Patch Management Procedure

Section 1 - Scope

(1) The Patch Management Procedure guides the process of assessing announced vulnerabilities as well as available patches to determine the risk they pose to ACU and the associated methods for patch deployment.

(2) Patch management relies on current maintenance agreements so that patches can be made available for all ACU equipment and software. If the software or hardware is no longer supported, this poses a risk to ACU. Outdated software and hardware need to be replaced or upgraded to remain currently supported and receive regular patches.

(3) Please note that SaaS (Software as a Service) is out of scope as ACU has no control over the patching cycle. For example, SharePoint Online is a SaaS product, but SharePoint 2010 is not. SharePoint 2010 is an application that is on-premises. ACU manages the SharePoint servers and is responsible for patching the application.

Communication channels

(4) At the time of this Procedure is written, there is no University-wide approved Change Control Procedure. Information Technology (IT) has an internal change control procedure. For this reason, the Technical System Owners will liaise with the appropriate Application System Owners for change management (including raising appropriate change request) and required application testing.

Section 2 - Definitions

Term	Definition
Application System Owners	are business system owners that are responsible for the applications or systems. Business system owners are typically senior business operational Managers within ACU with responsibility for business processes and data / content that are supported by the business system.
Applicable Support Team	could be teams from Information Technology (IT) or Support Team from Library, People and Capability, Research and Enterprise etc. where the department manages its own system / application without entirely relying on IT.
Patch Management	is the process of distributing and applying updates to the software. Patches mitigate security vulnerabilities and may also add new functionality or correct issues with existing functionality within applications and system software.
Technical System Owner	is accountable for technical implementation and support, in collaboration with their Business Owner and acts as a Subject Matter Expert. Technical System Owner is responsible for checking (per the patching schedule timeframe) if any outstanding patches must be deployed. Technical System Owner may be a staff employed by ACU or an external vendor.

Section 3 - Monitoring for Patches and Security Vulnerabilities

(5) All patches released by vendors should be reviewed before adoption within the ACU environment. Deployment of these patches should be in line with the schedules outlined in this document. As such, the technical and system /

application owners should ensure that their respective teams subscribe to relevant vendor patch announcements.

(6) The vulnerability and patch information published by the vendor will typically include:

a. a list of products and versions affected;
b. technical details of the vulnerability including an overview of how exploitation occurs;
c. typical consequences of exploitation, such as remote code execution, information disclosure, denial of service;
d. current exploitation status: whether the vulnerability is actively exploited;
e. the existence and details of any temporary workarounds; and
f. an overall measure of severity based on the above factors.

(7) Each vendor uses different means of communicating the severity of a vulnerability. The severity may be derived from a standard such as the Common Vulnerability Scoring System (CVSS) or based on vendor-defined categorisation such as 'Critical' or 'Important'.

(8) In addition to individual vulnerability / patch details, some vendors publish a consolidated bulletin which also contains the vendor's recommended deployment order.

#	Task	Responsibility
1	Monitor for vulnerabilities for systems in the team's area of responsibility.	· IT Enterprise Information Security · Applicable Support team*

* 'Applicable support team' could be teams from IT or support teams from the Library, People and Capability, Research and Enterprise etc. where the department manages its own system / application without entirely relying on IT.

Section 4 - Vulnerability Patch Risk Assessment

(9) A risk assessment allows ACU to properly assess the severity of a vulnerability / patch in the context of our environment. Technical and system / application owners are encouraged to reach out to the IT Enterprise Information Security Team if unsure how to conduct this risk assessment. IT Enterprise Information Security will analyse the relevant vulnerability / patch information to form the risk assessment.

(10) It is essential to consider the following factors when conducting risk assessment:

a. high value or high exposure assets. (Internet-facing systems fall into this category);
b. assets historically attacked in the past;
c. mitigating controls already in place, or soon to be in place for all affected assets; and
d. low risk of exposure for impacted assets.

(11) When assessing the risk, refer to Section 13 – Appendix 1: Patch Classification table below, and classify the patch as a critical, high, medium or low priority using the CVSS score, or the criticality description as appropriate. The patch rating may be impacted by the factors listed above; for example, a critical patch may be downgraded to high if proper mitigating controls are in place or will be put into place.

