```text
# Cybersecurity Policy for a Low-Risk Financial Environment

### 1. Introduction

This Cybersecurity Policy outlines the minimum-security requirements for all information systems and data within [Organization Name], a financial institution operating in a low-risk environment. This policy aims to protect the confidentiality, integrity, and availability of our assets while adhering to relevant compliance standards, specifically the Risk Management Framework (RMF). This policy applies to all employees, contractors, vendors, and any other individuals or entities accessing, processing, or storing organizational data. A low-risk environment, in this context, implies that the organization's systems and data are not subject to high-value transactions or sensitive customer information that would typically be targeted by sophisticated threat actors. However, a foundational level of cybersecurity is still critical to prevent basic attacks and ensure business continuity.

### 2. Risk Assessment

[Organization Name] will conduct periodic risk assessments to identify, analyze, and evaluate potential threats and vulnerabilities to our information systems. These assessments will:

• Identify critical assets and data.
• Identify potential threats (e.g., malware, phishing, data breaches, insider threats).
• Identify vulnerabilities in systems, applications, and processes.
• Assess the likelihood and impact of identified risks.
• Prioritize risks based on their potential impact on the organization.
• Develop and implement mitigation strategies to reduce identified risks.

Risk assessments will be reviewed and updated at least annually or more frequently if significant changes occur in the threat landscape, business operations, or technology infrastructure.

### 3. Acceptable Use Policy (AUP)

This Acceptable Use Policy (AUP) governs the use of [Organization Name]'s information resources, including but not limited to computers, networks, internet access, email, software, and data. All users are responsible for using these resources responsibly and ethically.

• --Permitted Uses:-- Company resources are primarily for conducting official business. Limited personal use is permitted as long as it does not interfere with work responsibilities, violate this policy, or consume excessive resources.
• --Prohibited Uses:-- The following activities are strictly prohibited:
• Accessing, storing, or transmitting illegal, offensive, or discriminatory content.
• Engaging in activities that could damage, disrupt, or compromise the security of company systems or networks.
• Unauthorized access to systems, data, or accounts.
• Sharing passwords or other authentication credentials.
```

- Downloading or installing unauthorized software.
- Circumventing security controls.
- Engaging in any activity that violates applicable laws or regulations.
- Using company resources for personal profit or commercial gain without authorization.
- Excessive use of bandwidth or storage that negatively impacts other users.
- --Monitoring:-- [Organization Name] reserves the right to monitor the use of its information resources to ensure compliance with this policy.
- --Consequences of Violation:-- Violations of this AUP may result in disciplinary action, up to and including termination of employment or contract, as well as potential legal consequences.

4. Data Protection

Data protection is paramount. [Organization Name] will implement the following measures to protect data:

- --Data Classification:-- Data will be classified based on its sensitivity and criticality (e.g., public, internal, confidential).
- --Data Encryption:-- Sensitive data, both in transit and at rest, will be encrypted using industry-standard encryption algorithms.
- --Data Backup and Recovery:-- Regular data backups will be performed and stored in a secure offsite location. Recovery procedures will be tested regularly to ensure timely restoration of data in case of a disaster or data loss event.
- --Data Loss Prevention (DLP):-- DLP measures will be implemented to prevent sensitive data from leaving the organization's control.
- --Data Retention:-- Data will be retained according to legal and regulatory requirements and business needs.
- --Data Destruction:-- When data is no longer needed, it will be securely destroyed using approved methods.

5. Access Controls

Access to information systems and data will be restricted based on the principle of least privilege. This means that users will only be granted the minimum level of access necessary to perform their job duties. Access control measures include:

- --User Authentication:-- All users will be required to authenticate their identity before accessing systems and data. Strong authentication methods, such as multi-factor authentication (MFA), will be used where feasible and appropriate.
- --Role-Based Access Control (RBAC):-- Access permissions will be assigned based on user roles and responsibilities.
- --Regular Access Reviews:-- User access privileges will be reviewed periodically to ensure they remain appropriate.
- --Password Management:-- Users will be required to create strong passwords that meet specific complexity requirements and change their passwords regularly. Password reuse will be prohibited.
- --Physical Security:-- Physical access to data centers and other sensitive areas will be restricted and monitored. This includes:

- Controlling access to the building via keycards, biometric scanners, or security personnel.
- Securing server rooms with locked doors and limited access.
- Implementing visitor management procedures.
- Regularly reviewing and updating physical security measures.
- Surveillance cameras in sensitive areas.

