BusinesS Processes and Security Policy

A white background with black and green text

Description automatically generated

**Cybertech Corporation**

**policy: Supplier Relationships**

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](#_Toc164216601)

[**2. Revision History** 4](#_Toc164216602)

[**3. Approval** 4](#_Toc164216603)

[**4. Reference** 4](#_Toc164216604)

[**3. Policy Overview** 5](#_Toc164216605)

[**3.1 Purpose** 5](#_Toc164216606)

[**3.2 Scope** 5](#_Toc164216607)

[**3.3 Terms and Definitions** 6](#_Toc164216608)

[**3.4 Roles and Responsibilities** 7](#_Toc164216609)

[**4. Policy Statements** 8](#_Toc164216610)

[**4.1 Information security in supplier relationships** 9](#_Toc164216611)

[4.1.1 Information security policy for supplier relationships 9](#_Toc164216612)

[4.1.2 Addressing security within supplier agreements 9](#_Toc164216613)

[4.1.3 Information and communication technology supply chain 9](#_Toc164216614)

[**4.2 Supplier service delivery management** 9](#_Toc164216615)

[4.2.1 Monitoring and review supplier services 9](#_Toc164216616)

[4.2.2 Managing changes to supplier services 9](#_Toc164216617)

[**5. Policy Compliance** 11](#_Toc164216618)

[**5.1 Compliance Measurement** 11](#_Toc164216619)

[**5.2 Exceptions** 11](#_Toc164216620)

[**5.3 Non-Compliance** 11](#_Toc164216621)

[**5.4 Continual Improvement** 11](#_Toc164216622)

# **2. Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Title** | **Author** | **Issue Date** | **Classification** | **Changes** |
| 1.0 | Supplier Relationships 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 protection of the organization's assets that is accessible by suppliers and to maintain an agreed level of information security and service delivery in line with supplier agreements.

.

## **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 in supplier relationships**

4.1.1 Information security policy for supplier relationships

4.1.2 Addressing security within supplier agreements

4.1.3 Information and communication technology supply chain

**4.2 Supplier service delivery management**

4.2.1 Monitoring and review supplier services

4.2.2 Managing changes to supplier services

### **4.1 Information Security In Supplier Relationships**

*To ensure protection of the organization's assets that is accessible by suppliers.*

### 4.1.1 Information Security Policy For Supplier Relationships

*Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.*

* When initiating a contract and establishing the Service Level Agreement (SLA), Cybertech's IT department and Information Security Officer will collaborate with the Project Management Officer to:
  + Clearly define the specific roles and responsibilities of each party involved.
  + Determine all necessary security controls (such as processes and procedures) to be enforced by each party.
* Cybertech's IT department, in collaboration with the Information Security Officer, will grant supplier access (such as VPN access) only after the supplier has executed a confidentiality agreement. This agreement, between Cybertech Corporation and the supplier, must comply with Cybertech Corporation's legal compliance policy and business requirements.
* Supplier-provided reports and records shall be periodically reviewed by Cybertech's IT department.
* In cooperation with the Project Management Office, Cybertech's IT department will regularly update their records of contracts, outsourced services, and SLA targets along with corresponding contact details. Cybertech's IT department will also provide similar contact details to the supplier.

### 4.1.2 Addressing Security Within Supplier Agreements

*All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.*

* Cybertech's IT department shall validate and define within the contract the security measures applicable to a supplier; any contract must detail the identified risks. In cases where supplier access involves other participants:
  + The contract should include a clause specifying all authorized participants and the conditions governing their access.
  + If sub-contracting or outsourcing is involved, the contract must include clauses addressing how to manage security risks and the measures and procedures for systems, networks, technological infrastructures, and sensitive information.
  + Contracts must stipulate that personnel with access to sensitive information secure a security clearance and commit to utmost confidentiality by signing an agreement (e.g., non-disclosure or confidentiality agreement).

### 4.1.3 Information And Communication Technology Supply Chain

*Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.*

* Access by suppliers to Cybertech Corporation's information shall not be granted until the following conditions are met:
  + Proper justifications are provided.
  + The access is approved by management.
  + Appropriate security controls are implemented.
  + If relevant, a contract is signed that defines the terms and conditions.
* Cybertech's IT department must ensure that all security control measures are effectively implemented to safeguard the security of Cybertech Corporation's information and IT facilities accessed, processed, or managed by suppliers.
* When allowing supplier access to IT facilities, a risk assessment must be conducted by Cybertech's IT department to identify all necessary security controls.

### **4.2 Supplier Service Delivery Management**

*To maintain an agreed level of information security and service delivery in line with supplier agreements.*

### 4.2.1 Monitoring And Review Supplier Services

*Organizations shall regularly monitor, review and audit supplier of service delivery.*

* Cybertech's IT department, in cooperation with the Information Security Officer, shall conduct random audits on supplier access (such as VPN access) to check for security violations, improper use, and ongoing necessity.
* Cybertech's IT department, along with the Project Management Officer, will develop a procedure to clearly identify the roles and responsibilities necessary for the effective and efficient monitoring and reviewing of supplier services.
* Cybertech Corporation will maintain adequate overall control and visibility over:
  + All security aspects concerning sensitive information or IT facilities that are accessed, processed, or managed by a supplier.
  + All security activities, including change management, vulnerability identification, and incident reporting and response, through a defined process.
* The responsibility for managing the relationship with suppliers will be assigned to a designated individual or team from Cybertech's IT department and Project Management Office.

### 4.2.2 Managing Changes To Supplier Services

*Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.*

* Any changes to the provision of supplier services shall be managed based on the criticality of Cybertech Corporation's systems and related processes.

# **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