BUSINESS PROCESSES AND SECURITY POLICY

CYBERTECH CORPORATION
POLICY: ACCESS CONTROL

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	Asset Management 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 Access Control Policy is to limit access to information and information process facilities, to stop unwanted access to programs and systems, to ensure authorized user access, to prevent unauthorized access to systems and services, and to make users accountable for safeguarding their authentication information

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 Business Requirements of Access Control

4.1.1 Access Control Policy

4.1.2 Access to Networks and Network Services

4.2 User Access Management

4.2.1 User Registration and De-registration

4.2.2 User Access Provisioning

4.2.3 Management of Privileged Access Rights

4.2.4 Management of Secret Authentication Information of Users

4.2.5 Review of User Access Rights

4.2.6 Removal or Adjustment of Access Rights

4.3 User Responsibilities

4.3.1 Use of Secret Authentication Information

4.4 System and Application Access Control

4.4.1 Information Access Restriction

4.4.1 Secure Log-on Procedures

4.4.2 Password Management System

4.4.3 Use of Privileged Utility Programs

4.4.4 Access Control to Program Source Code

4.1 Business Requirements of Access Control

To limit access to information and information process facilities.

4.1.1 Access Control Policy

An access control policy shall be established, documented and reviewed based on business and information security requirements.

□ Access management of data will be governed by predetermined access rules for every system under Cybertech Corporation's authority, in accordance with both business requirements and security requirements. These directives encompass:

- The implementation of both logical and physical safeguards for access.
- The security prerequisites for Cybertech Corporation’s business-critical applications.
- A clearly defined business justification for an individual’s access to specific data or operational processes, adhering to the principles of both 'need-to-know' and 'need-to-use'.
- A default stance of access denial, with permissions granted only as explicitly authorized by this policy.
- Modifications to user rights, whether conducted automatically or manually by a system administrator.
- Compliance with legal and contractual commitments to limit and secure access to Cybertech Corporation’s infrastructure.

□ For contractors or other third parties, access to Cybertech Corporation's business information assets will only be provided in accordance with the conditions of a signed contract. This agreement will encompass, but is not limited to:

- Detailed terms and conditions governing the access provided.
- The security obligations of the contractors or third-party partners.
- A commitment from the contractors or third-party personnel to comply with Cybertech Corporation's information security policies.

4.1.2 ACCESS TO NETWORKS AND NETWORK SERVICES

Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

□ At Cybertech Corporation, business and security imperatives, in addition to network-specific access control guidelines, shall strictly govern authorization and control of access to networks and network services. These guidelines shall encompass:

- The security prerequisites for the network or its services.
- A defined business need for an individual's access to the network (such as through VPN or wireless connections) or network services, adhering to the 'need-to-have' principle.
- The alignment of the user's security level with the security classification of the network.
- Requirements for user authentication to access different network services.
- The oversight and regulation of network service utilization.
- The procedures for authorizing access to various networks and network services based on established criteria.

□ The following requirements for network access control must be met by all computers before they can be connected to the Cybertech Corporation network or given complete access to network resources and the Internet:

- Adherence to operating system security policies.
- The presence of up-to-date antivirus definitions.
- Compliance with established firewall security protocols.

□ Guidelines for accessing shared folders are as follows:

- Access is limited to expressly authorized employees.
- Use is confined strictly to Cybertech Corporation business activities.
- The sharing of content not related to business activities, such as photos, videos, and audio files, is strictly prohibited.

□ Compliance with relevant legal and regulatory frameworks is required when establishing user identities.

□ Confirming the user's identity meticulously before providing access to information and technological resources.

□ The following access control and authorization guidelines will be included in a thorough plan that is approved and documented for handling user permissions:

- The 'Need-to-Know' and 'Need-to-Use' criteria.
- Segregation of duties to minimize risk.
- Least Privilege, ensuring users have the minimum level of access necessary for their roles.

□ To ensure secure and controlled access, verification controls will be implemented via an automated central access control system across all technical and informational assets.

□ To ensure personal accountability, it is not permitted to access Cybertech Corporation's data and technological resources using shared or generic accounts.

□ To improve security, systems will be set up to log off automatically after a predetermined amount of inactivity.

□ In order to prevent unwanted access, user accounts that remain inactive for a predefined period of time will be disabled.

