BusinesS Processes and Security Policy

A white background with black and green text

Description automatically generated

**Cybertech Corporation policy: Information Security Incident Management**

April 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**

[**1. Table of Contents** 2](#_Toc164216193)

[**2. Revision History** 4](#_Toc164216194)

[**3. Approval** 4](#_Toc164216195)

[**4. Reference** 4](#_Toc164216196)

[**3. Policy Overview** 5](#_Toc164216197)

[**3.1 Purpose** 5](#_Toc164216198)

[**3.2 Scope** 5](#_Toc164216199)

[**3.3 Terms and Definitions** 6](#_Toc164216200)

[**3.4 Roles and Responsibilities** 7](#_Toc164216201)

[**4. Policy Statements** 8](#_Toc164216202)

[**4.1 Management of information security incidents and improvements** 9](#_Toc164216203)

[4.1.1 Responsibilities and procedures 9](#_Toc164216204)

[4.1.2 Reporting information security events 9](#_Toc164216205)

[4.1.3 Reporting information security weaknesses 9](#_Toc164216206)

[4.1.4 Assessment of and decision on information security events 9](#_Toc164216207)

[4.1.5 Response to information security incidents 9](#_Toc164216208)

[4.1.6 Learning from information security incidents 9](#_Toc164216209)

[4.1.7 Collection of evidence 10](#_Toc164216210)

[**5. Policy Compliance** 11](#_Toc164216211)

[**5.1 Compliance Measurement** 11](#_Toc164216212)

[**5.2 Exceptions** 11](#_Toc164216213)

[**5.3 Non-Compliance** 11](#_Toc164216214)

[**5.4 Continual Improvement** 11](#_Toc164216215)

# **2. Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Title** | **Author** | **Issue Date** | **Classification** | **Changes** |
| 1.0 | Information Security Incident Management | Mehul Patel | April 13, 2024 | PUBLIC | Creation |
| 1.1 |  | John Joshy Francis | April 14, 2024 | PUBLIC | QA |
| 1.2 |  | Boby John | April 15, 2024 | PUBLIC | Update |
| 1.3 |  | Niharkumar Jadav | April 16, 2024 | PUBLIC | Update |
| 1.4 |  | Jaison Bhatti | April 17, 2024 | PUBLIC | Update |

# **3. Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Title** | **Date** | **Approved** |
| Ahmad Barakat | Professor of MGMT1100 | April 17, 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 a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

## **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 behaviors 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 Management of information security incidents and improvements**

4.1.1 Responsibilities and procedures

4.1.2 Reporting information security events

4.1.3 Reporting information security weaknesses

4.1.4 Assessment of and decision on information security events

4.1.5 Response to information security incidents

4.1.6 Learning from information security incidents

4.1.7 Collection of evidence

## **4.1 Management Of Information Security Incidents And Improvements**

*To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.*

### 4.1.1 Responsibilities And Procedures

*Management responsibilities and procedures shall be established to ensure a quick, effective* *and orderly response to information security incidents.*

* Responsibilities for information security incidents and appropriate procedures shall be established to ensure an effective response to security-related events.
* All Cybertech Corporation employees must be aware of their responsibilities regarding the reporting of security incidents.
* The Information Security Officer, in cooperation with Cybertech's IT department, shall develop an information security incident management process. This process should include:
  + Identifying the incident and analyzing its cause and the vulnerabilities it exploited.
  + Limiting or restricting further impact of the incident.
  + Monitoring and reporting the incident.
  + Tactics for containing the incident.
  + Responding to and escalating the incident.
  + Taking corrective action to repair damage and prevent recurrence.
  + Communicating with all within Cybertech Corporation who are affected.
  + Collecting any relevant evidence.
* Cybertech's IT department shall implement, where feasible, a monitoring control system to detect information security incidents.
* Information concerning information security incidents shall not be disclosed to third parties (such as the public or journalists).
* All information security incidents that result in service disruptions or loss of assets shall be analyzed to identify any emerging trends. All such incidents and their trend analyses must be reported to the Information Security Officer and Cybertech's IT department on a regular basis.
* Potential information security incidents must be communicated to relevant personnel who will assist in implementing corrective actions.

### 4.1.2 Reporting Information Security Events

Information security events shall be reported through appropriate management channels as quickly as possible.

