**Contents**

[1. Scope 3](#_Toc113274095)

[2. Responsibilities 3](#_Toc113274096)

[3. Software Updates and Patching 3](#_Toc113274097)

[4. Types of Patches 4](#_Toc113274098)

[5. Patch Management Checklist 4](#_Toc113274099)

[6. Penetration Testing 4](#_Toc113274100)

[7. Process Flowchart 5](#_Toc113274101)

[8. Procedures 5](#_Toc113274102)

[9. Evaluation of Patch Criticality 6](#_Toc113274103)

[9. Pre-Deployment Testing 7](#_Toc113274104)

[10. Deployment Schedule 7](#_Toc113274105)

**DOCUMENT REVISION CONTROL**

REVISION HISTORY

| **Date** | **Author** | **Version** | **Change Reference** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

REVIEWERS

| **Name** | **Position** | **Date** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

DISTRIBUTION

| **Date** | **Distributed to** | **Version** | **Distribution Format** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

APPROVALS

| **Date** | **Approved by** | **Version** | **Designation** | **Approval remarks** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

# Scope

This policy applies to all the Company's information systems and resources, whether they are owned or operated by the university or on its behalf. This policy must be followed by all Company-Related Persons who have access to company information or computers and systems that are managed or maintained on behalf of the organization.

# Responsibilities

* Chief Information Officer- Examine and accept any modifications to the patch management procedure.
* Information security Analyst- Alert the technical staff on campus when new patches are available. Organize with the campus the review of new patches.
* At the campus Change Management meetings, talk about patch releases.
* Upkeep of the vulnerability scanning tool; regular scanning of crucial systems for known flaws
* With the campus patch testing team and the patch server administrator, organize a review of new patches.
* Network engineer- Install patches and check the hardware setups of network devices.
* Application developer- Confirm that current patch levels are met; create and install updates; detect known and prospective vulnerabilities.
* Desktop Administrator- Install fixes, create and analyze patch reports at least once a month, and fix known vulnerabilities on systems that cannot be patched.
* Server Administrator- Install fixes, create and analyze patch reports at least once a month, and fix known vulnerabilities on systems that cannot be patched.
* Change Management Review- Before deployment, centrally deployed patches must be reviewed and approved.

# Software Updates and Patching

* All IT systems, whether owned by the company or developed and maintained by third parties, must be appropriately licensed, supported by the manufacturer, and run up-to-date and patched operating systems and application software.
* Before IT systems can be admitted into operational service, third-party vendors must be able to show proof of current patching.
* All patches must be thoroughly checked before being fully implemented, as changes may cause unexpected problems.
* Systems that have been disconnected from the network due to a lack of patching will only be restored once it can be proved that they have been patched and are no longer a threat to the Company's network.

# Types of Patches

|  |  |
| --- | --- |
| **Types** | **Patch** |
| Server | BIOS, firmware |
| Operating System | Service packs, patches, feature packs |
| Router and Switches | Firmware |
| Scanners | Driver, firmware |

# Patch Management Checklist

|  |  |  |  |
| --- | --- | --- | --- |
| **Server Name** | **Remediation Plan** | **Patching status** | **Operating system** |
| Win2k12r | None | In process | Windows 10 |
| Apexure | None | Completed | Windows 10 |
| Aristo media | None | Not started | Windows 10 |
| Fusion host | None | Pending | Windows 10 |

# Penetration Testing

* Penetration testing of the internal network, external network, and hosted applications should be done at least once a year or if the environment changes significantly.
* Any exploitable vulnerabilities discovered during a penetration test will be fixed and retested to ensure they were fixed.

# Process Flowchart

Yes

No

**Withdraw patch and re-evaluate**

**Submit via change management**

**Identify Patches, affected systems and evaluate criticality**

**Degradation or security impact**

**Submit via change management**

**Inform business owner for each affected system**

**Evaluate security impact of each patch**

# Procedures

1. Patching and updating are required for all digital assets, systems, and services to protect against security flaws.
2. Operating systems, applications, database systems, software components, etc. are all included in the patching scope.
3. All information systems must be kept up to date with the quickest and most frequent patches possible.
4. Considered a general patch management technique, this policy shall automatically apply to all information systems, digital assets, and services. Following a specialized patch management approach created by the Data Custodian and approved by Information Security, Information Systems with special needs may be maintained.
5. Before being implemented, patches must be verified to work with all system components.
6. Unless specifically stated in a unique patch management policy that has been approved, patches must be successfully tested on non-production systems before being installed on production systems.
7. Before being applied to live systems, all patches must receive the proper change control permission.
8. Unless there is an emergency, patching must be done during an allowed maintenance window.
9. Before applying new patches, important system data must be backed up.
10. In most circumstances, 45 days is the longest amount of time that AUC systems/services can go without a patch. Information Security will decide whether to reduce this tolerance time based on the seriousness of the vulnerability to reduce risk to assets.

# Evaluation of Patch Criticality

Patches vary in terms of their critical levels. Some patched fix vulnerabilities that are difficult to exploit, while others protect against viruses that spread rapidly. Based on our evaluation, we will then determine whether to deploy the patch immediately, schedule it for deployment at a later date, or take no action.

* How will the patch affect the system (e.g., understanding what services and/or ports will be disabled, and what other changes may occur)?
* What is the business impact of deploying the patch?
* What is the risk to the business if the patch is delayed?
* What is the approximate size of the patch?

|  |  |
| --- | --- |
| **Patch Criteria** | **Criticality** |
| The security of each individual system as well as the overall security of <Company Name> must be immediately patched.   * Affected systems or applications are crucial to corporate operations, and * Exploitation is conceivable or probable, * There is no workaround, and * Exploitation might expose further <Company Name> to risk, and * An exploit may jeopardize <Company Name> members' personal information. * Is vulnerable when no other perimeter defenses are in place | Critical |
| To ensure the security of each system individually and the overall security of Company Name>, urgent patching is required.   * Affected systems or applications are crucial to corporate operations, and * Exploitation is conceivable or probable, and * There is no workaround, and * Exploit may affect additional instances of [Company Name]. | Important |

# 9. Pre-Deployment Testing

In order to test patches as closely as possible to the production environment, <Company Name> will use a non-production environment.

Usability, security, and implications on other systems are all tested for. The test findings will subsequently be recorded, included in the change control request, and communicated to the business owners.

If a patch is determined to be flawed or the updated code is discovered to conflict with other software, <Company Name> will resolve the conflict as quickly as possible to reduce the likelihood that the affected system or application will be exposed to a threat that the patch is designed to counter.

# 10. Deployment Schedule

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Purpose** | **Critical** | **Important** | **Moderate** | **Low** |
| Updates that could cause a network interruption | Less than 24 hours | Less than 3 days | Less than 2 weeks | The patch will be scheduled in the next maintenance cycle |
| For services that can be patched during business hours without suffering major interruptions. | Less than 3 days | Less than 1 week | The patch will be scheduled in the next maintenance cycle | The patch will be scheduled in the next maintenance cycle |
| Service maintenance for systems and devices | Less than 1 week | The patch will be scheduled in the next maintenance cycle | The patch will be scheduled in the next maintenance cycle | The patch will be scheduled in the next maintenance cycle |