□ All identity and access management systems will undergo modifications to guarantee that logging operations are centralized for efficient cybersecurity monitoring and event record management.

□ To protect data security and integrity, applications will be the only ones with direct access to databases of sensitive systems, excluding database administrators.

□ The protocols for handling Service Accounts will be formally recorded and authorized, emphasizing the secure communication between applications and systems and forbidding interactive human involvement, in order to guarantee the inclusion of strong security elements.

4.2 USER ACCESS MANAGEMENT

To ensure authorized user access and to prevent unauthorized access to systems and services.

4.2.1 USER REGISTRATION AND DE-REGISTRATION

A formal user registration and de-registration process shall be implemented to enable assignment of access rights.

□ Cybertech Corporation's IT department is responsible for creating a formalized access control procedure that outlines precise procedures for creating, modifying, suspending, and terminating user accounts.

□ The designated Owner must authorize user access, approve changes to current access rights, and revoke access while taking certain considerations into account:

- The principle of Least Privilege, ensuring access is granted strictly on a 'need-to-know' basis.
- The segregation of duties to prevent conflicts of interest and fraud.
- The specific level of access necessary for the user's role.

□ The management of user IDs will adhere to the following guidelines:

- To ensure their identity is verified, each employee of Cybertech Corporation is given a unique ID. A password, token, or biometric verification is just a few examples of the minimum authentication factors that need to be used to secure this ID.
- The registration of all Cybertech Corporation employees must follow the company's officially sanctioned user registration process.
- The use of redundant, shared, or group user IDs is strictly forbidden.
- Any redundant user IDs must be promptly removed or disabled.
- Only those with a valid business need for such access will be granted privileged user IDs, which will be distributed under strict control.
- To distinguish their privileged access from their regular operational access, administrators of multi-user systems must keep at least two distinct user IDs.
- Standard user ID codes and naming conventions for production files, programs, and system names will be used to maintain uniform access control across all Cybertech Corporation systems.

4.2.2 User Access Provisioning

A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

- □ All authorized user access to Cybertech Corporation's assets is defined and documented, and the authorization process is monitored and recorded to include:
  - ▪ Date of authorization
  - ▪ Identity of the individual approving access
  - ▪ Detailed description of access privileges granted
  - ▪ Reasons for granting the specified access privileges
- □ The process for assigning or revoking user access rights shall encompass:
  - ▪ Securing proper authorization from the system or service owner
  - ▪ Implementing segregation of duties to ensure appropriate access levels
  - ▪ Activation of access rights only after the completion of the authorization process
  - ▪ Maintaining centralized, up-to-date records of all user access rights
  - ▪ Adjusting user access rights in line with changes in employees' roles and responsibilities
  - ▪ Periodic review of user access rights
- □ Users' access rights to Cybertech Corporation's systems and services will be determined by their job description and business role, which will ensure that access is appropriate for them.
- □ Access requests must include the system name, request type, validity, and duration, and must be submitted via a form or system process that has been approved by the system owner and the direct manager.
- □ Access to the company's information and technological resources is provided to users based on their individual roles and responsibilities.
- □ Accurate tracking and association of user activities under a "User ID" are made possible by the adoption of a standardized mechanism for creating user identities.
- □ Implementing a policy that forbids users from logging in from several devices at once (Concurrent Logins).

4.2.3 Management of Privileged Access Rights

The allocation and use of privileged access rights shall be restricted and controlled.

□ Management of privileged access rights includes:

- Evaluating which access permissions need to be granted for every process or system, encompassing networks, databases, operating systems, and applications.
- Providing access permissions in compliance with the criteria particulars to each event and the need-to-use principle.
- Specifying the settings for each access permission's expiration.
- Granting access permissions in accordance with the configuration of the system's capabilities.

□ Limitations of a user's ability to access administrative accounts or privileges on their computers.

□ Providing a single user access privilege to those seeking for important and private rights (like Administrator Privilege), which is subsequently distributed based on their job roles and the concept of splitting of tasks.

□ Password history features are enabled in order to track changes and keep track of previously used passwords.

□ Restricting the frequent utilization of accounts with sensitive and important authorities for everyday tasks.

