Vendor Risk Management Policy

Business Supplies Inc. (BSI)

Effective Date: September 5, 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 Vendor Risk Management Policy is to establish a standardized process for assessing, monitoring, and mitigating risks associated with Business Supplies Inc.'s (BSI) third-party vendors and service providers. This policy aims to protect BSI's assets, data, and reputation by ensuring that vendors adhere to appropriate security, privacy, and compliance standards.

1.2 Scope

This policy applies to all vendors, contractors, and third-party service providers that have access to BSI's systems, data, or facilities. It covers the entire vendor lifecycle, from selection and onboarding to ongoing monitoring and offboarding.

2 Roles and Responsibilities

2.1 Vendor Risk Management Team

- Develop and maintain the Vendor Risk Management Policy
- Oversee the vendor risk assessment process
- Provide guidance and support to business units on vendor risk management
- Report on vendor risk status to senior management

2.2 Business Unit Managers

- Identify vendors requiring risk assessment
- Collaborate with the Vendor Risk Management Team in conducting assessments
- Ensure compliance with this policy within their respective units
- Monitor vendor performance and report issues

2.3 Legal Department

- Review and approve vendor contracts
- Ensure appropriate risk mitigation clauses are included in contracts
- Provide legal advice on vendor-related issues

2.4 Information Security Team

- Assist in technical aspects of vendor risk assessments
- Review vendor security practices and controls
- Provide recommendations for security requirements in vendor agreements

2.5 Procurement Department

- Incorporate vendor risk management requirements into the procurement process
- Maintain a central repository of vendor information and risk assessments
- Coordinate vendor selection and contract negotiation processes

3 Vendor Risk Assessment Process

3.1 Vendor Categorization

Vendors will be categorized based on the following criteria:

- Criticality of services provided
- Level of access to BSI systems or data
- Volume and sensitivity of data processed
- Regulatory requirements applicable to the vendor's services

Categories:

1. Critical: High-risk vendors with access to sensitive data or critical systems
2. Significant: Moderate-risk vendors with limited access to sensitive data
3. Low Risk: Vendors with minimal access to BSI systems or data

3.2 Initial Risk Assessment

1. Business unit identifies need for new vendor
2. Vendor Risk Management Team conducts initial screening
3. Vendor completes risk assessment questionnaire
4. On-site assessment or virtual review conducted for Critical and Significant vendors
5. Risk rating assigned based on assessment results

3.3 Due Diligence

For Critical and Significant vendors:

- Review financial stability
- Check references and reputation
- Evaluate security and privacy practices
- Assess compliance with relevant regulations
- Review business continuity and disaster recovery plans

3.4 Contract Requirements

Vendor agreements must include:

- Clear definition of services and performance metrics
- Data protection and confidentiality clauses
- Right to audit clause
- Incident reporting and management procedures
- Business continuity requirements
- Compliance with applicable laws and regulations
- Termination and exit clauses

4 Ongoing Monitoring and Reassessment

4.1 Continuous Monitoring

- Regular performance reviews against SLAs
- Monitoring of vendor financial stability and news
- Tracking of security incidents and breaches
- Review of audit reports and certifications

4.2 Periodic Reassessment

- Critical vendors: Annual full reassessment
- Significant vendors: Biennial full reassessment
- Low Risk vendors: Reassessment every three years or upon significant changes

4.3 Triggers for Ad-hoc Reassessment

- Major changes in vendor's ownership or management
- Significant security incidents or data breaches
- Changes in regulatory requirements
- Expansion of vendor's scope of work

5 Risk Mitigation Strategies

- Implement additional security controls
- Increase monitoring frequency
- Require remediation of identified vulnerabilities
- Limit scope of vendor access or services
- Implement compensating controls within BSI
- Consider alternative vendors for high-risk services

6 Vendor Offboarding

- Develop and follow a formal offboarding checklist
- Ensure return or secure destruction of BSI data
- Revoke all access to BSI systems and facilities
- Conduct final security assessment
- Update vendor inventory and risk register

7 Reporting and Escalation

- Quarterly vendor risk reports to senior management
- Immediate escalation of critical vendor issues to executive leadership
- Annual review of vendor risk management program effectiveness

8 Training and Awareness

- Provide annual training on vendor risk management to relevant staff
- Include vendor risk management in employee onboarding for applicable roles
- Conduct periodic awareness campaigns on vendor-related risks

9 Policy Compliance

- All employees involved in vendor management must comply with this policy
- Non-compliance may result in disciplinary action
- Exceptions must be documented and approved by the Vendor Risk Management Team and senior management

10 Policy Review and Updates

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

11 Appendices

11.1 Appendix A: Vendor Risk Assessment Questionnaire Template

11.2 Appendix B: Vendor Risk Rating Matrix

11.3 Appendix C: Vendor Management Workflow

12 Document Revision History

Version	Date	Description of Changes	Author
1.0	09/05/2024	Initial document creation	A. Anthony

13 Approval

This document has been reviewed and approved by:

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

14 Disclaimer

This Vendor Risk Management Policy provides guidelines for assessing and managing risks associated with third-party vendors. While it aims to address common scenarios, there may be situations that require additional consideration. Employees should consult with the Vendor Risk Management Team or their manager if they are unsure about how to proceed in specific vendor-related situations.

15 Contact Information

For any questions or clarifications regarding this Vendor Risk Management Policy, please contact:

Name: Anderson Anthony
Title: Vendor Risk Management Lead
Email: Anderson@cloudstrategik.com
Phone: +1 (555) 123-4567