Business Processes And Security Policy

CYBERTECH CORPORATION POLICY: SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

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	System Acquisition, Development and Maintenance 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 that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks. To ensure that information security is designed and implemented within the development lifecycle of information systems. To ensure the protection of data used for testing.

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 Security Requirements of Information Systems

4.1.1 Information Security Requirements Analysis and Specification

4.1.2 Securing Application Services on Public Networks

4.1.3 Protecting Application Services Transactions

4.2 Security in Development And Support Processes

4.2.1 Secure Development Policy

4.2.2 System Change Control Procedures

4.2.3 Technical Review of Application After Operating Platform Changes

4.2.4 Restrictions on Changes to Software Packages

4.2.5 Secure System Engineering Principles

4.2.6 Secure Development Environment

4.2.7 Outsourced Development

4.2.8 System Security Testing

4.2.9 System Acceptance Testing

4.3 Test Data

4.3.1 Protection of Test Data

4.1 Security Requirements of Information Systems

To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

4.1.1 Information security requirements analysis and specification

The information security-related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

- Information security needs for the introduction of new systems or the improvement of existing ones must be thoroughly analyzed, with essential controls incorporated via a formalized procedure.

- Throughout the software development lifecycle, including design and deployment phases, Cybertech's IT department must:
    - Ensure that activities related to system development or acquisition adhere to documented requirements, standards, procedures, Cybertech Corporation's business operations, and industry best practices.
    - Implement adequate controls (such as segregation of duties) to minimize the risks of information loss, errors, or misuse within the system.
    - Maintain a comprehensive and up-to-date system security plan for each system.
    - Define, document, execute, and monitor specific risk-based security measures for all critical systems underpinning its activities.

- In collaboration with the Information Security Officer, Cybertech's IT department should perform a security threat and risk assessment during the requirements phase of developing, implementing significant modifications to, or acquiring a system to:
    - Determine the necessary security measures (for instance, connections to logging, monitoring, and preventing data leaks) to protect the system.
    - Designate a security classification for the system.

4.1.2 SECURING APPLICATION SERVICES ON PUBLIC NETWORKS

Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

- All data involved in application services transmitted over public networks must be shielded from fraudulent activities, contract disputes, unauthorized access, and alterations. Security measures to consider include:
  - The use of secure authentication methods, such as public key cryptography or digital signatures.
  - The establishment of resilience against attacks, including Denial of Service (DoS) attacks.
  - Formulating a documentation agreement with vendors, if necessary.

- The integrity of information presented on publicly accessible systems (such as Cybertech Corporation's website) needs protection against unauthorized changes. Considerations should include, but are not limited to:
  - Cybertech Corporation's website should be developed and managed exclusively by adequately qualified and authorized staff.
  - Any modifications to the website must be recorded and managed via Cybertech Corporation's Change Management Procedure.
  - The website should feature a clear warning indicating that information cannot be duplicated or reproduced without basic copyright notices.
  - Information sourced from the internet must be confirmed for accuracy before its application in Cybertech Corporation's business operations.

4.1.3 PROTECTING APPLICATION SERVICES TRANSACTIONS

Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

- Information involved in online transactions must be safeguarded to avert incomplete transmissions, misdirection, unauthorized disclosures, modifications, duplications, or replays of messages.

- In all application service transactions between parties, the following must be ensured:
  - Secure authentication is verified.
  - The communication pathway is encrypted.
  - Data privacy is maintained.
  - Transaction confidentiality is upheld.

4.2 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

To ensure that information security is designed and implemented within the development lifecycle of information systems

4.2.1 SECURE DEVELOPMENT POLICY

Rules for the development of software and systems shall be established and applied to developments within the organization.

- Cybertech's IT department will establish and enforce guidelines for software development within Cybertech Corporation. These guidelines will include, but not be limited to:
  - Adhering to a secure software development methodology.
  - Employing secure coding practices, including standards, baselines, and code reviews.
  - Identifying and remedying security flaws, such as vulnerabilities.

- Cybertech's IT department will appoint skilled and trained software developers and programmers who are proficient in designing, testing, and verifying software code in accordance with global best practices.

4.2.2 SYSTEM CHANGE CONTROL PROCEDURES

Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

- Cybertech's IT department must guarantee that formal system change control procedures are thoroughly documented and applied.

- Cybertech's IT department must ensure all system alterations are rigorously tested, documented, updated, and managed. This includes, but is not limited to:
  - Testing all new software changes or installations in a dedicated testing environment.
  - Keeping the testing environment completely isolated from the production environment.

  - Scheduling changes implementation at opportune times to avoid adverse impacts on Cybertech Corporation’s business operations.

4.2.3 Technical Review of Application after Operating Platform Changes

When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

- Before installation, new or updated versions of the operating platform must undergo the established change management process in accordance with Cybertech Corporation's business requirements.

