BUSINESS PROCESSES AND SECURITY POLICY

CYBERTECH CORPORATION
POLICY: ASSET MANAGEMENT

March 17, 2024

Student ID	Student Name
100952215	Mehul Patel
100956102	Boby Anna John
100955867	John Joshy Francis
100950933	Niharkumar Jadav
100344918	Jaison Bhatti

1. TABLE OF CONTENTS

2. REVISION HISTORY

Version	Title	Author	Issue Date	Classification	Changes
1.0	Asset Management Policy	Mehul Patel John Joshy Francis Boby John Niharkumar Jadav Jaison Bhatti	March 17, 2024	CONFIDENTIAL	Creation

2.1 REFERENCE

This policy was created using the ISO 27001:2013 as the reference.

3. POLICY OVERVIEW

This section describes the purpose and scope of the Asset Management Policy

3.1 PURPOSE

The main purpose of the Asset Management Policy is to:

- Identify Cybertech Corporation's organizational assets and define appropriate protection responsibilities, to ensure that information receives an appropriate level of protection in accordance with its importance to Cybertech Corporation and to prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

3.2 SCOPE

The policy statements written in this document are applicable to all resources at Cybertech Corporation and at all levels of sensitivity such as:

- All full-time, part-time and temporary employees staffed by Cybertech Corporation.
- Contractors and consultants who are working on behalf of Cybertech Corporation.
- Any individual or third-party groups who have been granted access to Cybertech Corporations's internal systems and information.

4. POLICY STATEMENT

The following sections will present the policy statement in 3 sections broken down into 10 main aspects:

Responsibility for Assets

Inventory of Assets

Ownership of Assets

Acceptable Use of Assets

Return of Assets

Information Classification

Classification of Information

Labelling of Information

Handling of Assets

Media Handling

Management of Removeable Media

Disposal of Media

Physical Media Transfer

4.1 RESPONSIBILITY FOR ASSETS

4.1.1 INVENTORY OF ASSETS

- Cybertech Corporation shall establish a process and procedure for recording, documenting, maintaining, and updating an inventory of all information assets owned and managed by Cybertech Corporation. This inventory shall be categorized into four main types: hardware, software, information, and people.
- Assets inventory shall contain the identification, description, location, classification, value, and ownership of the asset.

4.1.2 OWNERSHIP OF ASSETS

- Cybertech Corporation shall assign an Owner for each asset and they will be responsible for assigning classification to assets. They will also be responsible for protecting, handling and managing of critical assets

Each asset will be identified as such:

Role	Description	Responsibilities
Owner	Managers of organization units where their primary tasks are associated with authority of assets	▪ Classifying the assets. ▪ Applying appropriate labels to identify sensitive data as needed. ▪ Ensuring that proper controls are in place to address confidentiality, integrity, and availability of information. ▪ Conducting regular reviews of asset classifications. ▪ Ensuring availability of information at all times. ▪ Informing data custodians and users about the necessary security measures and requirements ▪ Regularly updating and assessing access limitations and categorizations in line with relevant access control protocols. ▪ Routinely revising backup and recovery plans, including the testing of backup processes,

		restoration speed, and data integrity post-recovery.
Custodian	Administrators and Service Providers designated by the owner to manage and process information assets	▪ Protecting Cybertech Corporation's information to ensure its confidentiality, integrity and availability. ▪ Applying information security policies and best practices to the information. ▪ Identifying and documenting the criteria for legitimate access to the corporation's data. ▪ Conducting systematic backup procedures and tests for data accuracy ▪ Detecting and responding to security violations, security breaches and vulnerabilities. ▪ Monitoring compliance with information security policies and best practices. ▪ Notifying the appropriate parties of any potential or actual security incidents or data breaches. ▪ Taking prior approval of the owner before sharing information. ▪ Performing regular administrative tasks.
User	Users and groups authorized by the owner to access information assets	▪ Understanding the information asset classifications, abiding by the security controls defined by the owner and applied by the custodian. ▪ Preserving the established asset classification and labelling system as determined by the data owner. ▪ Consulting the data owner in cases of unlabeled information or uncertain classification. ▪ Utilizing the data solely for sanctioned activities of Cybertech Corporation. ▪ Alerting the relevant authorities, custodian or owner, regarding any observed or potential security incidents or data compromises.

