UNIVERSITY OF CENTRAL FLORIDA

University Standards

Subject:	Patch Management Standards
Standards Number:	105
Effective Date:	8/27/2019
Revised Date:	
Responsible Authority:	Information Security Office
Pages:	4

ACCOUNTABILITY/APPLICABILITY:

The acceptable patching procedures outlined in this document apply to all systems and applications that connect to the University network via physical, wireless, or VPN connections in order to ensure a secure computing environment. Each department is responsible for the patch management of the devices and systems under their control.

STANDARDS STATEMENT:

The purpose of this document is to establish the minimum acceptable patch management procedures, and requirements to be applied in order to ensure the appropriate protection of UCF's information systems from unauthorized access and misuse. In order to maintain the integrity of UCF's network systems and university data, all systems must follow the minimum standards listed below.

Any exception to the standards must be documented and approved by the Information Security Office in advance.

BACKGROUND:

The time between vulnerability discovery and exploit availability is critical, making security patches ever important. To ensure that the University of Central Florida can protect the confidential data in its possession, frequent security patches for applications and systems is vital. The maintenance of the university's secure computing environment, as security patches/configurations function as an embedded solution or mitigation to a vulnerability.

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476

STANDARDS:

1. Security updates must be deployed within **30 days** of their release. This includes the time it takes to test the patches.
    a) Enable systems or applications to automatically update wherever possible.
    b) End user devices may require a reboot to apply updates. End users should be given a period of time to manually apply the patches at a convenient time that does not disrupt work. If end users did not opt to install the updates during this manual installation period, they should expect a forced reboot at some point in the patch cycle to ensure all security patches are deployed within the window defined in standard 1 above. It is recommended that end users manually apply patches or plan for a forced reboot of their device.
2. If a patch addresses a critical vulnerability that poses significant risk to the organization, the UCF Information Security Office will notify Department Security Coordinators and IT staff to install the patch immediately.
3. Updates must be tested before deployed in production environments
    a) Updates should be tested in an environment that accurately reflects the application's production environment.
    b) System and application owners should be made aware when patches are being deployed for testing and production.
4. System owners that manually manage patches on their systems or cannot adhere to the defined patch cycle will be required to implement compensating controls and provide a remediation plan to the Information Security Office.

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476

DEFINITIONS:

Information Security Office (ISO): The mission of the Information Security Office is to provide a secure infrastructure that protects the confidentiality, integrity, and availability of information resources. To this end, the ISO develops security best practices, coordinates security issues, conducts investigations, and works with Information Technology (IT) and other campus departments to minimize security risks and assure compliance with security policies and procedures.

Compensating Controls. Security measures that successfully mitigate the risk associated with a security requirement that cannot be met (typically due to technical or documented business constraints)

Department Security Coordinator (DSC). A designated information security representative for a UCF department.

Patch Cycle. The expected turnover timeline for the administration of security updates for applications or operating systems.

Remediation Plan. A plan to address a documented security vulnerability, flaw, or issue.

System Center Configuration Manager (SCCM). A third-party tool developed by Microsoft that offers some type of functionality. We may not need to define this because we don't explicitly reference it within the document- it is a third-party tool.

RELATED DOCUMENTS:

1. 2.100.1 Florida Public Records Act—Scope and Compliance policy
    a. https://policies.ucf.edu
2. 4-008.1 Data Classification and Protection policy
    a. https://policies.ucf.edu/
3. CIS System Benchmarks
    a. http://benchmarks.cisecurity.org/
4. NIST Cybersecurity Standards
    a. https://csrc.nist.gov/publications/sp800

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

CONTACTS:

Information Security Office https://infosec.ucf.edu infosec@ucf.edu	Security Incident Response Team (SIRT) https://infosec.ucf.edu/incident-response/ sirt@ucf.edu
Identity Access Management (IAM) https://infosec.ucf.edu/iam iam@ucf.edu	UCF IT Support Center (407) 823-5117 https://ucf.service-now.com/ucfit itsupport@ucf.edu

INITIATING OFFICE: Information Security Office

STANDARDS APPROVAL
(For use by the Information Security Office)

Standards Number: *105*

Initiating Office: Information Security Office

Chief Information Security Officer: *Chris Vakhordjian*

Signature: chrisv Digitally signed by chrisv Date: 2019.08.28 08:47:45 -04'00' Date: _____

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution