Cybersecurity Policy for Low-Risk Finance Environment

1. Introduction

This Cybersecurity Policy outlines the essential security measures implemented to protect the confidentiality, integrity, and availability of information assets within our organization. While our risk assessment identifies a relatively low-risk profile, maintaining a robust security posture is crucial to preserving trust, ensuring business continuity, and complying with relevant regulations, specifically aligned with the principles of ISO/IEC 27001. This policy applies to all employees, contractors, vendors, and other authorized users who access or utilize our systems and data. All users are expected to adhere to the guidelines described within this document.

2. Risk Assessment

Our organization conducts periodic risk assessments to identify, analyze, and evaluate potential threats and vulnerabilities to our information assets. These assessments consider factors such as:

- --Asset Valuation:-- Determining the relative importance and sensitivity of our information assets.
- --Threat Identification:-- Identifying potential sources of harm, such as malware, phishing attacks, unauthorized access, and data breaches.
- --Vulnerability Assessment:-- Evaluating weaknesses in our systems, processes, and physical environment that could be exploited by threats.
- --Likelihood and Impact Analysis:-- Assessing the probability of a threat occurring and the potential consequences to our business.

Given our classification as a low-risk environment, the primary focus is on implementing cost-effective and proportionate security controls to mitigate identified risks. Risk assessments are reviewed and updated at least annually, or more frequently in response to significant changes in our business environment or threat landscape. The outcome of the risk assessment will be used to guide the selection and implementation of security controls outlined in this policy.

3. Data Protection

Protecting sensitive data is paramount. We implement the following data protection measures:

- --Data Classification:-- Data is categorized based on its sensitivity and criticality (e.g., Public, Internal, Confidential, Restricted). Appropriate security controls are applied based on the classification level.
- --Data Encryption:-- Encryption is used to protect sensitive data both in transit (e.g., via HTTPS) and at rest (e.g., encrypting storage devices).
- --Data Loss Prevention (DLP):-- Measures are in place to prevent sensitive data from leaving the organization without authorization. This may include monitoring outbound communications and restricting access to removable media.
- --Data Backup and Recovery:-- Regular backups of critical data are performed and stored securely. Recovery procedures are tested regularly to ensure timely restoration in the

event of a data loss incident.

- --Data Retention and Disposal:-- Data is retained only as long as necessary to meet business and regulatory requirements. When data is no longer needed, it is securely disposed of using approved methods.

4. Access Controls

Access to information systems and data is restricted to authorized users based on the principle of least privilege. The following access control measures are implemented:

- --User Authentication:-- Strong passwords, multi-factor authentication (MFA) where feasible, and secure login procedures are required for all users.
- --Role-Based Access Control (RBAC):-- Access rights are granted based on job roles and responsibilities. Users are only granted the minimum level of access necessary to perform their duties.
- --Access Reviews:-- Periodic reviews of user access rights are conducted to ensure that access remains appropriate and that unnecessary privileges are revoked.
- --Remote Access:-- Secure remote access methods (e.g., VPN) are used to protect data transmitted over public networks.
- --Physical Security:-- Physical access to server rooms, data centers, and other sensitive areas is restricted to authorized personnel.

5. Incident Response

A well-defined incident response plan is in place to handle security incidents effectively and efficiently. The plan includes the following elements:

- --Incident Detection and Reporting:-- Procedures for detecting and reporting security incidents, including suspicious activity, data breaches, and malware infections. All employees are responsible for reporting any suspected security incidents to the designated security team.
- --Incident Containment:-- Measures to isolate and contain the impact of a security incident, preventing further damage or data loss.
- --Incident Eradication:-- Procedures for removing the cause of a security incident, such as malware or vulnerabilities.
- --Incident Recovery:-- Steps to restore systems and data to a normal operational state.
- --Post-Incident Analysis:-- Review of security incidents to identify root causes and improve security controls. Lessons learned are documented and used to update the incident response plan.
- --Communication:-- Establish protocols for communicating about security incidents to relevant stakeholders, including management, employees, customers, and regulatory authorities, as required.

6. Security Awareness Training

Security awareness training is provided to all employees to educate them about cybersecurity threats and best practices. Training covers topics such as:

- --Phishing Awareness:-- Recognizing and avoiding phishing attacks.
- --Password Security:-- Creating strong passwords and protecting them from compromise.

- --Data Protection:-- Handling sensitive data securely.
- --Social Engineering:-- Recognizing and avoiding social engineering tactics.
- --Incident Reporting:-- Reporting suspected security incidents.
- --Mobile Device Security:-- Securing mobile devices used for work purposes.

Training is provided upon hire and annually thereafter, or more frequently as needed to address emerging threats.

7. Compliance and Auditing

This Cybersecurity Policy is aligned with the principles of ISO/IEC 27001 and other relevant regulatory requirements. We conduct regular internal audits to assess compliance with this policy and identify areas for improvement. External audits may also be conducted to provide independent assurance of our security posture. Audit findings are reviewed by management and used to strengthen our security controls.

Specific compliance tasks include:

- --Regular Vulnerability Scanning:-- Scans are conducted on critical infrastructure to proactively identify and remediate vulnerabilities.
- --Log Monitoring:-- Logs from critical systems are monitored for suspicious activity.
- --Policy Review:-- This policy is reviewed and updated at least annually to ensure its continued relevance and effectiveness.
- --Vendor Security Assessments:-- Third-party vendors who access our systems or data are subject to security assessments to ensure that they meet our security requirements.

8. Conclusion

This Cybersecurity Policy is essential for protecting our information assets and maintaining a secure operating environment. By adhering to the guidelines outlined in this policy, all users contribute to the overall security of our organization. Management is committed to providing the resources necessary to implement and maintain this policy effectively. Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.