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 [Company Name]. This policy applies to all employees, contractors, vendors, and any other individuals or entities accessing or using [Company Name]'s systems and data. Recognizing our low-risk operating environment, this policy adopts a risk-based approach aligned with the Risk Management Framework (RMF) to ensure proportionate and effective security measures. This policy is designed to meet the specific needs of our low-risk financial operation, focusing on protecting customer data and maintaining operational integrity while optimizing resource allocation for cybersecurity.

2. Risk Assessment

[Company Name] conducts periodic risk assessments to identify, analyze, and evaluate potential threats and vulnerabilities to its information assets. Given our low-risk profile, these assessments will be performed annually, or more frequently if significant changes occur to our business operations, technology infrastructure, or the threat landscape.

--Process:--

- --Identification:-- Identify critical assets, potential threats (e.g., phishing, malware), and vulnerabilities (e.g., unpatched software, weak passwords).
- --Analysis:-- Evaluate the likelihood and impact of each threat exploiting a vulnerability, considering existing controls.
- --Evaluation:-- Determine the overall risk level for each identified threat/vulnerability pair.
- --Documentation:-- Maintain a risk register documenting the assessment results, including identified risks, their likelihood and impact, and planned mitigation strategies.
- --Review:-- Risk assessments are reviewed and updated at least annually, or when significant changes occur. The output of the risk assessment will determine the level and type of security controls to be implemented.

3. Data Protection

Data protection is paramount. [Company Name] implements measures to protect sensitive data, including customer information, financial records, and proprietary business data.

--Measures:--

- --Data Classification:-- Classify data based on its sensitivity and criticality (e.g., public, internal, confidential).
- --Data Encryption:-- Employ encryption, both in transit and at rest, for sensitive data. This includes encrypting data stored on laptops, portable storage devices, and in databases.
- --Data Loss Prevention (DLP):-- Implement basic DLP measures to prevent sensitive data from leaving the organization's control, such as restricting the use of unauthorized cloud

storage services.
- --Data Backup and Recovery:-- Regularly back up critical data and store backups in a secure, offsite location. Test data recovery procedures periodically to ensure business continuity.
- --Data Retention and Disposal:-- Establish and adhere to data retention policies. Securely dispose of data when it is no longer needed, using methods that prevent unauthorized access.
- --Access Control:-- Restrict access to sensitive data based on the principle of least privilege. Access should only be granted to individuals who require it to perform their job duties.

4. Access Controls

Access to systems and data is carefully controlled to minimize the risk of unauthorized access.

--Controls:--

- --User Account Management:-- Implement a process for creating, modifying, and deleting user accounts. Enforce strong password policies, including minimum length, complexity, and regular password changes. Multifactor authentication should be enabled wherever technically feasible, especially for remote access and privileged accounts.
- --Principle of Least Privilege:-- Grant users only the minimum necessary access rights required to perform their job duties.
- --Access Reviews:-- Conduct periodic reviews of user access rights to ensure they remain appropriate.
- --Remote Access:-- Secure remote access to the network using VPNs and multifactor authentication where technically feasible.
- --Physical Security:-- Implement physical security measures to protect access to data centers and other sensitive areas, such as badge access and security cameras.
- --Network Segmentation:-- Implement basic network segmentation to isolate critical systems from less secure areas of the network.

5. Incident Response

[Company Name] has established an incident response plan to effectively address and manage cybersecurity incidents.

--Plan Elements:--

- --Incident Identification:-- Define procedures for identifying and reporting security incidents.
- --Incident Containment:-- Implement measures to contain the spread of an incident, such as isolating affected systems.
- --Incident Eradication:-- Remove the root cause of the incident and restore affected systems to normal operation.
- --Incident Recovery:-- Restore systems and data to their pre-incident state.
- --Post-Incident Analysis:-- Conduct a post-incident review to identify lessons learned and improve security controls.

- --Reporting:-- Report significant security incidents to relevant stakeholders, including management and, where required, regulatory authorities.
- --Regular Testing:-- Incident response plan will be tested annually through tabletop exercises.

6. Security Awareness Training

All employees, contractors, and vendors receive security awareness training to educate them about cybersecurity threats and best practices.

--Training Program:--

- --Initial Training:-- Provide initial security awareness training to all new employees.
- --Annual Training:-- Conduct annual refresher training to reinforce security best practices.
- --Targeted Training:-- Provide targeted training on specific threats, such as phishing, malware, and social engineering.
- --Phishing Simulations:-- Conduct periodic phishing simulations to test employees' ability to identify and report phishing emails.
- --Training Content:-- Cover topics such as password security, data protection, social engineering, malware, and incident reporting.

7. Compliance and Auditing

[Company Name] is committed to complying with all applicable laws, regulations, and industry standards.

--Compliance Activities:--

- --Risk Management Framework (RMF):-- Implement security controls based on the RMF guidelines.
- --Internal Audits:-- Conduct periodic internal audits to assess compliance with this policy and other relevant security standards.
- --External Audits:-- Engage external auditors to conduct independent assessments of our security posture.
- --Policy Review:-- This policy will be reviewed and updated at least annually, or when significant changes occur to our business operations, technology infrastructure, or the threat landscape.

8. Conclusion

This Cybersecurity Policy provides a framework for protecting [Company Name]'s information assets in a low-risk environment. By adhering to this policy, we can minimize the risk of cybersecurity incidents and maintain the confidentiality, integrity, and availability of our data. All employees, contractors, and vendors are expected to comply with this policy. Management is responsible for enforcing this policy and providing the resources necessary to support its implementation. This policy demonstrates our commitment to cybersecurity and our dedication to protecting the interests of our customers and stakeholders.