
 جامعة الإمارات العربية المتحدة United Arab Emirates University 	Information Technology Policies Manual		Policy Number	IT-14
			Effective Date	12-Aug-2018
	Subject		Most Recent Review Date	15-Apr-2018
	Patch Management and System Updates		Due Date for Next Review	01-Sep-2021
	<i>Responsible Office:</i> Chief Information Officer		Page Number	1 of 2

14. Patch Management and System Updates

Overview

This policy will review, evaluate, and appropriately apply software patches in a timely manner. If patches cannot be applied in a timely manner due to hardware or software constraints, mitigating controls will be implemented based upon the results of a risk assessment.

Scope



1. Applies to all Information Technology staff.
2. These rules cover all servers, workstations, network devices, operating systems (OS), applications, and other information assets for which vendors provide system patches or security updates.

Objective

The objective of this policy is to have streamlined software and patch update process for all systems hosted by UAEU.

Policy

1. In order to ensure the security of the network and protect the UAEU data, all computers network devices and applications must be maintained at vendor supported levels and critical security patches must be applied.
2. System administrators will use automated tools, where available, to create a detailed list of all currently installed software on workstations, servers and other networked devices. A manual audit will be conducted on any system or device for which an automated tool is not available.
3. Systems and software will be evaluated to verify currency of patch and update levels and an analysis of vulnerabilities will be performed.
4. Automated tools will scan for available patches and patch levels, which will be reviewed.
5. Manual scans and reviews will be conducted on systems for which automated tools are not available.
6. An informal risk assessment will be performed within 2 business days of the receipt of notification of patches.
7. Vendor supplied patch documentation will be reviewed in order to assure compatibility with all system components prior to being applied.
8. Where possible, patches will be successfully tested on non-production systems installed with the majority of critical applications/services prior to being loaded on production systems.
9. Successful backups of mission critical systems will be verified prior to installation of patches and a mechanism for returning to the patch levels in effect prior to patching.

 جامعة الإمارات العربية المتحدة United Arab Emirates University 	Information Technology Policies Manual		Policy Number	IT-14
			Effective Date	12-Aug-2018
	Subject		Most Recent Review Date	15-Apr-2018
	Patch Management and System Updates		Due Date for Next Review	01-Sep-2021
	<i>Responsible Office:</i> Chief Information Officer		Page Number	2 of 2

10. Patches will be applied during an authorized maintenance window in cases where the patch application will cause a service interruption for mission critical systems.
11. Patches will be prioritized and applied in accordance with criticality level.
12. Logs will be maintained for all system categories (servers, desktops, switches, etc.) indicating which devices have been patched. System logs help record the status of systems and provide continuity among administrators. Information to be recorded will include but is not limited to: date of action, administrator's name, patches and patch numbers that were installed, problems encountered, and system administrator's remarks.
13. In the event that a system must be recovered, all relevant data on the current OS and patch level will be recorded. The system should be brought back to the patch levels in effect before reloading.