# Cybersecurity Policy

## Introduction

***[Organization Name]*** is committed to maintaining the confidentiality, integrity, and availability of its information assets, including but not limited to computer systems, networks, applications, and data. To achieve this, the company has established a comprehensive cybersecurity policy to guide the actions of all employees, contractors, and other authorized users of its information assets.

## Purpose

The purpose of this policy is to establish a framework for the protection of the company's information assets from unauthorized access, use, disclosure, modification, or destruction. This policy provides guidance on the roles and responsibilities of employees and other authorized users in maintaining the security of the company's information assets and sets out the procedures for responding to security incidents.

## Scope

This policy applies to all employees, contractors, and other authorized users of the company's information assets. It covers all forms of information, whether in electronic, paper, or other format, and all systems, networks, and applications used to store, process, or transmit such information.

## Policy Details

### **Roles and Responsibilities**

The following are the roles and responsibilities for ensuring the security of the company's information assets:

* Management: The management of the company is responsible for establishing and enforcing cybersecurity policies, procedures, and standards. They must ensure that appropriate resources are allocated for cybersecurity measures and that all employees are trained on cybersecurity awareness and best practices.
* IT Department: The IT department is responsible for implementing and managing the company's cybersecurity controls, including firewalls, antivirus software, intrusion detection and prevention systems, and other technical measures. They must also maintain an incident response plan in case of a security breach.
* Employees: All employees are responsible for complying with the company's cybersecurity policies and procedures. They must ensure that their passwords are secure, refrain from sharing sensitive information with unauthorized individuals, and report any suspicious activity or security incidents to the IT department.

### **Security Controls**

The following are some of the security controls that the company has implemented to protect its information assets:

* Access Control: Access to the company's information assets is restricted to authorized personnel only, based on the principle of least privilege. Passwords must be strong and changed regularly.
* Encryption: Sensitive information, including personally identifiable information (PII), must be encrypted during transmission and storage.
* Firewall: The company's network is protected by a firewall, which filters incoming and outgoing traffic to prevent unauthorized access.
* Antivirus Software: All endpoints, including desktops, laptops, and mobile devices, must have up-to-date antivirus software installed.
* Incident Response Plan: The company has established an incident response plan to ensure a prompt and effective response to security incidents.

### **Training and Awareness**

The company provides regular training and awareness programs to help employees understand the importance of cybersecurity and how to protect the company's information assets. Training programs cover topics such as password security, phishing, social engineering, and incident reporting.

### **Enforcement and Compliance**

The company takes violations of this policy seriously and will take appropriate disciplinary action against employees or other authorized users who violate this policy. The company reserves the right to monitor the use of its information assets to ensure compliance with this policy.

## Related Laws and Regulations

The Cybersecurity Policy at ***[Organization Name]*** is compliant with the following laws and regulations:

* Federal Information Security Modernization Act (FISMA)
* Health Insurance Portability and Accountability Act (HIPAA)
* Gramm-Leach-Bliley Act (GLBA)
* Sarbanes-Oxley Act (SOX)
* Payment Card Industry Data Security Standard (PCI DSS)
* California Consumer Privacy Act (CCPA)
* General Data Protection Regulation (GDPR)

## Disciplinary Action

Disciplinary actions are an important aspect of any cybersecurity policy to ensure that all employees take their responsibilities seriously and adhere to the policy's requirements. The disciplinary actions for violating the policy should be clearly defined and communicated to all employees to avoid any misunderstandings. Here are some possible disciplinary actions for violating the cybersecurity policy:

* Verbal Warning: First step for minor policy violations. Serves as a reminder of policy requirements and consequences of non-compliance.
* Written Warning: Issued for more serious violations or if the employee has already received a verbal warning. Provides details of the violation and consequences of further non-compliance.
* Suspension: Appropriate for serious violations or if the employee has received a written warning before. The length of suspension should reflect the severity of the violation.
* Termination: Necessary for repeated or severe violations. Employee access to company information assets should be immediately revoked, and an escort out of the building may be necessary.
* Legal Action: In cases of cybersecurity policy violations, legal action may result in civil or criminal charges depending on severity of the violation.

It is important to note that the disciplinary actions should be applied consistently and fairly to all employees, regardless of their position in the company. The policy should also include a process for appealing disciplinary actions if an employee feels that they have been unfairly penalized.

## Declaration

I, ***[Employee Name]***, understand that cybersecurity is a critical aspect of my job, and that the protection of the company's information assets is essential to its success. I acknowledge that I have received a copy of the company's cybersecurity policy and that it is my responsibility to read and comply with its requirements.

I agree to:

* Use only authorized hardware and software to access company information assets.
* Follow best practices for password management, including creating strong passwords and not sharing them with others.
* Report any suspected or actual cybersecurity incidents to the appropriate personnel immediately.
* Protect company information assets from unauthorized access, modification, disclosure, and destruction.

Failure to comply with the cybersecurity policy may result in disciplinary action, up to and including termination of employment. I also understand that the company may monitor my use of company information assets and that my personal use of these assets may be limited or prohibited.

By signing this declaration, I acknowledge my understanding of the company's cybersecurity policy and my commitment to comply with its requirements.

**Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**