Enterprise Cybersecurity Risk Assessment

STEMByte Initiative, Inc.

Framework: NIST Cybersecurity Framework (CSF)
Assessment Type: Baseline / Current-State Assessment
Assessor: Terrell Hull
Date: ____________________

1. Organization Overview

Organization Name: STEMByte Initiative, Inc.
Organization Type: Growing nonprofit focused on STEM and cybersecurity education.
Mission: STEMByte Initiative, Inc. provides accessible STEM and cybersecurity education to youth and underserved communities through school-based programs, workshops, and virtual learning experiences.

Scope of Operations:

- Approximately 15 staff members (employees and core leadership)
- Regional operations with both in-person and virtual programming
- Programs delivered through schools, community organizations, and online platforms

Technology Environment:

- Google Workspace (email, Drive, Docs, Sheets)
- Cloud-based storage and collaboration
- Zoom for virtual instruction and meetings
- Public-facing website
- Bring Your Own Device (BYOD) laptops
- Approximately 20 active devices
- One shared account used for operational purposes

Data Sensitivity: STEMByte handles high-risk data, including student personally identifiable information (PII), parent and guardian contact information, staff PII, donor and grant documentation, educational records, photos and videos of minors, and login credentials.

2. Asset Inventory (Summary)

Hardware Assets

Asset Type	Quantity	Notes
Staff Laptops (BYOD)	~20	Mixed personal devices
Mobile Devices	Various	Used for email and MFA

Software & Platforms

System	Purpose
Google Workspace	Email, storage, collaboration
Zoom	Virtual instruction and meetings
Website Platform	Public engagement and outreach
Cloud Storage	Document and data storage

Data Assets

Data Type	Risk Level
Student & Minor Data	High
Donor & Grant Data	High
Staff Records	Medium
Public Content	Low

Executive Summary

STEMByte Initiative, Inc. operates as a growing nonprofit delivering critical STEM and cybersecurity education services to youth and underserved communities. While the organization’s mission is impactful, the current cybersecurity posture reflects early-stage maturity that introduces elevated risk due to the sensitive nature of the data handled, including student information, donor records, and media involving minors.

The assessment identified several high-risk areas, most notably the reliance on trust-based access controls, the use of shared accounts, limited security awareness training, and the absence of a formal incident response capability. These gaps increase the likelihood and potential impact of phishing attacks, unauthorized data access, and delayed response to security incidents.

Despite these risks, STEMByte is well-positioned to significantly improve its security posture through targeted, low-cost governance and procedural improvements. Implementing foundational controls such as multi-factor authentication, role-based access, standardized policies, and an incident response playbook would materially reduce risk without hindering organizational agility.

By aligning security practices with the NIST Cybersecurity Framework, STEMByte can responsibly scale operations, strengthen stakeholder trust, and demonstrate cybersecurity readiness to partners, grantors, and the communities it serves.