(12) Determine whether the impacted software is used within ACU and identify the business service(s) that rely on the software to operate. Using the Service Criticality table (Section 14 – Appendix 2 below), determine the criticality of the business service.

(13) As with all assessments, the IT Enterprise Information Security Team have an over-riding veto on all patch management decisions and through their assessment of the vulnerability, patches, and systems can determine that a course of action is not derived by the processes contained within this document is more appropriate.

(14) Using the Patch Deployment Decision Matrix, cross-reference the identified patch criticality and service criticality to determine the patch implementation time frame. The more critical the service is to ACU, and the more critical or severe the security weakness that may be exploited, the quicker the patch or appropriate compensating controls should be deployed.

#	Task	Responsibility
2	Identify the vulnerable business services and assess the risk to determine if a patch should be deployed or not and if so, how quickly and when the patch should be deployed.	· IT Enterprise Information Security Team · Applicable Support team

Section 5 - Temporary Mitigations

(15) Temporary mitigations should only be used when there is no vendor supported patch available, or it is impractical to apply due to valid business reasons. These mitigations may be published in conjunction with, or soon after, the vulnerability announcement.

(16) Temporary mitigations may include disabling the vulnerable functionality within the software or device or restricting or blocking access to the vulnerable service using firewalls or other access controls.

(17) The decision on whether temporary mitigation is implemented should be risk-based. The length of time it will take to implement the patch will guide how long the temporary workaround should be in place as well as the amount of time and effort expended in designing and implementing the workaround.

#	Task	Responsibility
3	Determine response until a patch can be deployed.	IT Enterprise Information Security Team, and applicable Support team.
4	Implement response until the patch is deployed.	IT Enterprise Information Security Team, and applicable Support team.

Section 6 - Patch Testing and Implementation

(18) Many vendors, including Microsoft, perform thorough testing of all patches before their release to the public. This testing is performed against a wide range of environments, applications, and conditions. ACU must gain assurance that the patch will not negatively impact the production environment. Thorough testing should be performed of all patches before they are implemented.

(19) Patches, where practical, shall be tested on a set of non-critical pilot systems. For systems that do not have a non-production environment to test patches (e.g. Firewall or other limited hardware equipment), ACU must seek assurance from the software or hardware vendor that patches will not adversely affect the production environment, with rollback options (if available).

(20) Patches will ordinarily be deployed according to the patching cycle for the software being patched (unless the risk assessment concludes that the patch must be rolled out quicker due to the risk). For patches that need to be deployed outside of patching cycle, technical system owners must get approval from the application system owner.

#	Task	Responsibility
5	Test patch for defects or adverse effects	Applicable Support teams
6	For defective patches, determine a course of action	Applicable Support teams
7	Plan patch deployment, identify patch dependencies, like reboots and determine deployment date and time	Applicable Support teams
8	Deploy patch	Applicable Support teams
9	Confirm patch deployment	Applicable Support teams
10	Post verification testing	IT Enterprise Information Security Team, and applicable Support team

Section 7 - Patch Rollback

(21) Sometimes, even after testing, patches once deployed in the production environment can introduce unintended consequences. It is essential to ensure that all patch implementations have a defined and tested rollback mechanism and plan. Where a patch cannot be rolled back, the patch should be tested on a test or dev system first in conjunction with vendor support.

#	Task	Responsibility
11	Approve patch rollback	Applicable Support teams
12	Patch rollback	Applicable Support teams
13	Confirm patch uninstallation	Applicable Support teams
14	Post verification testing	Applicable Support teams

Section 8 - Patch Compliance Reporting

(22) Monthly patch compliance reports will be performed by the IT Enterprise Information Security Team and reported to the IT Senior Leadership Team every month. The desired outcome of regular reporting is to identify issues with people, processes, and technology, resulting in undue risk to the ACU environment. Issues identified through compliance reporting will be discussed during a monthly presentation with actions / resources and prioritisation being given to responsible teams to help improve.

