Okay, here's a cybersecurity policy tailored for a finance industry context, addressing low-risk scenarios primarily while aligning with NIST standards. This example focuses on a specific "Low" risk example - employees using non-company approved cloud storage f non-sensitive documents. It's a starting point and will require customization based on your specific organizational needs and environment.

Cybersecurity Policy for [Your Finance Company Name]

1. Introduction

1.1. Purpose: This Cybersecurity Policy outlines the mandatory security controls and practices that must be adhered to by all employees, contractors, vendors, and any other individuals or entities accessing or using [Your Finance Company Name]'s information assets and systems. This policy aims to protect the confidentiality, integrity, and availability of our data and systems, ensuring business continuity and compliance with applicable laws, regulations, and industry standards. This version of the policy is focused on addressing Low cybersecurity risks, and as such some elements will be simplified.

1.2. Scope: This policy applies to all information assets owned, leased, or otherwise controlled by [Your Finance Company Name], regardless of their physical location or the individual using them. This includes, but is not limited to:

- Computer systems (desktops, laptops, servers, virtual machines)
- Mobile devices (company-issued and personal devices used for company business)
- Networks (wired and wireless)
- Software applications
- Data (electronic and physical)
- Cloud services

• Physical facilities

1.3. Policy Objectives:

• To establish a framework for managing and mitigating cybersecurity risks.

• To protect the confidentiality, integrity, and availability of company data.

• To ensure compliance with all applicable laws, regulations, and industry standards.

• To promote a security-conscious culture within the organization.

• To provide guidance and direction for secure practices and behaviors.

1.4. Policy Ownership & Enforcement: The Chief Information Security Officer (CISO) is responsible for the development, maintenance, and enforcement of this policy. All employees are responsible for adhering to this policy. Violations may result in disciplinary action, up to and including termination of employment.

2. Risk Assessment

2.1. Risk Assessment Methodology: [Your Finance Company Name] employs a risk-based approach to cybersecurity, utilizing the NIST Risk Management Framework (RMF) as a guideline. Risk assessments are conducted periodically (at least annually) and whenever significant changes occur to the organization's systems, applications, or business processes.

2.2. Risk Identification: Risk identification involves identifying potential threats and vulnerabilities that could impact the confidentiality, integrity, or availability of company data.

2.3. Risk Analysis: Risk analysis involves assessing the likelihood and impact of identified risks to determine their overall severity.

2.4. Risk Mitigation: Risk mitigation involves implementing security controls to reduce

the likelihood or impact of identified risks to an acceptable level.

2.5 Specific Low Risk Example:

This policy acknowledges the risk of employees using unauthorized, non-company approv
cloud storage (e.g., personal Dropbox, Google Drive) for storing non-sensitive documents
This is considered a low risk because the data in question is not deemed confidential or
highly sensitive.

- Threat: Unauthorized access to non-sensitive data by third parties due to cloud storage
  providers vulnerabilities or employee negligence.
- Vulnerability: Employees using non-approved cloud storage services outside of compan
  oversight.
- Likelihood: Medium (employees may find it convenient, and security practices vary acr
  cloud providers)
- Impact: Low (non-sensitive data breach, potential for malware introduction, reputationa
  risk)
- Risk Level: Low

2.6. Mitigation Strategy for Low Risk Example: Awareness training emphasizing the
importance of using approved storage solutions, even for non-sensitive data, and clearly
defining what data is considered "non-sensitive."

3. Data Protection

3.1. Data Classification: Data is classified according to its sensitivity and criticality.
Examples: Public, Internal, Confidential, Restricted. (Note: For low-risk scenarios, a
simplified classification scheme may be appropriate). This specific policy element is not
as critical when focusing only on low-risk data.

3.2. Data Handling: All data must be handled in accordance with its classification.

Specific guidelines for handling each data classification will be provided separately.

3.3. Data Storage: Data must be stored securely, using appropriate encryption and acces
controls.

3.4. Data Transmission: Data transmitted over networks must be encrypted using strong
encryption protocols.

3.5. Data Disposal: Data must be disposed of securely when it is no longer needed, using
approved methods.

3.6. Cloud Storage:

- Only company-approved cloud storage services are permitted for storing company data
- Employees using non-approved cloud storage solutions must migrate the non-sensitive
  to the approved solutions.
- While non-sensitive data is allowed on these systems, it is recommended employees st
  use strong passwords, and are subject to occasional review.
- IT and security teams will not be responsible for managing data on non-approved cloud
  storage services.

