Cybersecurity Policy for Low Risk Environment

--1. Introduction--

This Cybersecurity Policy outlines the framework for protecting the confidentiality, integrity, and availability of [Company Name]'s information assets in a low-risk environment. This policy applies to all employees, contractors, vendors, and any other individuals or entities accessing or using [Company Name]'s systems and data. The goal of this policy is to establish a baseline of security controls proportionate to the assessed risk, balancing security needs with business efficiency and user experience. This policy is aligned with the Risk Management Framework (RMF) and will be reviewed and updated at least annually, or more frequently as needed, to address changes in the threat landscape, business operations, or regulatory requirements.

--2. Risk Assessment--

[Company Name] conducts regular risk assessments to identify, analyze, and evaluate potential threats and vulnerabilities that could impact our information assets. Given our determination as a low-risk environment, risk assessments will be performed annually, or when significant changes occur to our infrastructure, applications, or business processes.

The risk assessment process will:

- --Identify Assets:-- Catalog all critical IT assets, including hardware, software, data, and services.
- --Identify Threats:-- Recognize potential threats to these assets, such as malware, phishing attacks, data breaches, and insider threats. In a low-risk environment, the focus is on prevalent, readily available threats rather than advanced persistent threats (APTs).
- --Identify Vulnerabilities:-- Determine weaknesses in our systems, applications, and processes that could be exploited by threats. Vulnerability scanning will be conducted quarterly.
- --Assess Likelihood and Impact:-- Evaluate the probability of a threat exploiting a vulnerability and the potential impact on the business.
- --Determine Risk Level:-- Assign a risk level to each identified risk based on the likelihood and impact assessment. Risk levels are categorized as Low, Medium, or High. Only Low risk items are considered acceptable.
- --Develop Mitigation Strategies:-- For risks exceeding the acceptable level (Low), implement appropriate controls to reduce the likelihood or impact of the risk.

The results of the risk assessment will be documented and used to inform the development and implementation of security controls.

--3. Data Protection--

Protecting the confidentiality and integrity of our data is paramount.

- --Data Classification:-- Data will be classified based on its sensitivity and criticality. Data classification categories will include:
- --Public:-- Information freely available to anyone.
- --Internal:-- Information intended for internal use only.

- --Confidential:-- Sensitive information that requires protection from unauthorized disclosure.
- --Data Storage:-- Data will be stored securely using appropriate encryption and access controls, dependent on classification.
- --Data Transmission:-- Sensitive data transmitted electronically will be encrypted using industry-standard protocols.
- --Data Disposal:-- Data will be securely disposed of when it is no longer needed. Electronic data will be securely wiped, and physical media will be shredded.
- --Backup and Recovery:-- Regular backups of critical data will be performed and stored in a secure, offsite location. Backup and recovery procedures will be tested periodically to ensure their effectiveness.

--4. Access Controls--

Access to systems and data will be restricted to authorized personnel based on the principle of least privilege.

- --User Account Management:-- All users will have unique accounts with strong passwords. Accounts will be created, modified, and disabled promptly as needed. Password complexity requirements will be enforced. Multi-factor authentication (MFA) will be enabled for all privileged accounts and where deemed necessary based on risk assessment.
- --Role-Based Access Control (RBAC):-- Access to systems and data will be granted based on job roles and responsibilities.
- --Privileged Access Management:-- Access to privileged accounts will be strictly controlled and monitored.
- --Remote Access:-- Secure remote access will be provided using VPN or other secure technologies. Remote access will require MFA.
- --Physical Security:-- Physical access to data centers and other sensitive areas will be restricted to authorized personnel.

--5. Incident Response--

A comprehensive incident response plan will be maintained to address security incidents effectively.

- --Incident Identification:-- All employees are responsible for reporting suspected security incidents immediately to the designated incident response team.
- --Incident Containment:-- Actions will be taken to contain the incident and prevent further damage.
- --Incident Eradication:-- The root cause of the incident will be identified and eliminated.
- --Incident Recovery:-- Systems and data will be restored to normal operations.
- --Post-Incident Analysis:-- A post-incident analysis will be conducted to identify lessons learned and improve security controls.
- --Communication:-- A communication plan will be followed to keep stakeholders informed about the incident and its resolution.

--6. Security Awareness Training--

All employees will receive security awareness training to educate them about security threats and best practices.

- --Annual Training:-- Security awareness training will be conducted annually.
- --Training Topics:-- Training topics will include:
- Phishing awareness
- Password security
- Data protection
- Social engineering
- Incident reporting
- --Training Delivery:-- Training will be delivered through a variety of methods, such as online modules, workshops, and presentations.
- --Regular Reminders:-- Ongoing security awareness reminders and tips will be provided to employees.

--7. Compliance and Auditing--

[Company Name] is committed to complying with all applicable laws, regulations, and standards, including the Risk Management Framework (RMF).

- --RMF Compliance:-- This policy is aligned with the RMF framework, specifically tailored to a low-risk environment. Security controls will be selected and implemented based on the RMF guidelines.
- --Internal Audits:-- Regular internal audits will be conducted to assess compliance with this policy and other security standards. Audits will be performed at least annually.
- --External Audits:-- External audits may be conducted by third-party organizations to provide independent assurance of security controls.
- --Policy Review:-- This policy will be reviewed and updated at least annually, or more frequently as needed, to address changes in the threat landscape, business operations, or regulatory requirements.

--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 our exposure to security threats and maintain a secure and reliable IT environment. All employees are expected to understand and comply with this policy. Non-compliance with this policy may result in disciplinary action, up to and including termination of employment. This policy is a living document and will be continuously improved to address emerging threats and evolving business needs.