(23) Compliance thresholds will be agreed individually between the IT Enterprise Information Security Team and responsible support team and can be altered as required.

#	Task	Responsibility
15	Patch Compliance Reporting	IT Enterprise Information Security Team

Section 9 - Patch Management Responsibilities

#	Task	Responsibility
1	Monitor for vulnerabilities for systems in the team’s area of responsibility	· IT Enterprise Information Security Team · Applicable Support team
2	Identify the vulnerable business services, assess the risk to determine how quickly and when the patch should be deployed	· IT Enterprise Information Security Team · Applicable Support team

#	Task	Responsibility
3	Determine response until a patch can be deployed	· IT Enterprise Information Security Team · Applicable Support team
4	Implement response until the patch is deployed	· IT Enterprise Information Security Team · Applicable Support team
5	Test patch for defects or adverse effects	Applicable Support teams
6	For defective patches, determine a course of action	Applicable Support teams
7	Plan patch deployment, identify patch dependencies, like reboots and determine deployment data and time	Applicable Support teams
8	Deploy patch	Applicable Support teams
9	Confirm patch deployment	Applicable Support teams
10	Post verification testing	· IT Enterprise Information Security Team · Applicable Support team
11	Approve patch rollback	Applicable Support teams
12	Patch rollback	Applicable Support teams
13	Confirm patch uninstallation	Applicable Support teams
14	Post verification testing	Applicable Support teams
15	Patch Compliance Reporting	IT Enterprise Information Security Team

Section 10 - Technical and Application System Owners

(24) Whilst the IT Enterprise Information Security Team will monitor for security vulnerabilities in ACU systems, the Technical System Owner is responsible for checking (per the patching schedule timeframe) if any outstanding patches must be deployed. At a minimum, this check must be performed at least annually.

(25) The Technical System Owners will liaise with the Application System Owners for change management (including raising appropriate change request) and required application testing.

System / Application	Owner
Desktop / Notebooks	IT Service Delivery Team
Servers (Linux, Windows)	Digital Platform Services Team
SAN/NAS	IT Partner (Parallo team)
VMware Infrastructure	IT Partner (Parallo team)
Networking devices (including Firewall, CISCO)	Digital Platform Services Team
Unified Comms / AV	IT Service Delivery Team / Digital Platform Services Team
IT Banner	IT Application Support
Ellucian	IT Application Support
Web server	Digital Platform Services Team
WordPress	IT Application Support
Bespoke web applications	IT Application Support

System / Application	Owner
Sophos Endpoint protection	IT Service Delivery Team
Aurion	Supported by Vendor & People and Capability
Tech One	Supported by Vendor & Finance and Planning
Active Directory	Digital Platform Services Team

Section 11 - Patching Cycle

Desktop and Notebooks

(26) Patching system(s):

a. Windows SCCM;
b. Jamf Pro.

(27) Support Team:

a. IT Service Delivery; and
b. Digital Platform Services Team.

(28) The standard patching cycle for desktops and notebook computers is monthly and begins on Microsoft Patch Tuesday (which is on Wednesday for Australia) when Microsoft patches are released. Note that the patching cycle includes all the components listed below, except as noted. This means that all patches that are available at Patch Tuesday for the components listed below will be included in the patching cycle for that month. For example, if an update is available for an Application at the time the cycle commences, then the patch will be rolled out as part of that cycle along with all the available patches. Patches that are available after patch Tuesday are not applied until the following month's cycle (unless they are determined to be critical as per step two of the process):

a. once the manufacturer releases new patches, the relevant patch management system is updated with the new patches within one day;
b. all available patches are rolled out to a pilot group for five days for testing to determine if applying the new patches will cause any issues:
    i. critical patches will be an exception to #2 and will not have a 5-day gap but should be shortened appropriately to meet the critical patch timeline.
c. if no issues are identified, then the patches are rolled out to the remaining machines over two weeks;
d. if a machine misses a patch, when it next reconnects to the network, all outstanding patches will be applied (this does not apply if the machine connects over the VPN);
e. if issues are identified with a patch during the patch pilot phase, then the roll-out of the patch is delayed until the issue can be resolved;
f. reboots will be mandated to ensure compliance. However, a staff member may delay the reboot for up to a maximum of 12 hours; and
g. a system is defined as being remediated / fixed once the patch is fully installed and any reboot requirements have been met.

