CHRISTOPHER NEWPORT
UNIVERSITY

Systems and Software Patching Standard

VERSION 1.3

June 2023
Department: Information Security

Proprietary Statement

Review and Revision History

Date	Version	Description of Change (Affected Sections)	Author
August 2019	1.0	Initial Release - All	Wendy L. Murray
August 2020	1.0	Annual Review	Wendy Corrice
August 2021	1.1	Annual Review	Wendy Corrice
June 2022	1.2	Annual Review	Wendy Corrice
June 2023	1.3	Annual Review	Wendy Wilde

TABLE OF CONTENTS

Introduction

Regular application of vendor-issued critical security updates and patches are necessary to protect University data and systems from malicious attacks and erroneous function. Sensitive devices connected to the network routinely require patching for functional and secure operations.

Purpose

Software is critical to the delivery of services to Christopher Newport's users. This standard provides the basis for an ongoing and consistent system and application update policy that stresses regular security updates and patches to operating systems, firmware, productivity applications, and utilities. Regular updates are critical to maintaining a secure operational environment and comply with SEC501 SI-2 Flaw Remediation Standard.

Scope

This standard applies to systems designated as Sensitive according to Christopher Newport's Data Classification Standard and/or any other systems designated by the Information Security Officer.

Standards Statement

GENERAL

All system components and software shall be protected from known vulnerabilities by installing applicable vendor-supplied security patches. System components and devices attached to the University network shall be regularly maintained by applying critical security patches within ninety (90) days after release by the vendor. Other patches not designated as critical by the vendor shall be applied on a normal maintenance schedule as defined by normal systems maintenance and support operating procedures.

SYSTEM, UTILITY AND APPLICATION PATCHING

A regular schedule shall be developed for security patching of Sensitive University systems and devices. Patching shall include updates to all operating systems as well as application software, database software, third-party applications.

Most vendors have automated patching procedures for their individual applications. There are a number of third-party tools to assist in the patching process and Christopher Newport should

make use of appropriate management software to support this process. The regular application of critical security patches is reviewed as part of normal change management and audit procedures.

PATCHING EXCEPTIONS

Patches on production systems (e.g. servers and enterprise applications) may require complex testing and installation procedures. In certain cases, risk mitigation rather than patching may be preferable. The risk mitigation alternative selected should be determined through an outage risk to exposure comparison. The reason for any departure from the above standard and alternative protection measures taken shall be documented in writing. Deviations from normal patch schedules shall require Information Security Officer authorization.

SECURITY PATCHING PROCEDURES

Procedures shall be established and implemented for vulnerability and patch management. The process shall ensure that application, system, and network device vulnerabilities are:

- Evaluated regularly and responded to in a timely fashion
- Documented and well understood by support staff
- Automated and monitored wherever possible
- Executed in a manner applicable vendor-supplied tools on a regularly communicated schedule
- Applied in a timely and orderly manner based on criticality and applicability of patches and enhancements

AUDIT CONTROLS AND MANAGEMENT

Documented procedures and evidence of practice should be in place for this operational policy as part of the University's internal systems change management and update procedures. Examples of adequate controls include:

- Documented in change management per Christopher Newport's Change Management Policy
- System updates and patch logs when possible
- Update baseline system documentation
- Testing documentation post patch

Review

Next Review Date: June 2024