BUSINESS PROCESSES AND SECURITY POLICY

CYBERTECH CORPORATION POLICY: CRYPTOGRAPHY

March 31, 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	Cryptography Policy	Mehul Patel	March 27, 2024	PUBLIC	Creation
1.1		John Joshy Francis	March 28, 2024	PUBLIC	QA
1.2		Boby John	March 29, 2024	PUBLIC	Update
1.3		Niharkumar Jadav	March 30, 2024	PUBLIC	Update
1.4		Jaison Bhatti	March 31, 2024	PUBLIC	Update

3. APPROVAL

Name	Title	Date	Approved
Ahmad Barakat	Professor of MGMT1100	March 31, 2024	YES

4. REFERENCE

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

3. POLICY OVERVIEW

3.1 PURPOSE

The purpose of the Cryptography Policy is to guarantee the appropriate and efficient application of encryption to safeguard knowledge's honesty, secrecy, and validity.

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.

3.3 TERMS AND DEFINITIONS

Terms	Definition
Asset	Any item of value to the organization that needs to be protected, including information, software
Authentication	Process of verifying the identity of a user
Authorization	Granting of rights to a user, group, or system to access data or resources
Background Check	Process of verifying the legal, financial, and personal character of an employee or potential employee
Compliance	Adhering to laws, regulations, guidelines, and specifications relevant to the organization
Data Protection	Measures and processes for ensuring the privacy and protection of personal data
Encryption	Process of converting information or data into a code to prevent unauthorized access
Firewall	Network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules
Incident	Event that has the potential to compromise the integrity, confidentiality, or availability of information

Terms	Definition
Incident Management	Process of identifying, managing, recording, and analyzing security threats or incidents
Security Training	Programs designed to educate employees about the importance of information security and practices and behaviours that protect the organizations assets.

3.4 ROLES AND RESPONSIBILITIES

Roles	Responsibilities
CTO	Provide approval and official endorsement to this policy
CISO	Reviewing the policy and providing formal support
IT Director	Creation and upkeep of this policy, approving any deviations from its stipulations, and actively encouraging adherence among all stakeholders
Supervisors	Assist employees and contractors in understanding this policy's requirements and promptly address and notify the IT department about any breaches of this policy
Administrators	Ensure that contracts clearly specify the security responsibilities and obligations of all involved parties
Human Resource	Responsible for introducing new employees and contractors to Cybertech's IT and Security policies on their first day of employment and aiding all employees and contractors in understanding this policy's requirements
Users	Expected to report any observed and suspected breaches of this policy to their supervisor, manager, or team lead immediately

4. POLICY STATEMENTS

4.1 Cryptographic Controls

4.1.1 Policy on the Use of Cryptographic Controls

4.1.2 Key Management

4.1 CRYPTOGRAPHIC CONTROLS

To guarantee the appropriate and efficient application of encryption to safeguard knowledge's honesty, secrecy, et/or validity.

4.1.1 POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS

It is required to create and execute an agreement for the use of cryptographic controls for data security.

- □ In order to preserve the integrity of data and privacy, algorithms for encryption must be implemented as needed for Cybertech Corporation's vital business applications that handle sensitive information.

- □ Following encryption methods are going to be used for sending private information over public networks or the Internet in order to protect it:
  - The utilization of encryption to protect data privacy while it's being transferred or stored.
  - application of coded messages or digital signs to confirm the accuracy and legitimacy of personal information.
  - Utilizing encryption methods to reliably identify users and provide not repudiating, which provides indisputable proof of the happening or non-occurrence of an event or act.

4.1.2 KEY MANAGEMENT

Over the course of their entire career, regulations regarding the use, security, and lifetime of cryptographic keys must be devised and put into effect.

- □ Regarding cryptography usage inside Cybertech Corporation's network, a safe Information Administration plan (encompassing cryptographic passwords & methods) is being developed, guaranteeing the security and integrity of cryptographic activities.

- □ Cybertech Company is going to use Public Key Infrastructure (PKI) to facilitate the deployment of encrypted certifications for vital applications on its intranet, which are customized to address particular business requirements.

- □ To ensure the secure transportation and durability of cryptographic substances, devices assigned to generate, store, and archive digital keys shall be physically protected to thwart unwanted access, alteration, loss, or misuse of both secret and private keys.

5. POLICY COMPLIANCE

5.1 COMPLIANCE MEASUREMENT

- Cybertech's information security management team will ensure staff and guests will follow this policy by having reports from business tools, internal and external audits, and through feedback to the owner of this policy

5.2 EXCEPTIONS

- Any exception to the policy need to be approved and documented beforehand by Cybertech's information security management team. Exceptions will be reviewed by the management review team

5.3 NON-COMPLIANCE

- If an employee is found violating this policy, corrective action will be taken against them, which can be escalated to the point of job termination

5.4 CONTINUAL IMPROVEMENT

- As part of its continuous improvement process, this policy will be reviewed and revised at regular intervals