Support for issues with Microsoft patches is available through Microsoft Premium Support.

Servers

(29) Patching system(s):

a. Windows: SCCM; and
b. Red Hat: Satellite.

(30) Support Team: Digital Platform Services.

(31) All systems have a development / testing environment.

(32) Patches are applied to the development / testing environment for a period to determine if there are any negative impacts.

(33) If nothing is noted, the patch is then rolled out to production.

(34) The testing of operating system patches will be performed in conjunction with the Application Owner(s).

(35) Various platform owners will be notified of any upcoming scheduled patching.

(36) All systems will automatically install their updates.

(37) For extra sensitive systems, a manual reboot can be configured; however, additional processes will be required to ensure that reboot occurs. For all other systems, it is expected that the reboot will be automatic.

System	Component	Schedule	Comments
VMWare	Hypervisor & vCenter Upgrades	Every 4 months	Checked monthly, applied 2 months after release, results in near quarterly patching.
VMWare	ESXi & vCenter Security Updates	Every 4 months & ad-hoc	Checked and applied quarterly; Ad-hoc for critical patches following the Patch deployment decision matrix
Linux			
RedHat Enterprise Linux	OS	Monthly	Satellite partially implemented
Windows			
Application	OS	Ad-Hoc	Or ad-hoc for critical patches
Infrastructurei.e. Domain Controller, print server	OS	Monthly	Capability to roll out patches is available, patching schedule to be determined
SAN / NAS	OS	Every 4 months	In collaboration with ACU VMware and Storage partner (Parallo)

Networking Devices

(38) Patching system(s):

a. Cisco Prime.

(39) Support Team: Digital Platform Services.

(40) Patches are first deployed to the test lab and tested. If there are no issues detected, updates are applied to a pilot site for a couple of weeks to ensure that there are no negative impacts. If the pilot site trial is successful, then the patches are rolled out to a few sites and so on, until all sites and locations have been patched.

System	Component	Schedule	Comments
Routers	OS	Annually	Or ad-hoc for critical patches
Switches	OS	Annually	Or ad-hoc for critical patches
Wi-Fi Controller, Access points	OS	Every 6 months	Or ad-hoc for critical patches
Firewall	OS	Every 6 months	Or ad-hoc for critical patches
Load Balancer	OS	Annually	Or ad-hoc for critical patches

Applications

(41) Patches for application systems will be reviewed at least annually by the Technical System Owner to ensure that any missing patches are assessed to determine if they need to be applied, either to correct bugs and security vulnerabilities or to provide additional functionality. Patching of the underlying infrastructure such as the operating system, database, and web server will largely be driven by the ability to perform application testing to ensure that patching those components of the solution does not introduce errors or undesired consequences.

(42) The patching of all systems should be completed automatically except where the application does not support it, or there is a risk of adverse impact on the system.

(43) Support Team: Digital Platform Services.

System	Component	Schedule	Comments
Database	SQL Server database security update	Every 3 months	Or ad-hoc for critical patches
	SQL Server database functionality update	Annually	
	Oracle database	Every 3 months	Or ad-hoc for critical patches

Patching System(s)

(44) The WordPress application represents one of the most exploited online platforms in recent times. Whilst the WordPress systems automatic upgrade is something that has been added with much success; the biggest threat is still the modules / extensions that are often used. Where an upgrade to a module or extension breaks existing functionality, the IT Enterprise Information Security Team will need to assess to determine if a rollback is possible or if the impacted systems will need to be taken offline whilst the bug / code can be fixed.

(45) The standard patching cycle:

Service	Component	Schedule	Comments
WordPress		Automatic	WordPress sites need to be set to automatically upgrade
WordPress plugin / Extension		Monthly	WordPress plugins should be checked and upgraded monthly

Unified Communications / Audio-Visual (AV)

(46) Patching System(s):

a. Manual / SCCM.

