

Trim Location:	<Insert TRIM Location>
Document Category*:	Guideline
Purpose*:	This guideline outlines the scope and approach to Patch Management implemented by the University. This guideline will be reviewed on an annual basis and evaluated in line with changes to business processes.
Responsible Officer*:	Executive Director, ICT Services

1 Guideline Statement

It is the responsibility of ICT Services to provide a secure network environment for the staff, students, business partners and contractors of the University of Southern Queensland (USQ).

As part of this goal, it is the responsibility of ICT Services to implement appropriate measures to ensure that all computer devices (including servers, desktop computers, printers, mobile devices) connected to USQ's network have appropriate virus and malware protection, virus definition libraries are current, and that the most recent versions of approved operating systems and security patches have been installed.

This is achieved through a formal process of patch notification, evaluation and release management.

2 Principles

Scope

ICT Services is responsible for the ICT patch management implementation, operations and procedures. ICT Services will ensure that all appropriate and reasonable defences are in place to reduce network vulnerabilities while keeping the network operational. This responsibility includes the tasks detailed below.

Monitoring for Patches and Updates

ICT Services will monitor security mailing lists, review vendor notifications and web sites, and research specific public websites for the release of new patches and updates. Monitoring will include but is not limited to the following:

- Scanning the USQ network to identify known vulnerabilities;
- Identifying and communicating identified vulnerabilities and/or security breaches to ICT Services;
- Monitoring AusCERT, notifications, and web sites of vendors that have approved and supported hardware or software operating on the USQ network;
- Implementation of patch management solutions to identify the patch levels of critical systems including the status of applied patches, requirements for patches where they are yet to be applied, and similar actions.

Review and Evaluation

Once advised of a new patch, ICT Services will download and review the new patch. ICT Services will categorize the criticality of the patch according to the following:

- Emergency – an imminent threat to the USQ network;
- Critical – targets a security vulnerability;
- Not Critical – a standard patch release update;
- Not applicable to the USQ network environment.

Regardless of the platform or criticality, all patch releases will follow a defined process for patch deployment that includes assessing the risk, testing, scheduling, installing and verifying.

Risk Assessment and Testing

ICT Services will assess the effect of a patch to the corporate infrastructure prior to its deployment. ICT Services will also assess the specific patch for criticality relevant to each hardware platform (server, desktop, printer, etc). This will be performed in conjunction with information available from external organisations including assessments based on exposure, ratings by vendors on their criticality, and Third party IT Security Authorities on Vulnerability Mitigation (eg SANS, Auscert, Secunia).

If ICT Services categorizes a patch as an Emergency, ICT Services has made an assessment that it considers it an imminent threat to the USQ network. Under these circumstances, the University will inherit a greater risk by not implementing the patch as soon as is practical rather than waiting to test it before implementing.

Patches deemed Critical or Not Critical for systems that are supported by a development or test system will undergo testing for each affected platform before release for implementation. The scale of testing and environments involved in testing will be determined by the impact of the vulnerability, impact of the patch, impact and feasibility of effective testing and risk level as assessed by the vendor, third party security authority, or ICT, whichever is higher.

ICT Services will expedite testing for critical patches. ICT Services must complete validation against all operating system platforms (eg. Windows, Unix, etc) prior to implementation.

Notification and Scheduling

The schedule for implementation must be approved by ICT Services management prior to deployment. Regardless of criticality, each patch release requires the creation and approval of a Change Request following the [ICT Procedure for Change Management](#) prior to approval being sought to implement the patch.

Depending on the criticality, the Executive Management team of ICT Services will determine when notification to clients is necessary.

Implementation

ICT Services will deploy Emergency patches within eight hours of categorisation (ideally within eight hours of patch availability). As Emergency patches pose an imminent threat to the network, the release may precede testing. In all instances, ICT Services will perform testing (either pre- or post-implementation) and document it for auditing and tracking purposes.

ICT Services will obtain authorization for implementing Critical patches via an emergency Change Request and approval from USQ management.

ICT Services will implement Not Critical patches during regularly scheduled preventative maintenance periods.

Auditing, Assessment, and Verification

Following the release of all patches, ICT Services staff will follow the procedures outlined in the [ICT Procedure for Change Management](#) and review and verify the successful installation of the patch and check that there have been no adverse effects.

Patch Management solutions will generate reports on systems compliance, patch levels and patch application events. These reports should be presented to management on quarterly basis as well as on request.

3 Procedures

4 References

[ICT Procedure for Change Management](#)