□ Multi-Factor Authentication (MFA) must be utilized for the mandatory verification of sensitive and essential user accounts on technical and informational assets. MFA must incorporate at least two of the following verification methods:

- Knowledge: Something the user knows (e.g., a password).
- Possession: Something the user uniquely possesses (e.g., a random number generator, software, device, or a one-time password received via SMS).
- Inherence: A unique biometric attribute or feature (e.g., a fingerprint).

□ Multi-Object Identity Verification (MFA) must be utilized by all users who seek to access sensitive systems or the systems that handle and watch across those sensitive systems.

4.2.4 Management of Secret Authentication Information of Users

The allocation of secret authentication information shall be controlled through a formal management process.

- □ All Cybertech Corporation systems must use a safe way to recognize and verify users, like finger prints, passwords, unique IDs, or smart cards.
- □ Implementation of password authentication for system or application access includes:
  - Passwords for regular users must be at least 8 characters, and for IT administrators, a minimum of 12 characters.
  - Passwords must include a mix of at least three of the following four criteria:
    - At least one lowercase alphabetic character (a-z)
    - At least one uppercase alphabetic character (A-Z)
    - At least one number (0-9)
    - At least one special character (e.g., @#$%^&*()_+|~-=\`{}[]:";'<>/)
  - The password cannot contain any element of the user ID.
  - Passwords must not be completely numeric or alphabetical, nor may they include more than two successive characters of the exact same kind.
  - Using blank passwords is not permitted at all.
  - The first time a user logs in, they have to change their password right away.
  - Accounts that are failing to log in three times in a row will be locked for three minutes.
  - It is compulsory to change passwords at least once every ninety-two days, and past passwords cannot be repeated.
  - Initial passwords are to be used once, expiring at 23:59:59 on the date issued.
  - Passwords should be securely maintained and saved, preferred via hashing or encryption.
- □ Passwords must be changed immediately upon any suspicion of compromise and reported to the IT department.
- □ All Cybertech Corporation systems and software have default usernames and passwords that must be updated by the IT department as soon as they are implemented.
- □ Password resets for users will only be carried out by the IT department following official proof of identity verification.

4.2.5 Review of User Access Rights

Asset owners shall review users' access rights at regular intervals.

- □ The Cybertech Department is required to promptly withdraw rights upon detection of any misuse.
- □ The formally authorized User Physical and Local Access Control Procedure shall be implemented when reviewing each user's access permissions.
- □ The Cybertech Department will cooperate with the Information Security Officer and Asset Owners to:
  - ▪ Develop a plan for reviewing user access rights, detailing:
    - o The systems under review.
    - o The frequency of reviews.
  - ▪ Conduct reviews of access privileges as follows:
    - o For high-risk systems (mission-critical systems), every three months.
    - o For medium-risk systems, every six months.
    - o For normal-risk systems, annually.

4.2.6 Removal or Adjustment of Access Rights

The access rights of all employees and external party users to of access rights information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

- □ Department managers have to immediately inform the Cybertech Department, the Human Resources Department/Administration Unit, and any other major modifications to an employee's job or employment status.
- □ When a worker quits the organization permanently:
  - ▪ System administrators ought to be made aware.
  - ▪ The employee's access rights must all be promptly terminated.
  - ▪ One month after work ends, the Cybertech Department will get rid of every file in the employee's directory unless told differently.

4.3 User Responsibilities

To make users accountable for safeguarding their authentication information

4.3.1 Use of Secret Authentication Information

Users shall be required to follow the organization's practices in the use of secret authentication information.

□ Users are accountable for anything they do while utilising their access privileges.

□ Users are prohibited from acquiring passwords, decryption keys, or any other authentication methods that could allow unauthorized access.

□ Specific prohibitions for users include:

- Not disclosing passwords over the phone to anyone.
- Avoiding password disclosure in email messages.
- Not sharing passwords with anyone, including Cybertech Administrators or supervisors.
- Refraining from discussing passwords in the presence of others.
- Not hinting at password formats, including personal information or predictable patterns.
- Not disclosing passwords on questionnaires or security forms.
- Not sharing passwords with family members.
- Avoiding password disclosure to colleagues, even while on vacation.
- Not writing down passwords where they can be found by unauthorized individuals.

□ The IT department is tasked with ensuring:

- Password encryption in storage or system logs.
- Passwords are not saved in internet browsers, preventing automatic password completion and login.
- Systems are built and kept up to date to prevent passwords from being retrieved or utilized without authorization.

