Cybersecurity Policy for Operations - Low Risk Environment

1. Introduction

This Cybersecurity Policy outlines the standards and procedures implemented to protect the confidentiality, integrity, and availability of information assets within our Operations environment. This policy is designed to address the specific risks associated with our industry while acknowledging the assessment of a "Low Risk" operating environment. All employees, contractors, vendors, and any other individuals with access to our systems and data are expected to adhere to this policy. This policy supports our commitment to responsible data handling and compliance with applicable regulations, including the DDRO compliance standard.

2. Risk Assessment

Due to the identified "Low Risk" environment, we will conduct risk assessments on an annual basis, or more frequently if significant changes occur in our operational environment, threat landscape, or regulatory requirements. These assessments will identify potential threats, vulnerabilities, and their potential impact on our business operations. While the overall risk is deemed low, the assessments will still consider factors such as:

- --Data Sensitivity:-- Identifying the classification of data handled (e.g., public, internal, confidential).
- --System Criticality:-- Determining the importance of IT systems to business operations.
- --Threat Landscape:-- Monitoring for emerging threats relevant to our industry and business profile.
- --Vulnerability Scanning:-- Regularly scanning systems for known vulnerabilities.

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

3. Data Protection

Despite operating in a low risk environment, data protection is paramount. The following measures are in place:

- --Data Classification:-- Data will be classified based on sensitivity and business value. This will inform appropriate handling and storage procedures.
- --Data Storage:-- Data will be stored securely using appropriate physical and logical controls, including encryption where deemed necessary based on data classification.
- --Data Transmission:-- Sensitive data transmitted electronically will be protected using encryption protocols such as TLS/SSL.
- --Data Backup and Recovery:-- Regular backups of critical data will be performed and stored securely offsite. A documented recovery plan will be maintained and tested periodically.
- --Data Disposal:-- Data will be securely disposed of using methods that prevent unauthorized access, such as data wiping or physical destruction of storage media.

4. Access Controls

Access to systems and data will be granted based on the principle of least privilege. The

following access control measures are implemented:

- --User Authentication:-- Strong passwords or multi-factor authentication (MFA), where feasible, will be required for all users.
- --Role-Based Access Control (RBAC):-- Access permissions will be assigned based on job roles and responsibilities.
- --Account Management:-- User accounts will be created, modified, and terminated promptly. Regular reviews of user access rights will be conducted.
- --Remote Access:-- Secure methods, such as VPNs, will be used for remote access to the network.
- --Physical Security:-- Physical access to IT infrastructure will be restricted to authorized personnel only.

5. Incident Response

Even in a low risk environment, it is crucial to have procedures in place to effectively manage security incidents. An Incident Response Plan (IRP) will be maintained and regularly reviewed. The IRP outlines the steps to be taken in the event of a security incident, including:

- --Incident Identification:-- Procedures for identifying and reporting potential security incidents.
- --Incident Containment:-- Measures to contain the impact of a security incident.
- --Incident Eradication:-- Steps to remove the cause of the incident.
- --Incident Recovery:-- Procedures for restoring systems and data to normal operation.
- --Post-Incident Analysis:-- A review of the incident to identify lessons learned and improve security controls.

6. Security Awareness Training

All employees will receive security awareness training upon hire and annually thereafter. Training will cover topics such as:

- --Password Security:-- Creating and maintaining strong passwords.
- --Phishing Awareness:-- Recognizing and avoiding phishing scams.
- --Data Handling:-- Proper procedures for handling and protecting sensitive data.
- --Incident Reporting:-- Procedures for reporting security incidents.
- --Social Engineering:-- Recognizing and avoiding social engineering attacks.

The training will be tailored to the specific risks and threats relevant to our Operations environment, despite it's low risk profile.

7. Compliance and Auditing

We are committed to complying with all applicable laws, regulations, and industry standards, including DDRO.

- --DDRO Compliance:-- We will implement and maintain controls necessary to achieve and maintain compliance with the DDRO standard. Specific requirements of DDRO regarding data handling, access controls, and incident reporting will be implemented and documented.
- --Internal Audits:-- Regular internal audits will be conducted to assess the effectiveness

of our security controls and compliance with this policy and relevant regulations.
- --External Audits:-- Periodic external audits may be conducted to provide independent assurance of our security posture and compliance with applicable standards.

8. Conclusion

This Cybersecurity Policy is a critical component of our overall risk management strategy. While our environment is categorized as "Low Risk," adherence to this policy is essential to protect our information assets and maintain the trust of our stakeholders. This policy will be reviewed and updated periodically to ensure it remains relevant and effective in addressing evolving threats and regulatory requirements. The CISO is responsible for the implementation and enforcement of this policy, with support from all employees and stakeholders.