4.1.3 Acceptable Use of Assets

- Cybertech Corporation will establish an “Acceptable Use Policy” outlining the rules for managing assets, ensuring these guidelines reflect the company’s values of openness, trust, and integrity.
- The use of all Cybertech Corporation assets must align with business objectives as specified in the information security policy.
- All Cybertech Corporation employees:
  - Must recognize and commit to the protection of the company’s information, abiding by the information security policy in their everyday tasks.
  - Are prohibited from engaging in unlawful actions, including unauthorized asset access, hacking, introducing malware, or any activities that could hinder the operational functionality of these assets.
- Cybertech Corporation will engage in monitoring, recording, or conducting regular audits on the usage of its information systems and equipment. Any misuse or suspicious activity should be promptly reported to the designated company authority.

4.1.4 Return of Assets

- The Human Resources Department alongside other pertinent departments at Cybertech Corporation must ensure that employees return all company assets (like laptops, desktops, and printers) when they leave the company, as dictated by the exit procedures. This includes, but is not limited to:
  - Implementing a standardized procedure for asset return, which could involve comparing returned items against an inventory list.
  - Establishing a process for either returning or securely disposing of all types of company information.
  - Setting forth protocols for securely deleting Cybertech Corporation data from personal devices that were used for work.
- During the notice period of employee termination, Cybertech Corporation will enforce measures to prevent the unauthorized duplication of critical company data, including software, business intelligence, and confidential information.

4.2 INFORMATION CLASSIFICATION

Cybertech Corporation shall ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

4.2.1 CLASSIFICATION OF INFORMATION

- Cybertech Corporation will categorize information according to its sensitivity, importance, confidentiality, privacy needs, and overall value.
- Every piece of information produced or utilized by Cybertech Corporation, regardless of its format, will be assigned one of four classification levels:

Classification	Description
Highly Confidential	▪ This level is designated for extremely sensitive business information exclusive to Cybertech Corporation's internal use. ▪ If such information were disclosed without authorization, it could severely jeopardize the company's long-term strategies or even its existence, significantly harming the organization and its stakeholders. ▪ Legal consequences may follow any unauthorized sharing or exposure of this information. ▪ Individuals must obtain specific permission to access this data, with authorization granted by the Information Owner. ▪ The Information Owner will also evaluate the associated risks and approve access accordingly. ▪ Examples include Social Security numbers, client personal identification details, financial documents, employee personal data, banking information, strategic communications, and management directives.
Confidential	▪ Pertains to sensitive data intended for internal use that, if disclosed without permission, could disrupt Cybertech Corporation's short-term operational goals or tactics. ▪ The proprietor of the information is tasked with establishing protective measures against unauthorized access, alteration, or release. ▪ Instances include proprietary or in-development intellectual assets, procurement data, supplier agreements, system configurations, log files, and internal audit findings or risk evaluations.

Internal	▪ Encompasses all business information disseminated through internal communications or notices that is less sensitive than “Confidential” material. ▪ If information not explicitly labeled as “Confidential” or “Public” is released, it should be considered “Internal Use Only.” ▪ Unauthorized release may lead to slight embarrassment or operational hitches but won’t critically affect Cybertech Corporation, its workforce, or stakeholders as the leakage of Confidential information would. ▪ Adequate security protocols should be enforced for internal data. ▪ Examples are standard correspondences, staff bulletins, office memos, company guidelines and procedures, educational resources, and staff notices.
Public	▪ This category includes information that doesn’t fall under the other specified classes and has been cleared by Cybertech Corporation’s leadership for public distribution. ▪ There’s no risk of improper disclosure here, and such information can be freely shared without adverse effects on Cybertech Corporation. ▪ Examples include informational booklets, press announcements, promotional content, the company website, employee directories, and marketing resources.

- The designated owner for each type of information within Cybertech Corporation is tasked with determining the most suitable classification level based on the company’s operational necessities.
- When amalgamating information of varying sensitivity levels, the entire set should be assigned the highest, most restrictive classification present among the individual elements.
- It is mandatory for all employees of Cybertech Corporation to adhere to the established protocol for information classification.
- The classification assigned to each piece of information must undergo a biannual review to ensure its accuracy and relevance.
- Any changes in the value, sensitivity, or criticality of the information throughout its lifecycle should prompt an update to its classification status accordingly.