- A technical assessment of application controls and integrity is required before any non-emergency implementation into the production environment. These controls must align with the information security framework and receive approval from Management as part of the formal change management protocol.

- System capacity planning should precede the deployment of any new critical business application and be reassessed during upgrades. Necessary measures must be taken to prevent any issues with the availability of current applications or systems.

4.2.4 Restrictions on Changes to Software Packages

Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

- Continuous documentation of change management and impact analysis for application modifications should be integrated into the system development lifecycle, following Cybertech Corporation's business necessities.

- Alterations to software packages should be minimized. Wherever feasible and practical, vendor-supplied software packages should be utilized as is, without modifications.

- A software patch management strategy must be established to guarantee the installation of the latest approved patches and updates. Considerations include:
    - Ensuring software is updated with the most recent patches and configurations endorsed by the vendor to mitigate risks.
    - Implementing vendor-recommended configuration hardening practices to secure software against security threats.

4.2.5 Secure System Engineering Principles

Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

- Cybertech's IT department will establish, document, maintain, and execute principles for designing secure systems across all architectural layers, including business, data, applications, and technology. These principles should be regularly reviewed and updated.

- To ensure the security and integrity of applications and databases, appropriate validation checks for both input and output, as well as processing controls, should be employed to:
    - Authenticate the data entering and leaving the system.
    - Identify any corruption of information, whether it occurs due to processing errors or deliberate actions.
    - Confirm the accurate and appropriate processing of stored data.

- Cybertech's IT department is responsible for maintaining the validity and integrity of data entered into systems by:
    - Restricting input fields to specific data ranges, including defining values outside of these ranges or setting upper and lower limits for data volumes.
    - Screening for invalid characters in data fields.
    - Designating essential fields as compulsory.
    - Assessing the suitability of input data against business regulations.
    - Guarding against common cybersecurity threats, such as buffer overflows and denial-of-service (DoS and DDoS) attacks.
    - Employing control balances to ensure the completeness of input data and its processing.

- Cybertech's IT department must outline and document the responsibilities of all technical team members involved in the data input and output processes, including developers, system analysts, and system designers.

4.2.6 Secure Development Environment

Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

- Cybertech's IT department must create a secure development environment, incorporating people, processes, and technology, as an integral part of the software development lifecycle's prerequisites. These requirements should encompass the following elements:
  - The sensitivity of the data being handled or produced.
  - The relevance of both internal policies and external regulations to the development process.
  - The adoption of security protocols to safeguard the development environment and its outputs.
  - The establishment of clear boundaries between different development environments to prevent unauthorized access or data leakage.
  - The specification of access levels and the authentication methods required for each role within the development process.
  - The management of changes to ensure they are properly documented, authorized, and implemented without compromising security.
  - The regulation of data movement into and out of the development environment, ensuring that data transfers are secure and comply with all relevant data protection standards.

4.2.7 Outsourced Development

The organization shall supervise and monitor the activity of outsourced system development.

- For outsourced system development, the requirements should encompass, but not be limited to:
  - Adherence to an approved system development and maintenance methodology.

  - Adequate oversight and management of activities, including testing and user acceptance.

4.2.8 System Security Testing

Testing of security functionality shall be carried out during development.

- Cybertech's IT department must evaluate security features and functionalities within a system throughout the development stages, focusing on:
  - Mechanisms for access control and authentication.
  - The allocation and administration of privileges.
  - Procedures for backup and data recovery.
  - Strategies for data encryption and ensuring privacy.

4.2.9 System Acceptance Testing

Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

- Cybertech's IT department is tasked with ensuring that the prerequisites and standards for the acceptance of new systems are precisely outlined, agreed upon, documented, and verified. Criteria to consider include, but are not limited to:
  - Performance benchmarks and system capacity needs.
  - Error handling, restart processes, and backup plans.
  - Development and verification of routine operational procedures.
  - Implementation of a predefined set of security measures.
  - Business continuity strategies.
  - Proof that installing new hardware does not negatively impact existing control and automation systems, especially during peak operations.
  - Assurance that new hardware does not compromise the overall security posture of Cybertech Corporation's systems.
  - Training for the operation or utilization of new devices.
  - Guarantees and maintenance support.

4.3 TEST DATA

To ensure the protection of data used for testing.

4.3.1 PROTECTION OF TEST DATA

Test data shall be selected carefully, protected and controlled.

- Security measures in place in the production environment must also be applied within test environments to safeguard test data adequately. Considerations should include:
    - In specific, pre-authorized instances where accessing production data is necessary for the development or testing of business applications or systems, only "Read" and "Copy" permissions are allowed and should be rescinded after the task is completed.
    - Separate approvals must be obtained each time production data is transferred to a development or testing environment.
    - Any reproductions of production data utilized in development or testing settings must be deleted immediately after the completion of these activities.

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