Information Security Policy

Business Supplies Inc.

Effective Date: August 15, 2024

Contents

1 Introduction

1.1 Purpose

This Information Security Policy outlines Business Supplies Inc.'s (BSI) approach to protecting its information assets and maintaining the confidentiality, integrity, and availability of its data. This policy establishes guidelines and standards for all employees, contractors, and third parties who access BSI's information systems.

1.2 Scope

This policy applies to all individuals who have access to BSI's information systems, including but not limited to employees, contractors, vendors, and temporary staff. It covers all information assets, whether they are stored electronically, on paper, or in any other form.

2 Roles and Responsibilities

2.1 Chief Information Security Officer (CISO)

The CISO is responsible for:

- Developing and maintaining the Information Security Policy
- Overseeing the implementation of security controls
- Conducting regular risk assessments
- Reporting on the organization's security posture to executive management

2.2 IT Department

The IT Department is responsible for:

- Implementing and maintaining technical security controls
- Monitoring systems for security events
- Providing technical support for security-related issues
- Conducting regular vulnerability assessments and patch management

2.3 Managers and Supervisors

Managers and supervisors are responsible for:

- Ensuring their staff understand and comply with this policy
- Reporting security incidents to the IT Department
- Assisting in the implementation of security measures within their departments

2.4 All Users

All users are responsible for:

- Complying with this policy and all related procedures
- Reporting any suspected security incidents or vulnerabilities
- Participating in security awareness training

3 Acceptable Use Policy

3.1 General Guidelines

- BSI's information systems are to be used for business purposes only
- Users must not engage in any activity that could harm BSI's reputation or expose it to legal liability
- All users must comply with applicable laws and regulations

3.2 Email and Internet Use

- Users must exercise caution when opening email attachments or clicking on links
- Personal use of email and internet should be minimal and not interfere with work duties
- Users must not use BSI's email system to send or forward offensive or inappropriate content

3.3 Software and Hardware

- Users must not install unauthorized software on BSI devices
- All software must be properly licensed and approved by the IT Department
- Users must not connect personal devices to BSI's network without approval

4 Access Control

4.1 User Authentication

- All users must have unique user IDs and strong passwords
- Multi-factor authentication is required for remote access and sensitive systems
- Passwords must be changed regularly and meet complexity requirements

4.2 Access Rights

- Access rights must be granted based on the principle of least privilege
- Regular access rights reviews must be conducted
- Access rights must be promptly revoked when no longer needed

5 Data Protection

5.1 Data Classification

BSI classifies data into four categories:

- Public
- Internal Use Only
- Confidential
- Restricted

Users must handle data according to its classification level.

5.2 Data Handling

- Confidential and Restricted data must be encrypted when stored or transmitted
- Users must not store BSI data on personal devices or cloud services
- Regular backups of critical data must be performed

6 Physical Security

- Access to BSI's facilities must be controlled and monitored
- Sensitive areas (e.g., server rooms) must have additional security measures
- Users must not leave sensitive information unattended on desks or printers

7 Incident Response

- All security incidents must be reported immediately to the IT Department
- BSI maintains an Incident Response Plan that outlines procedures for handling security incidents
- Regular incident response drills must be conducted

8 Compliance and Auditing

- Regular security audits and assessments must be conducted
- BSI must comply with all relevant laws and regulations
- Non-compliance with this policy may result in disciplinary action

9 Policy Review and Updates

This policy will be reviewed annually and updated as necessary to reflect changes in technology, business requirements, and the threat landscape.

Approved by: ____________________________
Chief Information Security Officer
Date: ________________________