BusinesS Processes and Security Policy

A white background with black and green text

Description automatically generated

**Cybertech Corporation policy:**

**Information Security Aspects of**

**Business Continuity 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](#_Toc164216094)

[**2. Revision History** 4](#_Toc164216095)

[**3. Approval** 4](#_Toc164216096)

[**4. Reference** 4](#_Toc164216097)

[**3. Policy Overview** 5](#_Toc164216098)

[**3.1 Purpose** 5](#_Toc164216099)

[**3.2 Scope** 5](#_Toc164216100)

[**3.3 Terms and Definitions** 6](#_Toc164216101)

[**3.4 Roles and Responsibilities** 7](#_Toc164216102)

[**4. Policy Statements** 8](#_Toc164216103)

[**4.1 Information security continuity** 9](#_Toc164216104)

[4.1.1 Planning information security continuity 9](#_Toc164216105)

[4.1.2 Implementing information security continuity 9](#_Toc164216106)

[4.1.3 Verify, review and evaluate information security continuity 9](#_Toc164216107)

[**4.2 Redundancies** 9](#_Toc164216108)

[4.2.1 Availability of information processing facilities 9](#_Toc164216109)

[**5. Policy Compliance** 10](#_Toc164216110)

[**5.1 Compliance Measurement** 10](#_Toc164216111)

[**5.2 Exceptions** 10](#_Toc164216112)

[**5.3 Non-Compliance** 10](#_Toc164216113)

[**5.4 Continual Improvement** 10](#_Toc164216114)

# **2. Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Title** | **Author** | **Issue Date** | **Classification** | **Changes** |
| 1.0 | Information Security Aspects of Business Continuity Management Policy | 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 information security continuity shall be embedded in the organization's business continuity management systems and information processing facilities shall be implemented with redundancy sufficient to meet availability requirements*.*

.

## **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 Information security continuity**

4.1.1 Planning information security continuity

4.1.2 Implementing information security continuity

4.1.3 Verify, review and evaluate information security continuity

**4.2 Redundancies**

4.2.1 Availability of information processing facilities

## **4.1 Information Security Continuity**

*Information security continuity shall be embedded in the organization's business continuity management systems.*

### 4.1.1 Planning Information Security Continuity

*The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.*

* With respect to assessing the information security requirements, Cybertech will:
  + assess and define the essential requirements for information security to ensure operational resilience during adverse situations, such as natural disasters or cyberattacks.
  + conduct regular risk assessments to identify and prioritize information security needs aligned with business objectives and legal obligations.
* With respect to developing continuity strategies, Cybertech will:
  + develop and maintain a comprehensive strategy for information security continuity that includes preventive controls and mitigation strategies.
  + This strategy will address the recovery of critical information systems and the protection of data integrity under all conditions.
* Integrate with Business Continuity:
  + Information security continuity plans will be integrated with Cybertech’s broader business continuity management systems.
  + Ensure that information security is embedded in all business continuity plans and disaster recovery protocols.
* Stakeholder Engagement:
  + Regularly engage with key stakeholders to align the information security continuity plans with stakeholder expectations and contractual obligations.
  + Provide training and awareness sessions to ensure stakeholders understand their roles and responsibilities during adverse situations.

### 4.1.2 Implementing Information Security Continuity

*The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse* *situation.*

* Formalize Control Procedures:
  + Establish and document specific procedures and controls necessary to support information security continuity.
  + These procedures will include incident response, disaster recovery, and business continuity practices.
* Resource Allocation:
  + Allocate appropriate resources, including financial, human, and technological, to support the implementation of continuity controls.
  + Ensure redundant systems and backup facilities are in place and regularly tested.
* Training and Preparedness:
  + Conduct regular training for all employees to ensure they are prepared to act according to the continuity plans during a crisis.
  + Simulate different adverse scenarios to test employee readiness and the effectiveness of the response procedures.

### 4.1.3 Verify, Review And Evaluate Information Security Continuity

*The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse* *situations.*

* Regular Audits and Reviews:
  + Conduct regular audits and reviews of the information security continuity measures to ensure they are current and effective.
  + Assess the adaptability of the continuity measures to accommodate evolving threats and business requirements.
* Testing and Improvement:
  + Regularly test the established information security continuity plans to verify their effectiveness in adverse situations.
  + Based on testing outcomes, update and refine the plans to address any identified weaknesses or changes in the operational environment.
* Stakeholder Feedback:
  + Solicit and incorporate feedback from internal and external stakeholders on the effectiveness of the continuity controls.
  + Engage with industry peers to benchmark and enhance Cybertech’s continuity practices.

## **4.2 Redundancies**

*To ensure availability of information processing facilities.*

### 4.2.1 Availability Of Information Processing Facilities

*Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.*

* Redundancy Requirements:
  + Design and Implementation:
    - Implement redundant information processing facilities to meet the defined availability requirements essential for business operations.
    - Design redundancy to cover critical components such as data centers, network paths, storage systems, and power supplies.
  + Strategic Placement:
    - Position redundant facilities in diverse geographic locations to mitigate risks from local disruptions due to natural disasters or other regional issues.
* Regular Testing and Maintenance:
  + Testing will include the following:
    - Conduct regular tests to ensure the effective operation of redundant systems during both normal and adverse conditions.
    - Simulate failures to test failover processes and ensure minimal disruption during actual events.
  + Maintenance will be scheduled and conducted in intervals:
    - Establish and adhere to a strict maintenance schedule for all critical systems to minimize the risk of unplanned downtime.
    - Ensure maintenance activities are performed during low-impact hours to reduce the operational effect on business processes.
* Capacity Planning:
  + Continuous Monitoring:
    - Implement monitoring tools to continuously assess the performance and capacity utilization of information processing facilities.
    - Use predictive analysis to identify potential capacity issues before they impact service availability.
  + Scalability Provisions:
    - Plan for future growth by ensuring that information processing facilities are scalable to handle increasing data loads and processing demands.
    - Invest in scalable technologies that can be easily upgraded or expanded as required.
* Incident Management and Response:
  + Incident Response Plans:
    - Develop and maintain an incident response plan that includes procedures for responding to failures of information processing facilities.
    - Ensure the plan includes clear roles and responsibilities, and procedures for quickly restoring services to operational status.
  + Communication Strategy:
    - Maintain a communication strategy to inform stakeholders of incidents affecting availability, including expected resolution times and potential workarounds.
* Documentation and Compliance:
  + Documentation of Architecture:
    - Maintain comprehensive documentation of the redundancy architecture, including diagrams and specifications of all critical systems.
  + Compliance with Standards:
    - Ensure all redundant systems comply with industry standards and best practices for high availability and disaster recovery.

# **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