Cybersecurity Policy for Operations (Low Risk Environment)

1. Introduction

This Cybersecurity Policy outlines the essential security measures for protecting the confidentiality, integrity, and availability of information assets within our Operations environment. It applies to all employees, contractors, vendors, and any other individuals accessing or using company resources. This policy aims to establish a security foundation that supports our operational efficiency while maintaining an acceptable level of risk, tailored for a low-risk profile and aligned with NIST cybersecurity framework principles. This policy will be reviewed and updated annually, or more frequently as required by changes in business operations, threat landscape, or regulatory requirements.

2. Risk Assessment

While this environment is categorized as low-risk, regular risk assessments are crucial to identify and address potential vulnerabilities. These assessments will be conducted at least annually, focusing on identifying assets, threats, and vulnerabilities, and determining the likelihood and impact of potential security incidents. The outcomes of these risk assessments will inform the prioritization and implementation of appropriate security controls outlined in this policy. Due to the low-risk designation, risk assessments will focus on common threats like phishing, malware, and weak passwords. A simplified, documented risk assessment methodology will be used, focusing on practical and cost-effective mitigation strategies.

3. Data Protection

Data protection is paramount, even in a low-risk environment. All data will be classified based on its sensitivity and criticality. Basic data handling procedures will be implemented to ensure appropriate storage, access, and disposal of information.

- --Data Classification:-- Data will be classified into three categories: Public, Internal, and Confidential. Definitions for each category will be maintained and easily accessible to all employees.
- --Data Storage:-- Sensitive data (Internal and Confidential) must be stored on secure, designated systems.
- --Data Transmission:-- Transmission of sensitive data (Internal and Confidential) outside the internal network requires encryption. Approved methods for encryption will be communicated and supported.
- --Data Disposal:-- All data must be securely disposed of when no longer needed, following established procedures. Physical documents containing sensitive information must be shredded. Digital data must be securely wiped using approved methods.

4. Access Controls

Access to systems and data will be granted based on the principle of least privilege. User access rights will be reviewed regularly (at least annually) and revoked promptly when no longer required.

- --User Authentication:-- Strong passwords are required for all user accounts. Multifactor

authentication (MFA) is encouraged where available, especially for access to critical systems. Password complexity requirements will be enforced.
- --Account Management:-- A formal process for creating, modifying, and disabling user accounts will be maintained. All user accounts must be uniquely identifiable. Shared accounts are prohibited.
- --Authorization:-- Access to systems and data will be granted based on job roles and responsibilities. Access requests must be approved by the relevant data or system owner.

5. Incident Response

A basic incident response plan will be maintained to address potential security incidents. This plan will outline the procedures for reporting, investigating, and resolving security incidents.

- --Incident Reporting:-- All employees are responsible for reporting suspected security incidents to the designated security contact.
- --Incident Handling:-- A defined process will be followed for investigating and resolving security incidents. This process includes containment, eradication, recovery, and post-incident analysis.
- --Communication:-- Clear communication channels will be established for disseminating information during a security incident.

6. Security Awareness Training

Regular security awareness training will be provided to all employees to educate them on common threats and security best practices.

- --Training Content:-- Training will cover topics such as phishing awareness, password security, data protection, and incident reporting.
- --Training Frequency:-- Security awareness training will be conducted at least annually, or more frequently as needed.
- --Training Delivery:-- Training will be delivered through a variety of methods, including online modules, presentations, and simulated phishing exercises.

7. Compliance and Auditing

This Cybersecurity Policy is aligned with NIST cybersecurity framework. Periodic security audits will be conducted to assess compliance with this policy and identify areas for improvement.

- --Policy Compliance:-- All employees are responsible for complying with this Cybersecurity Policy.
- --Audit Scope:-- Audits will cover all aspects of the policy, including data protection, access controls, and incident response.
- --Audit Frequency:-- Audits will be conducted at least annually, or more frequently as needed.
- --Corrective Actions:-- Any identified non-compliance issues will be addressed through corrective action plans.

8. Conclusion

This Cybersecurity Policy is essential for protecting our information assets and maintaining the integrity of our Operations environment. By adhering to these guidelines, we can collectively reduce our risk exposure and ensure the continued success of our operations. All employees are expected to understand and comply with this policy. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment.