Information Security Policy Statement

CyberSecure Ltd.

Acceptable Use of Technology Policy
Created by Alexander Egerev, Melanie Stewart, Parth Patel, Christina Maurice

Policy Development

Business Objectives

The purpose of this Policy is to explain rules and regulations for using a company's technology system (such as a computer, tablet, and/or devices belonging to the company), which is considered to be the company's assets. This is done to protect said assets against security threats, ensuring regulatory compliance from the company.

This document aims to define the limits of accessing a company's network(s), handling the company's data, and using the company's (or a person's) device(s). The goal is to reduce a company's legal liability and promote accountability in said company.

Key Stakeholders

The key stakeholders of this document are (but are not limited to):

- **Information Technology (IT) Managers/Support**: These people are responsible for outlining what is and what is not acceptable when it comes to using the company's technology.
- **Human Resources (HR)**: This division is responsible for communicating the policy to employees, training them, and setting disciplinary actions in place should there be a policy breach.
- **Lawyers/Attorneys**: These people make sure that federal, state, and local laws are followed and the company is in compliance with those laws.
- **Chief Executive Officer (CEO)**: Makes sure that the policy is part of the company's culture.
- **Employees/Interns/Contractors**: Must read, sign, and follow the policy; must understand their responsibilities to avoid any security breaches.

Each of them are responsible for their own scope of the Policy.

Policy Principles

This policy is in alignment with the Confidentiality, Integrity, and Availability (CIA) Triad:

- **Confidentiality**: This policy outlines what is and what is not acceptable when it comes to using the company's technology. This ensures that all data is confidential. Additionally, users agree not to distribute/disclose confidential company information/data outside of authorized personnel.
- **Integrity**: By following the policy, employees guarantee that the data on the company's technology is genuine, authentic, and unaltered.
- **Availability**: This policy ensures that all the company's information, both public and private, is available when management or HR needs it.

Accountability and Oversight

Users are solely responsible for their personal use of technology and protecting confidential data - such as login credentials - and complying with local/state/federal laws. They must also report incidents or violations to management.

The business reserves the right to monitor, access, and review network access, system logs, and emails to ensure security and compliance.

Prohibited Activities

-Illegal activities (including, but not limited to):

- Fraud, Harassment, Accessing/transmitting illegal content
- Security violations: Bypassing security, sharing passwords/login credentials, installing unauthorized software
- Misuse of Resources: Using company equipment for illegal, for-profit activities, or personal use
- Unauthorized Access: Network Intrusion

Implementation Strategy

Communication Plan

The HR staff and department management are responsible for communicating the policy to the company's employees. The policy could be posted on the company's **intranet** (a local or restricted communications network, especially a private network created using World Wide Web software), allowing employees to access and read it.

A physical copy will also be provided within the company's handbook.

Training Approach

There will be formal training in the company.

The HR staff will make sure that employees read and sign off on the policy, ensuring that said policy will be followed. There will also be mandatory training modules, and a more specific mandatory training; particularly the KnowBe4 interactive training (https://www.knowbe4.com/products/security-awareness-training). This training should take place.

Additionally, there will be onboarding materials provided. Examples include devices relevant to the business, like company phones, tablets, and smartwatches.

Success Metrics

The only way for the company to know that the policy is working is if one or more of the following are in place:

- **Security incidents**: Before the policy was implemented, security breaches were up by 25%. Once the policy is in place, breaches should be reduced by 15%.
- **User compliance**: IT support gets less tickets (10x less than before the policy was implemented) and more people complete the training course(s) (about 80% of employees).
- **System performance**: Less people download unauthorized software.

Feedback and Reporting

Employees can report issues/problems to the company's IT support staff, security officer, or HR. Employees must promptly report any policy violation, harmful incidents (such as a phishing attack), or security breaches to the correct department. Management will be responsible for conducting proper investigations if an attack occurs and will take all required actions in accordance with the company policy.

Users can submit a ticket at cybersecure.com/support to reach the IT support staff directly.

Reports of misconduct can be made anonymously within the support website. Reports made in good faith will not result in retaliation against the reporter.