Cybersecurity Policy for Low Risk Finance Environment

1. Introduction

This Cybersecurity Policy outlines the framework for protecting the confidentiality, integrity, and availability of information assets within our organization. Recognizing the sensitive nature of financial data and our commitment to regulatory compliance, this policy establishes minimum-security standards and guidelines for all employees, contractors, and third-party service providers. While our risk profile is currently assessed as low, vigilance and proactive security measures are paramount to maintaining this posture and preventing potential future compromises. This policy is aligned with the Risk Management Framework (RMF) and is designed to evolve with the organization's growth and the changing threat landscape.

2. Risk Assessment

A risk assessment will be conducted annually, or more frequently as needed, to identify potential threats, vulnerabilities, and their associated impact on the organization's business objectives. The assessment will consider:

- Asset Inventory: Maintaining an accurate inventory of all information assets, including hardware, software, and data.
- Threat Identification: Identifying potential threats such as malware, phishing attacks, unauthorized access, and data breaches.
- Vulnerability Assessment: Assessing vulnerabilities in systems, applications, and processes.
- Impact Analysis: Determining the potential impact of a successful attack on the confidentiality, integrity, and availability of information assets, considering financial losses, reputational damage, and legal repercussions.
- Risk Prioritization: Prioritizing risks based on their likelihood and impact to inform the implementation of appropriate security controls.

Given the low-risk environment, emphasis will be placed on preventative measures and readily available security solutions with automated capabilities.

3. Data Protection

Protecting sensitive data is a top priority. The following data protection measures will be implemented:

- Data Classification: Classifying data based on its sensitivity and implementing appropriate security controls for each classification level. Public, internal, confidential and restricted will be the data classification options.
- Data Encryption: Encrypting sensitive data at rest and in transit. This includes encrypting hard drives, databases, and network traffic. Transport Layer Security (TLS) 1.2 or higher will be enforced on all public facing websites and services.
- Data Loss Prevention (DLP): Implementing DLP measures to prevent sensitive data from leaving the organization's control. This includes monitoring network traffic and email communications for sensitive data. While a full DLP solution may not be necessary, email filtering and basic endpoint monitoring will be considered.

- Data Retention and Disposal: Establishing data retention policies and securely disposing of data when it is no longer needed. This includes securely wiping hard drives and shredding paper documents.
- Regular Data Backups: Performing regular data backups and storing backups in a secure offsite location. Backups will be tested regularly to ensure their integrity and recoverability.

4. Access Controls

Access to information assets will be restricted based on the principle of least privilege:

- User Authentication: Requiring strong passwords and multi-factor authentication (MFA) for all users. MFA will be required for all external access and privileged accounts.
- Access Authorization: Granting access to information assets based on job responsibilities and the principle of least privilege. Regular access reviews will be conducted to ensure that users only have access to the resources they need.
- Account Management: Establishing procedures for creating, modifying, and deleting user accounts. Dormant accounts will be disabled promptly.
- Privileged Access Management (PAM): Implementing PAM controls to restrict and monitor access to privileged accounts. Privileged accounts will be used only when necessary and will be subject to strict monitoring.
- Network Segmentation: Segmenting the network to isolate critical systems and data from less secure areas.

5. Incident Response

A documented Incident Response Plan (IRP) will be maintained and regularly tested to ensure a timely and effective response to security incidents. The IRP will include:

- Incident Identification: Establishing procedures for identifying and reporting security incidents.
- Incident Containment: Taking immediate steps to contain security incidents and prevent further damage.
- Incident Eradication: Removing the cause of the security incident and restoring affected systems to a secure state.
- Incident Recovery: Recovering data and systems affected by the security incident.
- Post-Incident Analysis: Conducting a post-incident analysis to identify the root cause of the incident and implement measures to prevent future occurrences.
- Communication Plan: Establishing a communication plan for notifying stakeholders about security incidents.

6. Security Awareness Training

All employees, contractors, and third-party service providers will receive regular security awareness training to educate them about cybersecurity threats and best practices. The training will cover:

- Phishing Awareness: Recognizing and avoiding phishing attacks.
- Password Security: Creating and maintaining strong passwords.
- Data Protection: Protecting sensitive data from unauthorized access and disclosure.

- Social Engineering: Recognizing and avoiding social engineering attacks.
- Mobile Security: Securing mobile devices and data.
- Reporting Security Incidents: Reporting suspected security incidents promptly.

Training will be conducted at least annually and will be tailored to the specific roles and responsibilities of the participants.

7. Compliance and Auditing

This Cybersecurity Policy is designed to comply with applicable laws, regulations, and industry standards, including the Risk Management Framework (RMF).

- Regular Audits: Conducting regular internal and external audits to assess compliance with this policy and applicable regulations.
- Vulnerability Scanning: Performing regular vulnerability scans to identify and remediate security vulnerabilities.
- Penetration Testing: Conducting periodic penetration testing to assess the effectiveness of security controls. While a full penetration test may not be required, periodic reviews of existing controls are expected.
- Compliance Reporting: Preparing regular compliance reports for management and regulatory agencies.
- Policy Review: This policy will be reviewed and updated at least annually, or more frequently as needed, to reflect changes in the threat landscape, technology, and regulatory requirements.

8. Conclusion

This Cybersecurity Policy is essential for protecting the organization's information assets and maintaining a secure operating environment. By adhering to the principles and guidelines outlined in this policy, we can minimize the risk of security breaches and maintain the trust of our customers and stakeholders. All employees, contractors, and third-party service providers are responsible for understanding and complying with this policy. The CISO is responsible for overseeing the implementation and enforcement of this policy.