Power

Vulnerability Management Policy

Effective Date: April 16, 2024

This policy has been established to safeguard the information assets of Power Digital Marketing. Its aim is to prevent or minimize security breaches that could result from vulnerabilities within the information systems. It provides a consistent framework for the efficient identification, assessment, and management of security vulnerabilities.

1. Purpose

This policy establishes guidelines and procedures for the proactive identification, assessment, and remediation of security vulnerabilities within our organization's systems, networks, and applications. It aims to strengthen our cybersecurity posture, mitigate the risk of cyber threats, and ensure compliance with regulatory requirements.

2. Scope

This policy applies to all employees, contractors, vendors, and third-party users who have access to the organization's systems, networks, and applications.

3. Policy Statement

It is the policy of Power Digital Marketing to maintain a comprehensive vulnerability management program to identify, assess, prioritize, and remediate security vulnerabilities across all systems, networks, and applications. This policy outlines the principles, procedures, and responsibilities for managing vulnerabilities effectively within the organization.

4. Policy Implementation

4.1. Vulnerability Assessments

Regularly conduct vulnerability assessments to identify potential security weaknesses, misconfigurations, and software flaws within the organization's infrastructure.
Define the frequency and scope of vulnerability assessments based on industry best practices, regulatory requirements, and organizational risk tolerance.

4.2 Penetration Testing

Conduct periodic penetration testing exercises to simulate real-world cyberattacks and assess the effectiveness of existing security controls.
Engage qualified security professionals or ethical hackers to perform penetration testing using a combination of automated tools and manual techniques.

4.3 Vulnerability Remediation

Prioritize identified vulnerabilities based on severity ratings, exploitability, and potential impact on business operations.
Develop and implement a remediation plan to address identified vulnerabilities in a timely manner, considering the criticality and risk exposure of each vulnerability.

4.4 Reporting and Documentation

Prepare comprehensive reports documenting the findings of vulnerability assessments and penetration testing exercises.
Include actionable recommendations for mitigating risks, improving security controls, and strengthening defenses.
Maintain detailed documentation of assessment results, remediation efforts, and validation activities for compliance and audit purposes.

4.5 Continuous Improvement

Establish a process for continuous monitoring, assessment, and improvement of vulnerability management practices.
Incorporate lessons learned from vulnerability assessments and penetration testing exercises to enhance security protocols and procedures.
Stay informed about emerging threats, vulnerabilities, and attack techniques to adapt and evolve the organization's vulnerability management strategy accordingly.

5. Policy Compliance

All employees, contractors, vendors, and third-party users must adhere to this policy to ensure compliance with vulnerability management requirements and maintain the security of organizational assets.

Power

6. Policy Review and Updates

This policy shall be reviewed annually by the IT department and updated as necessary to reflect changes in technology, business practices, or regulatory requirements.

7. Policy Acknowledgment

All personnel involved in vulnerability management activities must acknowledge receipt and understanding of this policy upon initial assignment of responsibilities and periodically thereafter.

8. Document History

Version	Date	Description	Author	Approved by
1.0	16/04/2024	First Version	Security Team	Jamie Schiese

By adhering to this Vulnerability Management Policy, we demonstrate our commitment to proactively identifying and addressing security vulnerabilities, reducing the risk of cyber threats, and maintaining a robust cybersecurity posture within our organization.