# Cybersecurity Policy for Low Risk Environment

--1. Introduction--

This Cybersecurity Policy outlines the mandatory security practices for all employees, contractors, and vendors ("Users") of [Company Name] and any individuals or entities accessing [Company Name]'s information assets, systems, and networks. This policy is designed to protect the confidentiality, integrity, and availability of company data, systems, and infrastructure, aligning with industry best practices and the requirements of ISO/IEC 27001, tailored to our low-risk operational profile. This policy applies to all information, regardless of format (electronic, paper, verbal), and covers all company-owned or managed devices, networks, and cloud services. Adherence to this policy is a condition of employment or engagement.

--2. Risk Assessment--

[Company Name] acknowledges its responsibility to conduct ongoing risk assessments to identify, analyze, and evaluate potential threats and vulnerabilities to its information assets. While operating in a low-risk environment, periodic risk assessments, at least annually, will be performed. These assessments will consider factors such as:

- The value and sensitivity of information assets.
- Potential threats, including malware, phishing, social engineering, and unauthorized access.
- Vulnerabilities in systems, networks, and applications.
- The likelihood and impact of identified risks.

The results of the risk assessments will be used to inform the development and implementation of appropriate security controls to mitigate identified risks. The risk assessment methodology will be documented and regularly reviewed.

--3. Data Protection--

[Company Name] is committed to protecting the confidentiality, integrity, and availability of its data. The following data protection measures will be implemented:

- --Data Classification:-- Data will be classified based on its sensitivity and criticality. Classifications will be reviewed annually.
- --Data Encryption:-- Encryption will be implemented for sensitive data at rest and in transit, where practical.
- --Data Backup and Recovery:-- Regular backups of critical data will be performed and stored in a secure location, with documented recovery procedures tested at least annually.
- --Data Retention and Disposal:-- Data will be retained only as long as necessary for business or legal requirements and securely disposed of when no longer needed, following a defined data retention policy.
- --Data Loss Prevention (DLP):-- Reasonable measures will be implemented to prevent data loss, such as monitoring for unauthorized data transfers and restricting access to sensitive data.

--4. Access Controls--

Access to information assets will be restricted based on the principle of least privilege. The following access control measures will be implemented:

- --User Account Management:-- All users will be assigned unique usernames and passwords. A formal process will be in place for creating, modifying, and disabling user accounts.
- --Password Policy:-- Strong passwords will be required, and users will be educated on password security best practices, including avoiding the reuse of passwords. Passwords must be changed every 90 days at minimum.
- --Multi-Factor Authentication (MFA):-- MFA will be implemented for access to sensitive systems and data, where feasible.
- --Role-Based Access Control (RBAC):-- Access to systems and data will be granted based on defined roles and responsibilities.
- --Regular Access Reviews:-- User access privileges will be reviewed periodically, at least annually, to ensure that they remain appropriate.

--5. Incident Response--

[Company Name] will maintain an Incident Response Plan (IRP) to effectively address security incidents. The IRP will outline the following:

- --Incident Reporting Procedures:-- Users will be trained on how to report suspected security incidents.
- --Incident Response Team:-- A designated Incident Response Team will be responsible for managing and coordinating incident response activities.
- --Incident Classification and Prioritization:-- Incidents will be classified and prioritized based on their severity and impact.
- --Incident Containment, Eradication, and Recovery:-- Procedures for containing, eradicating, and recovering from security incidents will be defined.
- --Post-Incident Analysis:-- A post-incident analysis will be conducted to identify the root cause of the incident and implement corrective actions to prevent future occurrences.
- --Regular Testing:-- The Incident Response Plan will be tested at least annually through tabletop exercises or simulations.

--6. Security Awareness Training--

[Company Name] recognizes that security awareness is critical to protecting its information assets. All users will be required to participate in security awareness training on an annual basis. The training will cover topics such as:

- Phishing awareness
- Password security
- Social engineering
- Data protection
- Incident reporting
- Acceptable use of company resources

Regular security reminders and updates will be provided to users throughout the year.

--7. Compliance and Auditing--

[Company Name] is committed to complying with all applicable laws, regulations, and contractual obligations, including the requirements of ISO/IEC 27001.

- --Internal Audits:-- Periodic internal audits will be conducted to assess compliance with this policy and other relevant security standards.
- --External Audits:-- External audits may be conducted to provide independent assurance of the effectiveness of security controls.
- --Policy Review:-- This policy will be reviewed and updated at least annually to ensure its continued relevance and effectiveness.

--8. Conclusion--

This Cybersecurity Policy is essential for protecting [Company Name]'s information assets and maintaining a secure operating environment. All users are responsible for understanding and adhering to this policy. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or engagement. The CISO is responsible for the enforcement and maintenance of this policy. Questions or concerns regarding this policy should be directed to the CISO or the IT department.