4.2.2 LABELLING OF INFORMATION

- Cybertech Corporation is accountable for the appropriate labeling of assets and ensuring the accuracy of asset records, adhering to the corporation's sanctioned naming conventions.
- Asset management, including maintenance, handling, storage, transportation, and disposal, must align with the directives provided in the Information Labelling and Handling Guidelines that correspond to the asset's classification.
- For all document holding information classified as "Highly Confidential", Cybertech Corporation shall:
  - Secure storage in locked cabinets or drawers.
  - Ensuring any room containing such documents remains locked when unattended.
  - Avoiding the practice of leaving keys within the office unless the authorized personnel are present.
- Cybertech Corporation will craft and enforce procedures to govern the handling and storage of information, safeguarding against unauthorized access or mishandling.
- Physical labels on documents, hardware, and removable media should reflect the designated security classification, as dictated by the Asset Management Policy.
- Media classified as "Highly Confidential" must not be transferred to external parties or third parties without explicit authorization from Cybertech Corporation, supported by a valid business rationale. In situations requiring media return to a third party, particularly if damaged, the third party must enter into a non-disclosure agreement.

4.2.3 HANDLING OF ASSETS

- The Information Security Officer alongside Cybertech Corporation is tasked with creating and implementing detailed procedures for the management, processing, storage, and transmission of information, categorized by its classification, to prevent unauthorized access or misuse.
- Employees responsible for handling Cybertech Corporation's sensitive data are required to adhere to stringent security and access control policies to shield this information from unauthorized exposure.

- The deployment of storage devices and peripherals, such as DVD writers, USB ports, and flash drives, should be strictly regulated and confined to business purposes. Centralized systems to monitor and restrict their usage should be considered.
- When not in operation, portable storage devices containing unencrypted, sensitive information from Cybertech Corporation must be secured in lockable furniture.
- Permissions to access sensitive or critical information within Cybertech Corporation should be assigned individually, based on the necessity of the information for the person's role, and must always receive prior approval from the company's management.

4.3 MEDIA HANDLING

4.3.1 MANAGEMENT OF REMOVABLE MEDIA

- Information security protocols must be integral to the governance of removable media and the associated technologies within Cybertech Corporation.
- The management of removable media should adhere to the following guidelines:
  - All media must be preserved in a secure and controlled environment, complying with both the manufacturer's recommendations and Cybertech Corporation's established information security policies and procedures.
  - Should the media become redundant, any data designated for deletion must be irretrievably erased to prevent potential recovery.
  - Usage of removable media drives is permitted solely based on legitimate business requirements.
  - To safeguard against data corruption or loss, multiple instances of crucial Cybertech Corporation data should be replicated and maintained across distinct storage media.

4.3.2 DISPOSAL OF MEDIA

- Disposal of sensitive media by Cybertech Corporation must align with the "Asset Management Policy and Procedure," adhering to stipulated retention periods or the end-of-use status of the media. Documentation and notification to the Owner are required post-disposal.
- Prior to the elimination or disposal of any media, authorization must be secured from the owner.
- A detailed media disposal log should be maintained to record all dispositions, ensuring a comprehensive audit trail is available.
- Secure disposal methods for sensitive Cybertech Corporation documents and electronic data that are no longer required should be employed, utilizing sanctioned equipment and techniques to guarantee irretrievability. These methods may include, but are not limited to:
  - shredding,
  - pulping/recycling,
  - or incineration.

- A disposal record for sensitive materials should be kept for a minimum of five years, in compliance with Cybertech Corporation's regulatory obligations. This record should minimally comprise of:
  - the disposal date,
  - the individual responsible for disposal,
  - the owner's name,
  - the owner's approval,
  - and the method of disposal utilized.
- Prior to transferring storage media to a third party, all sensitive data from Cybertech Corporation should be effectively erased, obscured, or substituted using approved methodologies

4.3.3 PHYSICAL MEDIA TRANSFER

- To safeguard sensitive data during transit of physical media, cryptographic techniques are recommended to preserve confidentiality, integrity, and authenticity.
- When transporting sensitive hardcopy information, Cybertech Corporation should utilize reliable courier services or registered mail, ensuring the process includes tracking via a bill of lading number and necessitates a signature upon receipt. The handover of such information to intermediaries is strictly prohibited.