

# Security Policy SuperHero Company

## Purpose

This document outlines the security policies and procedures for SuperHero Company. Our aim is to protect both our company's assets and our customers' data from unauthorized access and other cyber threats.

## Scope

This policy applies to all employees, contractors, and affiliates of SuperHero Company.

## Policy

### General Security Measures

- All employees must adhere to the established information security protocols.
- Regular security training will be provided to all staff members.
- We must do asset management

### Data Protection

- Sensitive data must be encrypted and securely stored.
- Access to sensitive data is restricted to authorized personnel only.

### Incident Response

- In the event of a security breach, immediate action must be taken following the incident response plan.
- The CISO, Jane Smith, is responsible for managing the response to any security incidents.

### Network Security

- Regular network security assessments will be conducted to identify and mitigate risks.
- Firewalls and anti-malware software must be maintained and updated regularly.

### Enforcement

- Violations of this security policy will be handled according to SuperHero Company's disciplinary procedures.
- Continuous monitoring will be conducted to ensure compliance with these policies.

## **Compliance Control**

Compliance controls covered by the document: - NIST ID.AM-6 - NIST ID.AM-1

## **Approval**

This policy has been approved by:

- CEO: John Doe
- CISO: Jane Smith

*Last Updated: [Insert Date]*