Okay, here's a cybersecurity policy tailored for a Finance company, focusing on a "Low" risk scenario (specifically, let's assume we're addressing the risk of unauthorized access to non-critical internal documentation) and adhering to GDPR principles. I'll include explanations of the reasoning behind the choices.

Reasoning and Context:

- Finance Industry Focus: The policy reflects the stringent regulatory environment of the finance industry, where data confidentiality, integrity, and availability are paramount, even when addressing seemingly "low" risks. Reputational damage alone can be devas
- GDPR Compliance: The policy is built with GDPR principles in mind. This means data minimization, purpose limitation, storage limitation, accountability, transparency, and the rights of data subjects (e.g., access, rectification, erasure).
- "Low" Risk Scenario - Unauthorized Access to Non-Critical Internal Documentation: This scenario is chosen to showcase how even a perceived low-risk needs a concrete, docur and measurable policy. This could include internal procedures or general company communications that if leaked, would not immediately present serious harm, but would be considered confidential and proprietary.
- Layered Security: The policy adopts a layered security approach, addressing data protection, access controls, incident response, and awareness training. It does not stop at technical implementations but also considers human factors, processes, and governa
- Proportionality: While we adhere to GDPR, the policy focuses on the principles of data protection without overburdening the organization for a risk considered to be low.

Cybersecurity Policy: Unauthorized Access to Non-Critical Internal Documentation

1. Introduction

1. 1. Purpose: This Cybersecurity Policy outlines the measures [Finance Company Name takes to protect non-critical internal documentation from unauthorized access, use, disclosure, disruption, modification, or destruction. This policy aims to maintain the confidentiality and integrity of sensitive information, even when it's classified as "low risk," and to comply with all applicable laws and regulations, including the General Data Protection Regulation (GDPR).

2. 2. Scope: This policy applies to all employees, contractors, vendors, consultants, and any other individuals or entities accessing or using [Finance Company Name]'s non-critical internal documentation, regardless of location or device. Non-critical internal documentation includes procedures, company communications, internal templates, and s information that is not directly related to customer data or core financial operations but remains confidential and proprietary to [Finance Company Name].

3. 3. Policy Ownership: The Chief Information Security Officer (CISO) is responsible for the development, implementation, and maintenance of this policy. Department Heads ar responsible for ensuring their teams adhere to this policy.

2. Risk Assessment

2. 1. Identification of Risk: [Finance Company Name] recognizes that unauthorized acce to non-critical internal documentation, while categorized as a "low" risk, can still lead to potential security incidents, reputational damage, and non-compliance with internal policies and external regulations.

3. 2. Risk Assessment Methodology: A risk assessment is conducted [Frequency, e.g., annually or upon significant system changes] to identify, analyze, and evaluate the risks associated with unauthorized access to non-critical internal documentation. This assessment considers the likelihood and impact of potential incidents.

4. 3. Risk Mitigation Strategy: Based on the risk assessment, the following measures are implemented to mitigate the identified risks:

- Implementation of Role-Based Access Control (RBAC) to limit access to documentation on job function.
- Regular review of access permissions.
- Training and awareness programs to educate employees on the importance of data sec
- Implementation of a document management system with version control.
- Secure storage and handling procedures for physical and electronic documents.

3. Data Protection

5. 1. Data Classification: All non-critical internal documentation is classified according to its sensitivity level. This classification determines the appropriate security measures to be applied.

6. 2. Data Minimization: Only necessary information is collected, processed, and stored. Redundant or unnecessary data is promptly removed.

7. 3. Data Encryption: While not all non-critical documentation requires strong encryption, reasonable measures should be taken to protect electronic documents, such password protection or access controls.

8. 4. Data Retention: Non-critical internal documentation is retained only for as long as necessary to fulfill its intended purpose and to comply with legal and regulatory requirements.

9. 5. Data Subject Rights (GDPR Considerations): While the focus is on internal documentation, if any internal documentation contains personal data (e.g., employee information in procedures), the company must respect data subject rights under GDPR, including the right to access, rectify, erase, restrict processing, and data portability.

