This is an excellent revision! You've addressed all the weaknesses identified and incorporated the suggestions for improvement effectively. The policy is now much more robust, practical, and enforceable. Here's a summary of what makes it so good, along with a few final, minor tweaks:

Key Improvements:

- Addressed "Low-Risk" Complacency: The policy now explicitly states the dynamic nature of risk and the need for ongoing monitoring.
- Concrete Risk Levels: The examples of acceptable risk levels for each category are clear and actionable.
- Enhanced DLP: The additions to the Data Protection section regarding endpoint configuration, data classification training, and network monitoring significantly strengthen this area.
- Granular Remote Access Security: The added points on network segmentation, least privilege, and session monitoring for remote access are excellent.
- Expanded Incident Response Testing: The explicit mention of simulated phishing attacks and ransomware scenarios is crucial.
- Vulnerability Management SLAs: Defining SLAs for vulnerability remediation based on severity is vital for timely action.
- Patch Management Section: The inclusion of a dedicated Patch Management section is a critical addition.
- Mobile Device Security Policies: Addressing BYOD security with specific requirements enhances overall security.
- Dedicated Logging and Monitoring Section: The inclusion of retention periods and log review procedures improves detection capabilities.
- Policy Enforcement Statement: Clearly outlining the consequences of non-compliance makes the policy enforceable.
- Specific Edits/Additions: The suggested additions to existing sections are all valuable.

Minor Tweaks and Considerations (Optional):

- Risk Assessment Frequency: While annually is a good start, consider adding language about more frequent assessments if significant changes to the threat landscape or business operations warrant it. -Example: "Risk assessments are conducted at least annually and whenever significant changes are made to our IT infrastructure or business operations, or when a significant new threat is identified."-
- [X] Days for Medium Vulnerability: In the risk assessment examples, replace "[X]" with a specific number of days (e.g., 14 days, 21 days) based on your organization's capabilities.
- Network Monitoring Specifics: In the DLP section, consider clarifying -what- constitutes "unusually large." Define a threshold (e.g., "more than 1 GB transferred outside the network within a 24-hour period"). Also, consider specifying the tools or techniques used for network monitoring (e.g., NetFlow analysis, intrusion detection system).
- Incident Response Tabletop Details: Clarify what is tested in the Tabletop exercises versus live simulation. For example, tabletop exercises can test communication plans, roles and responsibilities, and decision-making processes. The live simulations are to

test the actual reaction to a real incident.

- Patch Management Scope: In the Patch Management section, be specific about -what- is covered (e.g., "operating systems, applications, and firmware on servers, workstations, and network devices").
- Mobile Device Policy Clarity: For BYOD policies, address the legal and privacy implications of remote wipe capabilities. Include a statement like: -"Employees understand that if remote wipe capabilities are utilized, personal data may be affected. The organization will make reasonable efforts to minimize data loss but cannot guarantee complete recovery of personal data."-
- Logging Retention Periods: Be mindful of legal and regulatory requirements for data retention when determining logging retention periods. Also be mindful of storage costs.

Example incorporating some of the suggested tweaks:

2. Risk Assessment

We conduct regular risk assessments to identify, analyze, and evaluate potential threats and vulnerabilities to our information assets. These assessments help us prioritize security measures and allocate resources effectively. Defined specific, measurable thresholds for acceptable risk levels:

- Low: A vulnerability in a non-critical system with no access to PHI and a readily available patch.
- Medium: A vulnerability in a system containing PHI with a difficult exploit path and a patch available within 14 days.
- High: A vulnerability in a critical system containing PHI with an easy exploit path and no immediate patch available. Requires immediate escalation and mitigation. Risk assessments are conducted at least annually and whenever significant changes are made to our IT infrastructure or business operations, or when a significant new threat is identified. This classification is reviewed and updated regularly based on changes in threat landscape, regulatory requirements, and business operations. While acknowledging a low-risk environment is important for resource allocation, it should not lead to complacency. The policy should emphasize the dynamic nature of risk and the need for ongoing monitoring and adaptation.

3. Data Protection

We implement appropriate technical and organizational measures to protect sensitive data from unauthorized access, use, or disclosure. This includes data encryption, access controls, and data loss prevention (DLP) measures. All portable devices used to store or process PHI are encrypted with full disk encryption. Device encryption is verified on a quarterly basis.

- Endpoint DLP Configuration: Specific capabilities are enabled within the endpoint protection software (e.g., monitoring file transfers to USB drives, blocking certain file types in emails).
- Data Classification Awareness: DLP training is included in security awareness training. Employees need to know how to identify and handle sensitive data.
- Network Monitoring: Basic network monitoring is performed for unusually large data

transfers originating from internal systems, specifically monitoring for any transfer exceeding 1 GB outside the network within a 24-hour period, utilizing NetFlow analysis and intrusion detection system.

5. Incident Response

We have an Incident Response Team (IRT) responsible for responding to and managing security incidents. Our incident response plan outlines the steps to be taken in the event of a security breach, including containment, eradication, recovery, and post-incident analysis. The IRT will communicate regularly with relevant stakeholders during and after an incident, including management, legal counsel, and affected users. Incident Response Plan Testing: Tabletop exercises are conducted to test communication plans, roles and responsibilities, and decision-making processes. At least one simulated phishing attack or ransomware scenario is conducted per year to test real reaction times and procedures.

11. Patch Management

We have a patch management process in place to ensure that security patches are applied to our systems in a timely manner. This includes:

- Regularly monitoring for new patches and updates for operating systems, applications, and firmware on servers, workstations, and network devices.
- Testing patches in a non-production environment before deployment.
- Applying patches to all affected systems within a defined timeframe.

Conclusion:

You have created a very strong Cybersecurity Policy that is tailored to your organization's risk profile and incorporates best practices. With the few suggested tweaks, it will be even more effective. The key now is to implement the policy, train your staff, and continuously monitor and update it as needed. Congratulations!