INFORMATION SECURITY STANDARD

Level 3 High Severity – High Risk

Patch must be applied within fourteen (14) days
A vulnerability with a high risk, high severity, and potentially high impact or risk to NAU IT Resources
Emergency Change request may be necessary
Issued by vendor with an associated risk rating, or CVE ratings 7.0-8.9

Level 4 Critical Severity – Very High Risk

Patch must be applied as soon as possible but not to exceed seven (7) days
A vulnerability with a high risk, high severity, and likelihood of immediate impact or risk to NAU IT Resources
An Emergency Change request may be necessary
Issued by vendor with an associated risk rating, or CVE ratings 9.0-10

2. Change Management and Approval

7.2. Endpoints. The use of centralized desktop management tools such as System Center Configuration Manager (SCCM), Microsoft Defender for Endpoint, and JAMF may be used to report on patch and update levels for operating systems and applications.

8. Exception Requests. In the event patches and updates cannot follow the stated schedule, an exception request must be made that details why postponement or deferral is needed. The CIO or authorized designee will grant patch-postponement request approvals that will be submitted through the system designated by the CIO (e.g., ServiceNow, OnBase).

Reasons for exception requests may include:

Production system freeze or change blackout periods
Conflicts with other critical changes scheduled during the same period
Tested patches break functionality in non-production environment
End of life products that must remain in place (a