4.4 System and Application Access Control

In order to stop unwanted access to programs and systems.

4.4.1 Information Access Restriction

According to a control of access policy, access to information and application system functions must be limited.

- □ The following will be the control measures for application system features:
  - ▪ Limiting data output in order prevent unapproved information being disclosed.
  - ▪ To protect the confidentiality of the data, access to the information will be restricted based on individual access accounts.
  - ▪ Defining everyone's correct privileges, such as the ability to read, write, delete, and perform actions.
  - ▪ Construction of tangible and conceptual obstacles to separate essential components, improving safety in various operating contexts.

4.4.1 Secure Log-on Procedures

Access to systems and applications must be managed using an encrypted log-on process when mandated under the policy governing access control.

- □ The operating system will follow a formalized, safe login process when signing in.
- □ To strengthen the security stance, a broad alert stating that entry is permitted to authorized personnel only is going to be shown across every system.
- □ Less information about the system and its intended use will be displayed in the login screen, thereby lowering the likelihood of leaking data.
- □ Whenever strong verification is required given improved safety, methods of authentication other than password (things like token IDs, smart cards, or biometrics) will be used.
- □ Computers are going to put limitations upon how many consecutive unsuccessful tries for logging in by:
  - ▪ Recording attempts at logging in, whether successful as well as not successful, enabling auditing reasons.
  - ▪ To avoid attacks using brute force, an interval preceding allowing more attempts at authentication or barring more attempts with no express permission should be included.

  - ▪ When the maximum number of login attempts is reached, a notification is sent to the system's a console, guaranteeing that any possible safety concerns are handled quickly.

□ Periodic assessments of every single failed login attempts are going to be carried out by cyber tech managers with the goal to detect and address possible risks to security.

4.4.2 Password Management System

Login management solutions must guarantee high-quality credentials & being active.

□ The innovative password administration system created to be used by the Cybertech Department will be implemented:

  - ▪ Strengthen credentials with good monitoring.
  - ▪ Obligation, if appropriate, regular passwords changes.
  - ▪ To prevent reuse and maintain a record of all usernames that have been used in the past.
  - ▪ For enhanced safety, hide credentials from view when entering.
  - ▪ With further security, keep password databases as well as application system information apart.
  - ▪ Passwords should be encrypted both when being stored and being transmitted to prevent unwanted access.

□ In order to provide basic security, passwords must have a minimum length of eight characters.

□ It is required that passwords be complicated, with a minimum of 3 distinct kinds of characters to greatly improve protection:

  - ▪ Upper-case letters.(like, ABCD)
  - ▪ Lower-case letters.(like, abcd)
  - ▪ Numbers (like,1235).
  - ▪ Special characters (like, #%*@).

□ Clients are going to be notified beforehand when their passwords are about to expire, encouraging it to reactivate them at time for the deadline. Personalized credentials for access have to be protected at beginning by requiring individuals to change the interim credentials during first login process.

□ Default passwords for all data and technology assets need to be changed before being deployed so an actual setting in order to remove typical risks.

4.4.3 Use of Privileged Utility Programs

Utilities that have an opportunity to override system and application controls must be carefully regulated.

□ Network utility usage will be tightly regulated, and entry will be restricted with formal permission from the Cybertech Department, guaranteeing those vital resources are utilized only by those permitted.

□ For a thorough audit path, every interaction with system utilities will be painstakingly recorded & reviewed through the Cyber-tech Section.

□ Software program usage and access shall be strictly controlled to protect against illegal modifications and maintain systems security.

□ In order to minimize hazards and optimize the functioning of the system, all unnecessary applications or system-wide utilities will be carefully found as eliminated.

4.4.4 Access Control to Program Source Code

Application code accessibility must be limited.

□ In order to safeguard proprietary information and maintain the safety of the system, the use of vital resources for development, such as program source codes, configurations, and related documentation (including designs, specifications, confirmation, as well as confirmation strategies), shall be strictly limited to individuals with the appropriate authorization and carefully documented.

□ The source code are going to be centrally compiled, controlled, and up-to-date through the Cybertech Department, guaranteeing consistency, security, and integrity throughout the entire lifecycle of software development.

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