The process for handling these requests should be aligned with the company's overall GD compliance framework.

4. Access Controls

10. 1. Role-Based Access Control (RBAC): Access to non-critical internal documentation i granted based on job function and assigned roles. Users are granted only the minimum necessary access rights required to perform their duties.

11. 2. Authentication: Strong authentication methods, such as strong passwords and mu factor authentication (MFA), are encouraged, where feasible, to verify user identities.

12. 3. Authorization: Access permissions are regularly reviewed and updated to ensure users only have access to the documentation required for their current role.

13. 4. Least Privilege: Access is granted on a need-to-know basis. Users only have acces to the information they need to perform their job duties.

5. Incident Response

14. 1. Incident Reporting: All suspected or confirmed security incidents, including unauthorized access to non-critical internal documentation, must be immediately reporte to the IT Security Department or the designated incident response team.

15. 2. Incident Response Plan: [Finance Company Name] maintains an incident response to address security incidents promptly and effectively.

16. 3. Incident Handling: The incident response team will investigate reported incidents, take appropriate containment and eradication measures, and implement corrective actio prevent future occurrences.

17. 4. Notification: Depending on the nature and scope of the incident, relevant

stakeholders, including legal counsel, regulatory bodies, and affected parties, may be notified.

6. Security Awareness Training

18. 1. Training Program: All employees are required to participate in regular security awareness training to educate them on data security best practices, including this policy's requirements.

19. 2. Training Content: The training program covers topics such as password security, phishing awareness, data handling, access control, and incident reporting.

20. 3. Training Frequency: Security awareness training is conducted [Frequency, e.g., annually or bi-annually] and whenever significant changes occur in the threat landscape [Finance Company Name]'s security policies.

7. Compliance and Auditing

21. 1. Policy Compliance: All employees are responsible for complying with this policy. Violations of this policy may result in disciplinary action, up to and including termination of employment.

22. 2. Internal Audits: Regular internal audits are conducted to assess compliance with this policy and to identify areas for improvement.

23. 3. External Audits: [Finance Company Name] may be subject to external audits by regulatory bodies or other third parties to assess compliance with applicable laws and regulations, including GDPR.

24. 4. Policy Review: This policy is reviewed and updated [Frequency, e.g., annually] or as needed to ensure it remains effective and aligned with evolving security threats,

regulatory requirements, and business needs.

8. Conclusion

25. 1. This Cybersecurity Policy is essential to protecting [Finance Company Name]'s nor critical internal documentation from unauthorized access and maintaining a secure environment. By adhering to the guidelines outlined in this policy, employees can contribute to protecting the confidentiality, integrity, and availability of [Finance Company Name]'s information assets. This policy is an ever-evolving document that will reviewed, and updated, on a regular basis.

Key Considerations & Adjustments:

- Specificity: This is a template. Replace bracketed placeholders ([...]) with concrete information specific to your organization.
- Risk Assessment Detail: The level of detail in your risk assessment will influence the specific controls you implement. If the assessment reveals more granular risks (e.g., specific departments with higher risk profiles), you might need to tailor the policy further.
- Technology Stack: Adapt the policy to reflect the specific technologies used within your environment (e.g., specific document management systems, identity providers).
- Legal Review: Crucially, have this policy reviewed by legal counsel to ensure it aligns with all applicable laws and regulations, and that the language is legally sound.
- Employee Handbook: Consider integrating key elements of this policy into the employe handbook for broader dissemination and awareness.
- Communication: Communicate the policy clearly and effectively to all employees. Ans their questions and provide ongoing support.

- Enforcement: Consistently enforce the policy. This sends a clear message that securit is a priority.
- Documentation: Keep detailed records of policy changes, training sessions, audits, and incident responses. This is crucial for demonstrating compliance.

This detailed policy provides a solid foundation for addressing the risk of unauthorized access to non-critical internal documentation, while simultaneously adhering to the principles of GDPR and the specific needs of the finance industry. Remember to tailor it to your organization's unique context.