Document Management and IT Policies

Company Name: COERR Foundation
Address: 122/11 CBCT Building 6th floor, Soi Nonsi 14 (Naksuwan), Nonsi Road, Yannawa District, Bangkok, Thailand
Effective Date: January 2024 **Revision Date:** 1 August 2025
Focal Point: Sittikorn Somthai (IT Assistant) Lalita Rodthasana (Account Supervisor)
Purpose: This policy aims to ensure that the document retention, data and information technology resources are used responsibly, securely, and in compliance with legal, regulatory and business requirements. It provides guidelines for managing documentation, protecting, and using data and IT systems.
Scope: This policy applies to all employees, contractors, volunteers, and third-party service providers who access the organization's data or IT resources.
Data Protection and Privacy: • All personal and confidential data must be stored securely with access limited to authorized personnel. • Data must be encrypted during transmission and storage where appropriate. • Staff must comply with data protection laws (e.g., GDPR, local data privacy laws).
Acceptable Use of IT Resources • IT resources are provided for working purposes. • Users must not engage in activities that are illegal, harmful, or disruptive (e.g., downloading pirated software, spreading malware). • Personal use of IT resources should be limited and not interfere with official duties.
Software and Hardware Usage: • Only authorized software may be installed on organizational devices. • Hardware must be used responsibly and reported immediately if lost or damaged.
Monitoring and Auditing: • The organization reserves the right to monitor IT systems for compliance, security, and operational purposes. • Annual review, updating policies and follow up any actions required. • Regular audits will be conducted to ensure adherence to this policy.

Roles & Responsibilities:	
Focal Point	To activate and implement the IT policies, provide instructions to users, monitor, ensure compliance, report concerns and incident.
Management Team	To ensure that the policies are fit for their purpose over time and keep COERR safe from potential threats.
COERR Employees	All employees both permanent staff and contract staff including consultants and volunteers adhere to COERR's IT policy.
Detail Process and Controls:	
<u>Access Policy</u>	Password and Access Control • All users are required to create strong, unique passwords and update them regularly to maintain system security. • System and data access must be granted according to individual job responsibilities, following the principle of least privilege. • User accounts must be deactivated immediately upon termination of employment or change in role that no longer requires access. • Access to the COERR's email system is strictly reserved for COERR personnel only. • Each staff member must be assigned a unique email address in alignment with their designated role. The organization will regularly monitor the usage of email accounts to ensure they are actively used by legitimate users. • Users will be educated and guided on creating strong passwords to protect their personal and work-related information on mail servers and are required to reset passwords in a timely manner. • A standard email storage limit of 150 GB will be allocated per individual to manage system capacity effectively. • User profiles must be properly configured to grant access to key systems, including the COERR Data-based Tracking System and COERR Reporting System, hosted on both Google Drive and external servers.
<u>Protection Policy: System Security and Data Backup</u>	• An anti-virus program (Kaspersky Standard Device Software) must be installed on all COERR computers to protect against potential threats that could damage hardware or compromise the integrity of data systems.

	The expiry dates of software license must be closely monitored, and renewals must be conducted promptly to ensure uninterrupted protection. • Regular backups of the COERR database Tracking System and COERR reports must be conducted and stored in secure fallback locations, including an external hard disk and a remote server situated outside COERR's head office. These backups are essential for ensuring data availability and business continuity. • The data recovery process must be clearly documented, including step-by-step procedures for restoring data from backup sources in the event of a disaster or system failure. This documentation is crucial for effective emergency response and minimizing data loss. • All computer hardware procurements must comply with legal software licensing requirements. Each computer must be equipped with a licensed version of Windows 10 or Windows 11, as well as a licensed copy of Microsoft Office, to ensure both operational efficiency and legal compliance.

<u>Asset Management</u>	○ All IT hardware assets must be clearly labeled with a tag ID or asset code that corresponds to the asset registration details recorded in the Financial System. Custodians must formally acknowledge receipt of assigned assets.
	○ Asset registration records must include the following information:
	  ○ Photograph of the asset
	  ○ Date of acquisition
	  ○ Invoice or proof of purchase
	  ○ Name, position, and location of the assigned custodian
	• Physical verification of IT assets must be conducted at least once annually by the designated field supervisor or manager to ensure accuracy and accountability.
	• Any change in asset custodian or asset location must be documented using the Asset Transfer Template, which must be signed by both the outgoing and incoming custodians.
	• All cases of asset damage, loss, or disposal must be reported to the IT Officer for investigation. Final approval for asset disposal must be granted by the Finance and Administration Director.

Document Retention Policy	• This policy outlines how long specific types of documents must be retained and when they should be archived or securely disposed of. The policy ensures compliance with legal, regulatory, and business requirements while optimizing document storage. • **Retention Periods**: Specifies how long documents must be retained based on legal, regulatory, or business requirements. • **Document Categories**: The policy categorizes documents by type (e.g., financial, legal, HR) and applies different retention periods to each. • **Disposal Procedures:** Defines how documents should be securely disposed of when they are no longer needed, such as shredding or permanent deletion. • **Compliance and Security**: The policy must ensure that retention and disposal processes comply with data protection laws and security standards. • See **Appendix 1** – a comprehensive document retention specifying retention periods and procedures for maintaining and organizing documents that align with both Thai tax laws and donor requirements, regularly review and update the policy to ensure ongoing compliance and effective record-keeping.

Incident Report	• Common causes of system failure may include, but are not limited to, cyber-attacks, phishing or scam attempts, software malfunctions, network disruptions, and hardware failures.
	• In the event of a system incident, a formal report must be prepared summarizing the following:
	  ○ The nature of the incident and immediate response actions taken
	  ○ Identification of the root cause
	  ○ Assessment of the operational and financial impact
	  ○ Corrective actions implemented to resolve the issue
	  ○ Preventive measures to avoid recurrence
	• A draft of the incident report must be submitted to the Management Team within 10 days of the incident occurrence.

Enforcement:

• Violations of this policy may result in disciplinary action, up to and including termination of employment or legal action.

Policy Review:

• This policy will be reviewed annually or as needed to ensure its relevance and effectiveness.

Link to COERR Code of Conduct & Child Protection Policy:

- COERR recognizes that data protection is a key component of Child Protection, particularly when handling personal data related to children, vulnerable adults, and affected populations. This Data and IT Policy must be read in conjunction with COERR's Code of Conduct and Child Protection Policy, which outlines the principles and procedures for ensuring the safety and dignity of all individuals with whom we work.
- All staff must ensure that data collection, storage, and sharing practices uphold the principles of do no harm, confidentiality, and informed consent as defined in the Safeguarding Policy.

In particular:

- Any digital images, case notes, or identifiable information of beneficiaries, especially children, must be securely stored and accessed only by authorized personnel.
- Inappropriate access or misuse of such data is considered a Code of Conduct breach and will be addressed in accordance with both the IT Policy and Child Protection Policy.
- Reports of child protection concerns that involve IT or data misuse must follow the established reporting and referral procedures.