Introduction:

The purpose of this vulnerability management policy is to outline the procedures for identifying, assessing, prioritizing, and remedying vulnerabilities within our organization's information technology infrastructure. The policy applies to all personnel who are involved in the management and operation of our organization's IT systems, including employees, contractors, and third-party vendors.

Objectives:

The objectives of this vulnerability management policy are to:

1. Identify vulnerabilities within our organization's IT systems.
2. Prioritize vulnerabilities based on their severity and potential impact.
3. Remediate vulnerabilities in a timely and efficient manner.
4. Continuously monitor and assess our organization's IT systems for new vulnerabilities.

Policy Statement:

1. Vulnerability Identification:

Our organization will use a combination of automated scanning tools and manual assessments to identify vulnerabilities within our IT systems. These assessments will be performed on a regular basis, and any vulnerabilities discovered will be documented and prioritized based on their severity and potential impact.

1. Vulnerability Prioritization:

Vulnerabilities will be prioritized based on the following criteria:

* Severity: The severity of the vulnerability will be assessed based on industry-standard severity ratings.
* Potential impact: The potential impact of the vulnerability on our organization's operations and assets will be assessed.
* Exploitability: The likelihood of the vulnerability being exploited will be assessed.

Vulnerabilities will be assigned a priority level based on these criteria, and remediation efforts will be prioritized accordingly.

1. Vulnerability Remediation:

Our organization will implement remediation measures to address identified vulnerabilities based on their priority level. Remediation measures may include patching, updating software and hardware, configuration changes, or other mitigation strategies. Our organization will also track and document remediation efforts to ensure that all vulnerabilities are addressed in a timely and efficient manner.

1. Vulnerability Monitoring:

Our organization will continuously monitor our IT systems for new vulnerabilities and emerging threats. We will use a combination of automated scanning tools and manual assessments to identify and prioritize vulnerabilities on an ongoing basis.

1. Reporting:

Our organization will maintain a log of all identified vulnerabilities and remediation efforts. Reports will be provided to senior management on a regular basis to ensure that they are aware of the state of our organization's IT security posture.

1. Responsibility:

All personnel within our organization who are involved in the management and operation of our IT systems are responsible for complying with this vulnerability management policy. The IT department is responsible for implementing and enforcing this policy.

Conclusion:

This vulnerability management policy outlines the procedures for identifying, assessing, prioritizing, and remedying vulnerabilities within our organization's IT systems. By implementing this policy, we will be able to maintain a strong IT security posture and protect our organization's assets from potential threats.