(47) Support Team:

a. Digital Platform Services; and

b. IT Service Delivery Team.

(48) Some systems have a development / testing environment. Patches are applied to the development / testing environment for a period to determine if there are any negative impacts. If nothing is noted, the patch is then rolled out to production.

Service	Component	Schedule	Comments
Voicemail	SaaS	n/a	Externally managed service
Office 365	SaaS	n/a	Externally managed service
SharePoint	Application	Every 3 months	Managed by IT Service Delivery Team
Skype for Business Server / Session Border Controllers	Server	Every 3 months	Or ad-hoc for critical patches
Video conferencing – Room systems	Firmware	Ad-hoc as required	May be patched to fix bugs or when new code is required
Audio Visual room equipment i.e. Crestron and video cameras	Firmware	Ad-hoc as required	May be patched to fix bugs or when new code is required
Echo 360	Firmware	Ad-hoc as required	May be patched to fix bugs or when new code is required

Devices and Firmware

(49) Physical hardware presents a challenge to patching and vulnerability management. This will require a level of coordination to complete all patching at times when the systems are already being taken offline to do their OS-based patching.

(50) For example, an ESXi host should have its firmware upgraded when the ESXi is upgraded and patched. If a scheduled patching date comes up and only firmware is available and not an ESXi based patch, then the firmware should be applied to remediate the issue.

(51) If a Spectre / CPU microcode patch is available, the IT Enterprise Information Security Team will need to perform a risk assessment to determine how quickly it should be applied to safeguard ACU systems.

Section 12 - Review

(52) This Procedure must be reviewed every three years. The Chief Information and Digital Officer may initiate a shorter review period.

(53) Unless otherwise indicated, this Procedure will still apply beyond the review date.

Section 13 - Appendix 1: Patch Classification

Criticality	CVSS	Priority Rating	Description
1 (Critical)	9-10	P1	This rating is given to flaws that could be easily exploited by an unauthenticated, remote attacker and lead to system compromise (arbitrary code execution) without requiring user interaction. These are the types of vulnerabilities that can be exploited by worms. Exploits exist and are in use. The system is Internet-connected with no mitigating controls in place.

Criticality	CVSS	Priority Rating	Description
2 (High)	7-8.9	P2	This rating is given to flaws that can easily compromise the confidentiality, integrity, or availability of resources. These are the types of vulnerabilities that allow local users to gain privileges, allow unauthenticated, remote users to view resources that should otherwise be protected by authentication, allow authenticated remote users to execute arbitrary code, or allow remote users to cause a denial of service. Exploits exist and are in use. The system is in a protected enclave with strong access controls.
3 (Medium)	4-6.9	P3	This rating is given to flaws that may be more difficult to exploit but could still lead to some compromise of the confidentiality, integrity, or availability of resources, under certain circumstances. These are the types of vulnerabilities that could have had a Critical impact or Important impact but are less easily exploited based on a technical evaluation of the flaw or affect unlikely configurations.
4 (Low)	0-3.9	-	This rating is given to all other issues that have a security impact. These are the types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited or where a successful exploit would give minimal consequences. A vulnerability requires authenticated users to perform the exploit. Mitigating controls exist that make exploitation unlikely or very difficult.

Section 14 - Appendix 2: Service Criticality

Criticality	IT Service
1 (Critical)	Production, internet-facing
2 (High)	Production, Internal only
3 (Medium)	Dev servers
4 (Low)	Other services

Section 15 - Appendix 3: Patch Deployment Decision Matrix

(54) See the Patch Deployment Decision Matrix for a visual representation.

Section 16 - Appendix 4: Patch Deployment Flow Charts

(55) See the Patch Deployment Flow Charts for a visual representation.

Status and Details

Status	Current
Effective Date	28th February 2024
Review Date	29th April 2024
Approval Authority	Vice-Chancellor and President
Approval Date	28th February 2024
Expiry Date	Not Applicable
Responsible Executive	Russell Parker Chief Information and Digital Officer
Responsible Manager	Mark Brodsky Associate Director, IT Strategy and Program Delivery
Enquiries Contact	Information Technology