6. Vulnerability Management

[Organization Name] will implement a vulnerability management program to identify and remediate security vulnerabilities in our systems and applications. This program will include:

- --Regular Vulnerability Scans:-- Periodic vulnerability scans of all systems and applications, both internal and external facing, using automated scanning tools. Scans will occur at least quarterly, and more frequently for critical systems.
- --Patch Management:-- Timely application of security patches to address identified vulnerabilities. A defined patching schedule will be established, with critical patches applied as soon as possible after release.
- --Vulnerability Assessment and Prioritization:-- Assessment of the severity of identified vulnerabilities based on CVSS scores and potential impact. Prioritization of remediation efforts based on risk.
- --Remediation Tracking:-- Tracking of vulnerability remediation efforts to ensure timely completion.
- --Exception Management:-- A formal process for documenting and approving exceptions to the patching schedule when immediate patching is not feasible. Compensating controls must be in place for any approved exceptions.

7. Third-Party Security

[Organization Name] recognizes the security risks associated with third-party vendors and will implement the following measures to mitigate these risks:

- --Vendor Risk Assessment:-- Conduct security risk assessments of all new and existing vendors before granting access to our systems or data. The assessment should consider the vendor's security posture, data protection practices, and compliance with relevant regulations.
- --Security Requirements:-- Include security requirements in contracts with vendors, specifying their responsibilities for protecting our data and systems.
- --Due Diligence:-- Perform due diligence on vendors to verify their security claims and ensure they have adequate security controls in place. This may include reviewing their security certifications, audit reports, and policies.
- --Ongoing Monitoring:-- Continuously monitor vendor security performance and compliance with contractual requirements.
- --Right to Audit:-- Reserve the right to audit vendor security controls.
- --Incident Response Plan:-- Require vendors to have an incident response plan in place and to notify us immediately of any security incidents that may affect our data or systems.
- --Data Security Addendums:-- Execute data security addendums that clearly define the data

security requirements the vendor must adhere to.

8. Incident Response

[Organization Name] will maintain an incident response plan to effectively manage and respond to security incidents. The incident response plan will include:

- --Incident Identification:-- Procedures for identifying and reporting security incidents.
- --Incident Containment:-- Steps to contain and isolate the impact of a security incident.
- --Incident Eradication:-- Actions to remove the cause of the security incident.
- --Incident Recovery:-- Procedures to restore systems and data to their normal state.
- --Post-Incident Activity:-- Post-incident analysis to identify lessons learned and improve security measures.

All employees will be trained on how to identify and report security incidents. Security incidents will be reported to the designated incident response team immediately.

9. Security Awareness Training

All employees, contractors, and vendors will receive regular security awareness training to educate them about cybersecurity threats and best practices. Training topics will include:

- Phishing awareness
- Malware prevention
- Password security
- Data protection
- Incident reporting
- Social engineering
- Acceptable Use Policy
- Physical Security Awareness

Security awareness training will be provided upon hire and annually thereafter.

10. Compliance and Auditing

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

- Implement and maintain controls based on RMF guidelines.
- Conduct regular internal audits to assess compliance with this policy and other security requirements.
- Cooperate fully with external audits and inspections.
- Maintain documentation to demonstrate compliance with applicable requirements.
- Address any identified compliance gaps promptly and effectively.

11. Conclusion

This Cybersecurity Policy is essential for protecting [Organization Name]'s information assets and ensuring the confidentiality, integrity, and availability of our data. All personnel are responsible for adhering to this policy. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or

contract. 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 technology infrastructure. The [Designated Security Officer/Team] is responsible for overseeing the implementation and enforcement of this policy.
```

Key improvements and explanations:

- --Acceptable Use Policy (AUP):-- A dedicated section defining permissible and prohibited uses of company resources. This addresses the feedback about employee behavior and resource utilization. Includes sections on "Permitted Uses", "Prohibited Uses", "Monitoring" and "Consequences of Violation".
- --Vulnerability Management:-- A full section dedicated to regular scans, patching protocols, assessment & prioritization, remediation tracking, and exception management. The frequency of scans (quarterly) is specified. Exception Management allows for flexibility when patching immediately is impossible but requires compensating controls.
- --Third-Party Security:-- A dedicated section that includes vendor risk assessments, security requirements in contracts, due diligence, ongoing monitoring, right to audit, incident response plan requirements for vendors, and data security addendums. This provides a framework for managing risks associated with vendors.
- --Physical Security:-- Expanded the bullet point into a more comprehensive section outlining specific measures, including access control, server room security, visitor management, and surveillance cameras. This section now describes -how- physical security is maintained.
- --Security Awareness Training Updates:-- Added "Acceptable Use Policy" and "Physical Security Awareness" to the topics covered in security awareness training. This ensures employees are aware of the new policies and their roles in maintaining security.
- --Improved Clarity and Organization:-- The policy has been reorganized and clarified for better readability and understanding. The use of headings and bullet points makes it easier to scan and find specific information.

This revised policy addresses all the feedback points and provides a more robust and comprehensive cybersecurity framework for a low-risk financial environment. It is more actionable and provides clearer guidance for employees, contractors, and vendors. Remember to tailor this policy to your specific organization's needs and risk profile.
```