Vulnerability & Patch Management Policy

Grambling State University Information Technology

Jay Ellis, Chief Information Officer

Revision History

Version Number	Revision Date
1.0	

PURPOSE

Information system vulnerability assessment scans provide a mechanism to determine where Grambling State University information systems and devices could be exploited and/or threatened. Grambling State University IT Department maintains a recurring vulnerability scan of IT assets that provides insight into maintaining a secure and functional IT infrastructure. Due to new vulnerabilities being available on a regular basis, this will be a constant process to keep up with industry standards. Patch Management, or the process of distributing and applying updates to software, allows Grambling State University to fix flaws, bugs, vulnerabilities in our systems environment. Together, Vulnerability scans and Patch Management work together to help proactively protect our networks and systems from active or known threats and exploits.

POLICY

The Grambling State University Vulnerability and Patch Management Policy provides clear direction on the efforts, steps and processes involved with the continual identification and remediation of risks associated with discovered and unknown vulnerabilities. Grambling State University adheres to a regularly scheduled patch management procedure in order to effectively apply software updates, patches and fixes in a timely manner.

STANDARDS

1. Periodic external and internal vulnerability scans are to be performed to identify potential risks to Grambling State University information systems and assets.
2. The vulnerability scans will cover all internal and external assigned IP addresses.

3. All vulnerabilities identified during the scans will be reviewed upon receipt of scan report.
4. All vulnerabilities identified will be addressed according to the severity and asset risk level to ensure the integrity of the Grambling State University’s IT systems.
5. All scan results and remediation of vulnerabilities will be documented.
6. External sourced penetration testing is to occur annually or as appropriate to ensure compliance with relevant laws and regulations.

PROCEDURES

1. Vulnerability Scans are performed on a single asset, subnet or asset group
2. Scan results produce:
   a. Reports
   b. List of vulnerabilities with exploits
3. Information Security Action Items
   a. Generate Reports
   b. Validate exploits to test for false positives
4. Report is Generated & Reviewed
5. Remediation action items:
   a. Patch/Fix vulnerability
   b. Request Exclusion for any vulnerabilities if false positive or accepted risk.
6. Information Security action items:
   a. Audit Patch/Fix by running another vulnerability scan on those assets
      i. If not fixed, investigate for remediation
   b. Close tickets on accepted risks

Prioritization of Remediation

Remediation efforts will be prioritized depending upon the severity, criticality and/or frequency of discovered vulnerabilities.

Patching Cadence for routine updates & releases:

Server patching is done monthly on a phased approach to allow for testing prior to release.
End Points have patches pushed out and they are applied during first reboot.

Critical Patches and discovered vulnerabilities:

A separate plan is created based on criticality and perform the remediation asap.