BUSINESS PROCESSES AND SECURITY POLICY

CYBERTECH CORPORATION
POLICY: COMMUNICATIONS SECURITY

April 7, 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	Communications Security Policy	Mehul Patel	April 3, 2024	PUBLIC	Creation
1.1		John Joshy Francis	April 4, 2024	PUBLIC	QA
1.2		Boby John	April 5, 2024	PUBLIC	Update
1.3		Niharkumar Jadav	April 6, 2024	PUBLIC	Update
1.4		Jaison Bhatti	April 7, 2024	PUBLIC	Update

3. APPROVAL

Name	Title	Date	Approved
Ahmad Barakat	Professor of MGMT1100	April 7, 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 this policy is to ensure the secure transmission of information, the protection of information in networks and its supporting information processing facilities, and to maintain the security of information transferred within an organization and with any external entity.

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
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 Resources	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 Network Security Management

4.1.1 Network Controls

4.1.2 Security of Network Services

4.1.3 Segregation in Networks

4.2 Information Transfer

4.2.1 Information Transfer Policies and Procedures

4.2.2 Agreements on Information Transfer

4.2.3 Electronic Messaging

4.2.4 Confidentiality o Non-Disclosure Agreements

4.1 Network Security Management

To ensure the protection of information in networks and its supporting information processing facilities.

4.1.1 Network Controls

Networks shall be managed and controlled to protect information in systems and applications.

- Cybertech's IT department will identify and deploy necessary safeguards to:
    - Safeguard the confidentiality and integrity of sensitive data traversing public networks.
    - Secure systems and applications that are connected.
    - Ensure continuous availability of network services and connected computers.

- All Cybertech Corporation’s employees and visitors are prohibited from connecting any devices (such as personal computers, laptops, or network equipment) to the Cybertech Corporation’s network without obtaining the required authorization and approval from the IT department.

- Cybertech's IT department will approve all traffic routing to align with Cybertech Corporation’s business communication needs.

- Cybertech's IT department will establish suitable routing control measures to limit data flows to approved network routes.

- Cybertech's IT department is responsible for ensuring effective management and technical supervision over the security boundary architecture (for example, firewalls) and its current settings. Areas of focus include, but are not limited to:
    - Recording the security boundary rules and conducting regular reviews.
    - Logging configuration alterations and securing management's endorsement.
    - Obtaining managerial consent before implementing any changes to the security boundary regulations.
    - Exercising caution when modifying the security boundary rules to prevent significant disruption to the Cybertech Corporation’s operations.

- User connectivity will be controlled via network gateways that sift through traffic based on established tables or directives. These limitations will encompass, but are not limited to:
  - Messaging (such as email).
  - File transfers.
  - Interactive logins.
  - Access to applications.

4.1.2 Security of Network Services

Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

- Cybertech's IT department will safeguard the network infrastructure of Cybertech Corporation by applying appropriate network security measures and functionalities. Network services' security features should include, but not be limited to:
  - Technologies used for securing network services, such as authentication, encryption, and network connection controls.
  - Technical specifications necessary for secure connections to network services in line with security and network connection protocols, including firewalls, VPNs, and IDS/IPS systems.
  - Usage procedures for network services to limit access to network services or applications where needed.

4.1.3 Segregation in Networks

Groups of information services, users and information systems shall be segregated on networks.

- Cybertech's IT department will divide the network of Cybertech Corporation into logical segments, zones, or domains based on criteria that include, but are not limited to:
  - Access needs (for example, Management, Department, Employees, IT, Third Parties).
  - The relative cost and performance implications of integrating appropriate technologies.

  - The value and classification of the data stored or processed within the network (for instance, Critical, Sensitive).
  - Trust levels (for example, Trusted, Internet, DMZ).
  - Business units (such as Service, Support).

- The internal network will be isolated from the external network, employing distinct perimeter security measures for each network.

4.2 Information Transfer

To maintain the security of information transferred within an organization and with any external entity

4.2.1 Information Transfer Policies and Procedures

Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

- Formal measures, determined by the criticality of the information, will be established to safeguard the exchange of data via communication channels. The transfer of confidential data must be adequately secured

- Every user is required to handle the generation, storage, modification, duplication, and elimination or destruction of data (both electronic and paper-based) in a way that aligns with Cybertech Corporation's guidelines, ensuring the confidentiality, integrity, and availability of this data are maintained and safeguarded.

- Asset Owners must guarantee that suitable protocols are in place and adhered to for the protection of their information during transfer.

4.2.2 Agreements on Information Transfer

Agreements shall address the secure transfer of business information between the organization and external parties.

- Before exchanging information with external entities, a formal Service Level Agreement (SLA) featuring adequate security measures must be established. This agreement should address, but not be confined to:
    - Roles and responsibilities of management.
    - Protocols for manual and electronic data exchanges.
    - The sensitivity of the critical information being shared.
    - Requirements for the protection of information.
    - Obligations for notifying relevant parties.
    - Standards for packaging and transmitting data.

  - Procedures for courier verification.
  - Definitions of responsibilities and liabilities.
  - Ownership of data and software.
  - Duties and strategies for information protection.
  - Requirements for data encryption.

4.2.3 Electronic Messaging

Information involved in electronic messaging shall be appropriately protected.

- Security mechanisms need to be implemented to safeguard electronic messaging systems (such as email) against unauthorized access, alteration, or disruption of service

4.2.4 Confidentiality or Non-Disclosure Agreements

Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.

- The obligations related to confidentiality and non-disclosure agreements (applicable to Cybertech Corporation's employees and external parties) need to be pinpointed and periodically reassessed. In this regard, Cybertech's IT department, in collaboration with various support divisions (such as the Information Security Officer, Project Management Office, Human Resources Department/Administrative Unit, and Legal Department), will:
  - Identify the information requiring protection along with its necessary sensitivity levels.
  - Determine the duration of the confidentiality commitment.
  - Outline the conditions for returning or disposing of the information once the obligation ends.
  - Define the signatories' responsibilities and requirements to avoid unauthorized information leaks.
  - Announce the consequences for any individual who breaches the confidentiality agreement.

- Confidentiality and non-disclosure agreements must incorporate legally binding terms relevant to Cybertech Corporation to ensure the protection of the organization's assets.

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 needs 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