* The Information Security Officer, in collaboration with Cybertech's IT department, shall develop an "Information Security Incident Management Form" to report all security violations/incidents. This form is designed to establish a quick response mechanism for handling information security incidents.
* All employees of Cybertech Corporation should be aware and able to identify any unexpected or unusual behavior in the company's assets, which could indicate a software malfunction. Potential security events include, but are not limited to:
  + Uncontrolled system changes.
  + Access violations (e.g., password sharing).
  + Breaches of physical security.
  + Systems being hacked or manipulated.
  + Loss of information confidentiality (e.g., data theft).
  + Compromise of information integrity (i.e., damage to data or unauthorized modifications).
  + Misuse of information, assets, or services.
  + System infection by unauthorized or harmful programs and software.
  + Unauthorized access attempts.
  + Unauthorized changes to hardware, software, or infrastructure configuration.
  + Unusual system behavior.
* If a security event is detected, users should:
  + Record the symptoms and any error messages displayed.
  + Disconnect the workstation from the network if an infection is suspected, with assistance from Cybertech's IT department.
  + Avoid using any potentially infected removable media (e.g., USB memory sticks).
* All employees of Cybertech Corporation must immediately report all suspected security-related events to Cybertech's IT department. Reports should include, but not be limited to:
  + Contact name and number of the person reporting the incident.
  + Type of information or equipment involved.
  + Potential risk to people or other data due to the loss of information.
  + Location of the incident.
  + Inventory numbers of any affected equipment.
  + Date and time the security incident occurred.
  + Location of affected data or equipment.
  + Type and circumstances of the incident.
* Cybertech's IT department shall generate incident reports on a monthly basis and consolidate them into the IT Service Report every quarter.

### 4.1.3 Reporting Information Security Weaknesses

*Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.*

* All employees of Cybertech Corporation are required to report any suspected weaknesses related to information security in systems or services.
* Information security-related weaknesses should be reported to Cybertech's IT department as swiftly as possible, and the incident response and escalation procedures should be followed. Security weaknesses may include, but are not limited to:
  + Inadequate firewall or antivirus protection.
  + System malfunctions or overloads.
  + Malfunctions of software applications.
  + Human errors.

### 4.1.4 Assessment Of And Decision On Information Security Events

*Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.*

* Cybertech's IT department shall evaluate information security incidents for their criticality, based on their potential or actual business impact, according to the following scheme:
  + **Impact, Urgency: Priority**
  + **High, High: 1**
  + **High, Medium: 2**
  + **High, Low: 3**
  + **Medium, High: 2**
  + **Medium, Medium: 3**
  + **Medium, Low: 4**
  + **Low, High: 3**
  + **Low, Medium: 4**
  + **Low, Low: 5**
* All data relevant to security incidents must be classified according to the existing incident classification scheme. Cybertech's IT department is responsible for assigning the appropriate classification level to each security incident, with approval from Management.

### 4.1.5 Response To Information Security Incidents

*Information security incidents shall be responded to in accordance with the documented procedures.*

* Cybertech's IT department shall establish a formal "Information Security Incident Management Procedure" that outlines the necessary steps to respond to any information security incident.
* The response to an incident should be documented according to the following scheme:
  + Major Incidents should be responded to within 10 minutes and resolved within 4 hours
  + High should be responded to within 30 minutes and resolved within 8 hours
  + Medium should be responded to within 1 hour and resolved within 2 days
  + Low should be responded to within 4 hours and resolved within 5 days
* Recovery actions from an information security incident must be under formal control. Only identified and authorized employees will have access to the affected systems during the incident, and all remedial actions should be documented in as much detail as possible.
* Cybertech's IT department is responsible for tracking the status of incidents by following up with relevant parties and handling inquiries about the status. All information security incidents must be recorded and assigned an incident number for tracking and future reference. The record may include, but not be limited to:
  + Causes: both direct and indirect factors that led to the incident.
  + Impact: which systems were affected during the incident.
  + Actions taken: by the user and IT department employees to report and manage the incident.
  + Level of damage: the extent of losses incurred.
  + Date and time of occurrence.
* The incident response procedure should seamlessly continue from the event reporting process and include contingency plans to ensure the continuous operation of information systems during the incident.

### 4.1.6 Learning From Information Security Incidents

*Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.*

* Cybertech's IT department shall regularly collate and review post-incident information. Any changes made to the process as a result of the post-incident review should be formally recorded.
* After each incident, a lessons-learned exercise will be conducted by Cybertech's IT department, analyzed, and the results thoroughly documented. Considerations should include:
  + Conducting a timely post-incident analysis to assess the damage/cost, confirm the cause and motive of the attack, and identify any potential mitigating actions.
  + Assessing the involved systems to ensure that no unauthorized user accounts have been created and that user privileges have not been altered during the incident response.

### 4.1.7 Collection Of Evidence

*The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.*

* The Information Security Officer, in cooperation with Cybertech's IT department, shall identify, document, and maintain rules for the collection, retention, and presentation of evidence in accordance with Cybertech Corporation’s security, regulatory, and legal requirements.
* If an incident requires information collection for an investigation, strict adherence to the established rules is essential. The collection of evidence for a potential investigation must be handled with care, considering:
  + If evidence conclusively indicates that Cybertech Corporation has been the target of a computer or communications crime, a thorough investigation must be conducted.
  + This investigation should provide ample information to assist management in reinstating security measures and preventing the recurrence of such incidents.
* The Information Security Officer should be contacted immediately for guidance when collecting forensic evidence, which includes digital evidence, physical evidence, originals, and copies. Strict processes must be followed to ensure the integrity and legality of the evidence collection.

# **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