronic File Storage	1.Store on company computers 2. Store on SharePoint or systems provided by the company 3. If storing on external storage devices such as	1.Store on company computers 2. Store on SharePoint or systems provided by the company 3. If storing on external storage devices such as	1.Store on company computers 2. Store on SharePoint or systems provided by the company 3. If storing on external storage devices such as	1.Store on company computers 2. Store on SharePoint or systems provided by the company 3. If storing on external storage devices such as	Consider as appropriate.

Data Management	Confidentiality Levels of Data				
	Confidential Data	**Restricted Data**	**Personal Data**	**Internal Data**	**Public Data**
	external hard drives or flash drives, a device access password must be set.	external hard drives or flash drives, a device access password must be set.	external hard drives or flash drives, a device access password must be set.	external hard drives or flash drives, a device access password must be set.	
Access Permission to Storage Locations	Must be approved by the authorized personnel as specified in Clause 1.3(5), via email or any format that can verify the identity of the approver.	Must be approved by the authorized personnel as specified in Clause 1.3(5), via email or any format that can verify the identity of the approver.	Must be approved by the authorized personnel as specified in Clause 1.3(5), via email or any format that can verify the identity of the approver.	Must be approved by the authorized personnel as specified in Clause 1.3(5), via email or any format that can verify the identity of the approver.	Consider as appropriate.
Copying of Electronic Files	Must be authorized by the authorized personnel as specified in Clause 1.3(5)	Must be authorized by the authorized personnel as specified in Clause 1.3(5)	Must be authorized by the authorized personnel as specified in Clause 1.3(5)	Consider as appropriate.	Consider as appropriate.
Deletion of Electronic Files, including Emails	Must be permanently deleted and unrecoverable.	Must be permanently deleted and unrecoverable.	Must be permanently deleted and unrecoverable.	Consider as appropriate.	Consider as appropriate.

Appendix C: Data Request, Data Transfer, and Data Disclosure (in Hard Copy and Electronic File Formats)

Data Management	Confidentiality Levels of Data				
	Confidential Data	**Restricted Data**	**Personal Data**	**Internal Data**	**Public Data**
Data Request/Data Transfer/Data Disclosure to External Parties	1. Make a written request, such as via email, etc. 2. The authorized personnel as per Clause 1.3(5) must review and approve the request, considering the necessity of using the data. Other conditions may also be set, such as defining the purpose of data use or specifying the duration of data use. 3. If the data is received by an employee, the data must be used only for the purpose specified in the request, and the employee must not	1. Make a written request, such as via email, etc. 2. The authorized personnel as per Clause 1.3(5) must review and approve the request, considering the necessity of using the data. Other conditions may also be set, such as defining the purpose of data use or specifying the duration of data use. 3. If the data is received by an employee, the data must be used only for the purpose specified in the request, and the employee must not forward or disclose the data to other individuals.	1. Make a written request, such as via email, etc. 2. The authorized personnel as per Clause 1.3(5) must review and approve the request, considering the necessity of using the data. Other conditions may also be set, such as defining the purpose of data use or specifying the duration of data use. In this case, the purpose for which employees or external parties will use personal data must be specified in the Privacy Notice before approval can be granted.	Consider as appropriate.	Consider as appropriate.

Data Management	Confidentiality Levels of Data				
	Confidential Data	**Restricted Data**	**Personal Data**	**Internal Data**	**Public Data**
	forward or disclose the data to other individuals. The data must be destroyed immediately when no longer needed. 4. If the data is received by an external party, a confidentiality agreement must be established between the company and the external party.	4. If the data is received by an external party, a confidentiality agreement must be established between the company and the external party.	3. If the data is received by an employee, the data must be used only for the purpose specified in the request and must not be forwarded or disclosed to others. 4.If the data is received by an external party, a confidentiality agreement must be established between the company and the external party, as well as a Data Processing Agreement (DPA) between the data controller and the data processor.		
Document Delivery (Hard Copy)	The sender must ensure the completeness and accuracy of the delivery.	The sender must ensure the completeness and accuracy of the delivery.	The sender must ensure the completeness and accuracy of the delivery.	The sender must ensure the completeness and accuracy of the delivery.	Consider as appropriate.

Data Management	Confidentiality Levels of Data				
	Confidential Data	**ข้อมูลปกปิด**	**Confidential Data**	**ข้อมูลภายใน**	**Confidential Data**
Sending Electronic Files via Electronic Systems (e.g., email, etc.)	1. Set a secure password with at least 8 characters, including uppercase letters, lowercase letters, numbers, and special symbols. Avoid using birthdates or personal names. The password used to access the data must be sent separately from the data file itself. 2. If sending files to employees within the same company group, files can be shared or sent via a link through SharePoint, specifying the recipient's email address.	Consider as appropriate.	Consider as appropriate.	Consider as appropriate.	Consider as appropriate.