Vulnerability Management Program

STEMByte Initiative, Inc.

Prepared by: Terrell Hull
Framework Alignment: NIST CSF, CIS Controls
Tool Reference: Qualys Vulnerability Management
Responsibility Model: Shared IT and Security
Date: _____

Executive Summary

STEMByte Initiative, Inc. relies on cloud-based platforms, BYOD endpoints, and third-party services to deliver STEM and cybersecurity education programs. This operating model introduces exposure to software vulnerabilities, configuration weaknesses, and patching delays that may impact the confidentiality, integrity, and availability of sensitive organizational and student data.

This Vulnerability Management Program establishes a standardized, risk-based approach for identifying, prioritizing, remediating, and reporting vulnerabilities across STEMByte’s technology environment. The program is designed to be scalable, cost-conscious, and appropriate for a growing nonprofit organization while aligning with government-recognized cybersecurity best practices.

By implementing this program, STEMByte reduces the likelihood of exploitation, improves operational resilience, and demonstrates cybersecurity due diligence to partners, grantors, and stakeholders.

1. Program Purpose and Scope

The purpose of this Vulnerability Management Program is to establish a repeatable process for identifying, assessing, prioritizing, remediating, and reporting security vulnerabilities affecting STEMByte systems and data.

In Scope:
• BYOD laptops used by staff (approximately 20 devices)
• Google Workspace services
• Cloud storage and collaboration platforms
• Public-facing website
• Third-party services supporting operations

Out of Scope:
• Student-owned devices
• External partner-managed systems

2. Vulnerability Sources

- Automated vulnerability scans conducted using Qualys
- Configuration and access control reviews
- Patch and update status reviews
- User-reported technical issues
- Vendor and third-party security advisories
- Indicators identified during phishing or account compromise attempts

3. Vulnerability Lifecycle

Stage	Description
Identify	Detect vulnerabilities through scans, reviews, and advisories
Validate	Confirm vulnerability accuracy and relevance
Assess Risk	Evaluate likelihood and impact
Prioritize	Assign risk level and remediation urgency
Remediate	Apply patches or compensating controls
Verify	Confirm successful remediation
Report	Track and communicate vulnerability status

4. Risk Scoring and Prioritization

Vulnerability risk is determined using a likelihood and impact model that accounts for organizational context rather than relying solely on technical severity scores.

Impact Consideration	Description
Student or Minor Data	Exposure of sensitive youth information
Donor or Grant Data	Financial or reputational impact
Public-Facing Systems	Increased exploitability
Credential Compromise	Risk of account takeover

5. Remediation Service Level Agreements

Risk Level	Remediation Timeline
Critical	7 days
High	30 days
Medium	60 days
Low	90 days

Exceptions to remediation timelines require documented risk acceptance and leadership approval.

6. Roles and Responsibilities

Role	Responsibility
Leadership	Risk acceptance and prioritization
IT Support	Patch implementation and configuration changes
Security Function	Oversight, validation, and reporting
Vendors	Third-party vulnerability remediation

7. Reporting and Metrics

- Total open vulnerabilities categorized by risk level
- Vulnerability aging and remediation SLA compliance
- Repeat or recurring vulnerability findings
- Quarterly executive vulnerability risk summary

8. Alignment to NIST Cybersecurity Framework

NIST CSF Function	Program Alignment
Identify	Asset-based vulnerability scoping
Protect	Patch management and configuration hardening
Detect	Vulnerability scans and security advisories
Respond	Remediation workflows and escalation
Recover	Trend analysis and program improvement

9. Program Review and Continuous Improvement

The Vulnerability Management Program is reviewed quarterly to assess effectiveness, address emerging threats, and incorporate lessons learned. Program updates are documented to support continuous cybersecurity maturity improvement.