4. Access Controls

4.1. Principle of Least Privilege: Access to systems and data must be granted based on th
principle of least privilege, meaning that users should only have access to the
information and resources necessary to perform their job duties.

4.2. User Authentication: Strong authentication methods, such as multi-factor
authentication (MFA), should be used whenever possible.

4.3. Password Management: Users must create and maintain strong passwords and adhe
the company's password policy.

4.4. Access Reviews: User access rights must be reviewed periodically to ensure that the
are still appropriate.

4.5. Account Management: User accounts must be created, modified, and disabled in a ti
manner.

5. Incident Response

5.1. Incident Response Plan (IRP): [Your Finance Company Name] maintains a compreher
Incident Response Plan (IRP) to address security incidents.

5.2. Incident Reporting: All security incidents, or suspected security incidents, must be
reported immediately to the IT Security team. Even incidents involving low-risk scenarios
should be reported.

5.3. Incident Handling: Security incidents will be handled according to the IRP, including
containment, eradication, recovery, and post-incident analysis.

5.4. Communication: Communication regarding security incidents will be coordinated by
IT Security team.

6. Security Awareness Training

6.1. Mandatory Training: All employees are required to participate in security awareness
training upon hire and annually thereafter. Training will cover topics such as phishing
awareness, password security, data protection, and incident reporting.

6.2. Phishing Simulations: [Your Finance Company Name] may conduct periodic phishing
simulations to assess employee awareness and identify areas for improvement.

6.3. Ongoing Awareness: Security awareness messages will be communicated regularly t
various channels, such as email, newsletters, and posters.

6.4. Specific Focus on Unapproved Cloud Storage: Training will emphasize the risks associated with using unapproved cloud storage services, even for non-sensitive data, ar the availability of approved alternatives.

7. Compliance and Auditing

7.1. Compliance Requirements: [Your Finance Company Name] is subject to various laws regulations, and industry standards, such as [List relevant regulations like PCI DSS, GLBA, GDPR, etc.].

7.2. Internal Audits: Internal audits will be conducted periodically to assess compliance with this policy and other security requirements.

7.3. External Audits: External audits may be conducted by regulatory agencies or other third parties.

7.4. Policy Review: This policy will be reviewed and updated at least annually, or more frequently as needed, to reflect changes in the threat landscape, regulatory requirement or business operations.

7.5. Enforcement: The CISO, IT Department, and relevant department heads are respons for the enforcement of this policy.

8. Conclusion

This Cybersecurity Policy is critical to protecting [Your Finance Company Name]'s information assets and ensuring the confidentiality, integrity, and availability of our data. All employees are expected to understand and adhere to this policy. By working together, we can create a secure environment for our business and our customers. Questions or concerns regarding this policy should be directed to the IT Security team.

Important Considerations and Customization:

- Tailor to your Organization: This is a template. You must customize it with your company's name, specific systems, data classifications, and the exact regulations you a subject to.
- Detailed Procedures: This policy provides a high-level overview. You will need to create more detailed procedures and guidelines to support the policy.
- Technology Controls: Implement technical controls to enforce the policy (e.g., blocking unauthorized cloud storage services with a web proxy).
- Regular Review and Updates: The cybersecurity landscape is constantly changing. Regularly review and update your policy to keep it relevant and effective.
- Legal Review: Have your legal counsel review the policy to ensure compliance with all applicable laws and regulations.
- Exception Process: Establish a clear process for requesting exceptions to the policy.
- Documentation: Maintain thorough documentation of your security controls and proces
- Communication: Effectively communicate the policy to all employees and stakeholders Provide training and support to help them understand and comply with the policy.
- Risk Tolerance: Even "low" risk situations should be actively managed and evaluated f evolving threats.

This example provides a solid foundation for building a cybersecurity policy that addresses your specific needs. Remember to prioritize thorough customization and ongo maintenance to ensure its effectiveness.