Access Control Policy

Business Supplies Inc. (BSI)

Effective Date: September 26, 2024
Version: 1.0

Prepared by: CloudStrategik Consulting
Anderson@cloudstrategik.com

Confidentiality Statement

This document contains proprietary and confidential information of CloudStrategik Consulting and Business Supplies Inc. The information contained herein is disclosed to the recipient in confidence for the sole purpose of internal use. No part of this document may be disclosed, reproduced, or distributed without the prior written consent of CloudStrategik Consulting and Business Supplies Inc.

Contents

1 Introduction

1.1 Purpose

The purpose of this Access Control Policy is to establish guidelines and requirements for managing access to Business Supplies Inc.'s (BSI) information systems, networks, and data. This policy aims to ensure that access to BSI's assets is granted based on business need, follows the principle of least privilege, and is properly monitored and maintained throughout the access lifecycle.

1.2 Scope

This policy applies to all BSI employees, contractors, vendors, and any other individuals or entities that require access to BSI's information systems, networks, or data. It covers all IT assets owned or managed by BSI, including on-premises infrastructure, cloud-based services, and applications.

2 Policy Statement

BSI is committed to protecting its information assets by implementing and maintaining robust access control measures. Access to BSI's systems and data shall be granted only to authorized individuals based on their job responsibilities and shall be revoked promptly when no longer needed.

3 Access Control Principles

3.1 Least Privilege

Access rights granted to users shall be limited to the minimum necessary to perform their job functions.

3.2 Need-to-Know

Access to information shall be granted only to individuals who require it to perform their assigned duties.

3.3 Separation of Duties

Critical business functions and IT operations shall be divided among different individuals to reduce the risk of accidental or deliberate system misuse.

3.4 Default Deny

Access to systems and data shall be denied by default unless explicitly granted.

4 Roles and Responsibilities

4.1 Information Security Team

- Develop and maintain the Access Control Policy
- Conduct regular access reviews and audits
- Provide guidance on access control best practices
- Monitor and report on access control metrics

4.2 IT Operations Team

- Implement and maintain access control systems
- Process access requests and changes
- Assist in troubleshooting access-related issues

4.3 Human Resources

- Notify IT of personnel changes affecting access rights
- Assist in the user provisioning and deprovisioning processes

4.4 Managers and Supervisors

- Approve access requests for their team members
- Regularly review access rights of their staff
- Notify IT of changes in staff roles or responsibilities

4.5 Users

- Comply with this Access Control Policy and related procedures
- Maintain the confidentiality of their authentication credentials
- Report any suspected unauthorized access or security incidents

5 Access Control Procedures

5.1 User Account Management

5.1.1 Account Creation

- New user accounts shall be created based on a formal request process
- Requests must be approved by the user's manager and the relevant system owner
- Standard access profiles shall be used where possible to ensure consistency

5.1.2 Account Modification

- Changes to user access rights shall follow a formal change request process
- All changes must be documented and approved by authorized personnel

5.1.3 Account Termination

- Access rights shall be promptly revoked when a user leaves the organization or changes roles
- A formal offboarding process shall be followed to ensure all access is removed

5.2 Password Management

- All user accounts shall be protected by strong passwords
- Password complexity requirements:
  - Minimum length: 12 characters
  - Must include uppercase, lowercase, numbers, and special characters
  - Cannot contain common words or easily guessable information
- Passwords must be changed every 90 days
- Password history shall be maintained to prevent reuse of the last 10 passwords
- Failed login attempts shall be limited to 5 before account lockout

5.3 Multi-Factor Authentication (MFA)

- MFA shall be required for all remote access and for accessing critical systems
- Approved MFA methods include:
  - Hardware tokens
  - Soft tokens (smartphone apps)
  - Biometric authentication (where applicable)

5.4 Privileged Access Management

- Privileged accounts shall be strictly controlled and monitored
- Use of shared privileged accounts shall be minimized and require explicit approval
- Privileged account passwords shall be changed more frequently (every 60 days)
- All actions performed using privileged accounts shall be logged and audited

5.5 Remote Access

- Remote access shall be granted only through approved, secure methods (e.g., VPN)
- All remote access sessions shall be encrypted and require MFA
- Remote access shall be automatically disconnected after 30 minutes of inactivity

5.6 Third-Party Access

- Third-party access shall be granted only when necessary and with limited duration
- All third-party access must be approved by the Information Security Team
- Third-party accounts shall be regularly reviewed and disabled when no longer needed

6 Access Reviews and Auditing

6.1 Regular Access Reviews

- User access rights shall be reviewed at least quarterly
- Managers shall verify the appropriateness of their staff's access rights
- The results of access reviews shall be documented and any required changes implemented

6.2 Access Auditing

- Access-related events shall be logged and monitored
- Audit logs shall be retained for at least one year
- Regular audits shall be conducted to ensure compliance with this policy

7 Policy Compliance

7.1 Compliance Measurement

The Information Security Team will verify compliance with this policy through various methods, including but not limited to periodic audits, access reviews, and incident investigations.

7.2 Exceptions

Any exception to this policy must be approved by the Information Security Team in advance and documented.

7.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

8 Policy Review and Updates

This Access Control Policy shall be reviewed annually and updated as necessary to reflect changes in BSI's business requirements, technology environment, or regulatory obligations.

9 Document Revision History

Version	Date	Description of Changes	Author
1.0	09/26/2024	Initial document creation	A. Anthony

10 Approval

This document has been reviewed and approved by:

Name:	**Signature:**
Title:	**Date:**
Name:	**Signature:**
Title:	**Date:**

11 Disclaimer

This Access Control Policy provides guidelines for managing access to BSI's information systems and data. While it aims to address common scenarios, there may be situations that require additional consideration. Employees should consult with the Information Security Team or their manager if they are unsure about how to proceed in specific access-related situations.

12 Contact Information

For any questions or clarifications regarding this Access Control Policy, please contact:

Name: Anderson Anthony
Title: Information Security Manager
Email: Anderson@cloudstrategik.com
Phone: +1 (555) 123-4567