SECTION: 1.0 GENERAL

SUBJECT: CYBER VULNERABILITY MANAGEMENT

Title: Vulnerability Management Policy

Background: To ensure compliance with new Gramm-Leach-Bliley Act (GLBA) requirements effective June 9, 2023, and to align with recommendations from Lewis-Clark State College (LC State) financial auditor; this policy focuses solely on vulnerability management. A separate change management policy will focus on change management.

Point of Contact: Director of Information Technology

Other LC State offices directly involved with the implementation of this policy, or significantly affected by the policy: IT Executive Steering Committee, Office of the President, Office of the Provost, and Office of the Vice President for Finance and Administration

Date of approval by LC State authority: April 12, 2024

Date of State Board Approval: N/A

Date of Most Recent Review: April 12, 2024

Summary of Major Changes Incorporated in this revision to the policy:

- Updated policy name, previously "Patch Management Policy"
- Defined the philosophy of the policy
- Added formal definitions
- Updated policy to reflect current industry standards for deadlines of remediation
- Detail routine practices that augment and assist with vulnerability mitigation
- Added reference to GLBA compliance
- Updated to conform to current LC State policy format

1. Philosophy

A. Risk and Vulnerabilities

Known vulnerabilities present a clear risk to the confidentiality, integrity, and availability to college data, information systems, and all things that comprise college operations. That risk must be identified, communicated, and managed to the level acceptable to the college.

B. Management of Risk and Vulnerabilities

This policy defines the authorization, requirements, and responsibilities for managing the patches and updates to mitigate known information security vulnerabilities according to risk levels and associated remediation timeframes.

2. Definitions

A. Mitigate: To minimize the possibility and impact of exploitation of a vulnerability that cannot be fully eliminated.

B. Patch Management: Process of identifying, deploying, installing, and verifying the successful patching of vendor-provided updates and security enhancements.

C. Remediate: Eliminate the threats or vulnerability.

D. Risk Rating: A single value that can be qualitative or quantitative that indicates a combination of both the likelihood and impact of the exploitation of a given vulnerability. The higher the risk rating of a vulnerability, the more aggressive the timeframe must be to remediate or mitigate the vulnerability.

E. Vulnerability: Refers to any weakness in a system or process that exposes information to a threat.

F. Vulnerability Management: Refers to the process of identifying, analyzing, and managing system and equipment vulnerabilities.

G. Vulnerability Scanning: Refers to the process used to identify vulnerabilities present in existing systems and equipment.

3. Defined Processes

A. This policy requires the following process be followed to ensure the college identifies vulnerabilities and installs all necessary patches and updates. Create and maintain an established and current inventory of the college's IT systems.

i. Monitor professional cybersecurity information resources, including REN-ISAC and CISA, to identify any vulnerabilities potentially affecting the college and all known remediations.

ii. Conduct weekly external (Cyber Assessments - Cyber Hygiene Scans from the Cybersecurity and Infrastructure Security Agency, CISA) and internal vulnerability scans (Tenable.sc) on all college systems, servers, and desktops.

iii. Enable the approved Endpoint Detection and Response (EDR) system and ensure it is properly installed and functioning on all college computers and servers, with the EDR system receiving automatic updates at least daily.

iv. Ensure the EDR system does a full system scan at least once per day on all servers and at least once per week for all desktop and mobile computers.

v. Prioritize vulnerability remediation based on threat and potential impact.

vi. Mitigate vulnerabilities in a timely manner, defined as issues assigned with a VPR score of:

a) **Critical** risk rating should be investigated within five (5) business days and mitigated or remediated as soon as possible, with a goal of at least mitigation status within ten (10) business days;

b) **High** risk rating should be investigated within ten (10) business days and mitigated or remediated as soon as possible, with a goal of at least mitigation status within twenty (20) business days;

c) **Medium** risk rating should be evaluated within thirty (30) business days;

1) If that evaluation shows that the vulnerability does not directly affect college systems or services, the vulnerability should be noted and tracked to ensure the risk does not change.

2) If the vulnerability may or does affect college systems or services and a mitigation or remediation is identified, the vulnerability should be remediated as soon as practical, with a goal of at least mitigation status within forty-five (45) business days; and

d) **Low** risk rating should be investigated as time permits and mitigated or remediated when possible.

B. Remediation actions should be documented and verified through a review of the next scan results.

4. Authority

A. Idaho Technology Authority (ITA) is authorized by Idaho statute, Title 67, Chapter 57.1

i. ITA's directives are relevant to LC State because of the definition included in the statute. Description of ITA

ii. List of ITA policies

B. Questions, requests for assistance or other issues regarding this policy should be directed to Director of Information Technology.

C. Relevant websites include:
   i. Description of ITA: (https://its.idaho.gov/ita/the-ita/
   ii. List of ITA policies: (https://its.idaho.gov/ita/resources/)