

# (Standard) ICT Standard for Patch Management

## Document Purpose

<b>Document Purpose</b>	To ensure that the University has a coordinated, systematic, accountable and documented strategy for the effective and efficient handling of known vulnerabilities and operating system and application software patches, to assist managers and staff to better secure the University's information systems from malicious or accidental exploitation.		
<b>Document Information</b>	Version		
	Release Date		
	Release Status		
	Review Date		
	Author(s)	Manager, Business Continuity & Risk Management	
	Owner	Principal Manager, Infrastructure & Systems	
	Print Date	Last Printed: 7/09/2009 2:20:00 PM	
	Approved By		
	Policy	USQ ICT Policy for Information Management and Security	
	Type of Document	Standard	
	Electronic Location and Filename	<a href="http://www.usq.edu.au/resources/106.pdf">http://www.usq.edu.au/resources/106.pdf</a>	
<b>Version Control</b>	Version	Date	Author(s)
<b>Error Advisory</b>	<p>To the Reader:</p> <p>If you encounter any inaccuracies or printing faults in this document please contact the Owner (see Document Information section, above) as soon as possible. The Owner will then initiate the required modifications</p> <p>If you are unable to contact the Owner, contact that person's Manager Supervisor.</p> <p>Thank you for helping the Division of ICT Services maintain quality documentation.</p>		

# Table of Contents

<b>Document Purpose .....</b>	<b>1</b>
<b>Document Information .....</b>	<b>1</b>
<b>Error Advisory .....</b>	<b>1</b>
<b>1 Definitions.....</b>	<b>3</b>
<b>2 Introduction .....</b>	<b>3</b>
<b>3 Standards.....</b>	<b>4</b>
3.1 Accountability .....	4
3.2 Responsibility .....	4
3.3 Patch Management Team .....	4
3.4 Change Management.....	4
3.5 Prioritisation.....	4
3.6 Risk Assessment .....	5
3.7 Patch Cycle .....	5
3.8 Assurance Testing.....	5
3.9 Responsibility for Patch Installation.....	6
<b>4 Related Documents.....</b>	<b>7</b>

DRAFT

# 1 Definitions

The ICT Glossary and Definitions contains a description of any common ICT terminology referred to in the policy and standard documentation.

## 2 Introduction

Despite the efforts of vendors, all operating system and application software are released with vulnerabilities, weaknesses that can affect the functionality, security, performance and stability of the University of Southern Queensland's (USQ) information systems.

Often when a vulnerability is discovered the software manufacturer will release a piece of additional code to correct or mitigate against the vulnerability, a patch, hotfix, update, fix, service pack or other work around to:

- fix faults in operating system or application code
- increase or alter functionality, and/or
- change or modify the software to make it less susceptible to accidental or malicious exploits.

New vulnerabilities are constantly being discovered and patches for the wide range of software in service at USQ are often released. Timely attention to the application of these updates is critical to maintaining the confidentiality, integrity and availability of the University's information systems. Failure to keep software "patched" is however the most common mistake made by information technology professionals.

Applying patches or workarounds to mitigate known vulnerabilities can be complex, time-consuming and resource intensive., and it is often difficult to keep abreast of all new patches. A coordinated strategy for dealing with vulnerabilities and patches can make for a more efficient and effective outcome. The University's strategy will incorporate procedures to:

- Maintain an inventory of currently used operating system and application software;
- Identify newly discovered vulnerabilities and vendor supplied patches;
- Coordinate prioritisation of vulnerabilities and patches to develop a recommended patch implementation schedule based on assessed risk;
- Maintain a local USQ specific patch repository;
- Test patches for functionality and security to the degree possible with available resources and concurrent with the information system classification;
- Communicate vulnerability and patch information to responsible staff;
- Verify the correct application of workarounds and patches through network and host based vulnerability scanning;
- Train staff and clients in the implementation of patches and other steps to mitigate vulnerabilities;
- Deploy patches automatically where fitting;
- Configure the automatic update of client-based software where applicable.

[Based on [NIST SP 800-40: Procedures for Handling Security Patches](#), National Institute of Standards and Technology]

## 3 Standards

### 3.1 Accountability

The Principal Manager Infrastructure and Systems within the Division of ICT Services is accountable for ensuring that procedures are implemented for applying patches and for maintaining a recommended patch implementation schedule for all operating system, database and application software utilised at the University of Southern Queensland.

### 3.2 Responsibility

System Owners and delegated ICT Staff are responsible for applying patches and must take into account a recommended patch implementation schedule but will have the final approval for the implementation of patches for individual Information Systems under their administration.

These staff members are also responsible for maintaining an inventory of the operating system, database and application software, including relevant version numbers that is representative of the important software currently being utilised in the University.

### 3.3 Patch Management Team

A Patch Management Team will be formed within the Division of ICT Services to support responsible staff in finding, prioritising, fixing vulnerabilities, applying patches, and maintaining the recommended patch implementation schedule.

The Patch Management Team will actively monitor authoritative vendor and security related sources for newly discovered vulnerabilities and approved workarounds and/or security patches.

Where a serious vulnerability is identified where there is no satisfactory patch, the Patch management Team will develop steps to mitigate the weakness from being exploited until a patch or other permanent solution is made available.

### 3.4 Change Management

Patch management procedures will comply with the *ICT Standard for Operational Security Management* in conjunction with the *ICT Procedure for Change Management*.

### 3.5 Prioritisation

Specific attention will be applied to ensure that all operating system, database and application software utilised for secure, sensitive, or Internet facing information systems, is correctly addressed in the software inventory and recommended patch implementation schedule.

### 3.6 Risk Assessment

The Patch Management Team must assess risks associated with newly discovered vulnerabilities and prioritise the implementation of workarounds and patches based upon a variety of time, event and/or system classification (Secure, Sensitive or Public) data. The following schedule is proposed but can be influenced by other events. For example, a vulnerability may be assessed with regard to the following: Reported Denial of Service or local access exploit – Low impact; Reported remote access exploit – Moderate impact; Reported exploit released – Important impact; Reported automated exploit such as a virus or worm – Critical impact.

<b>Recommended Patch Implementation Schedule</b>					
	<b>Non-Security</b>	<b>Low</b>	<b>Moderate</b>	<b>Important</b>	<b>Critical</b>
<b>Public</b>	Normal cycle	Month	Month	Fortnight	Week
<b>Sensitive</b>	Normal cycle	Month	Fortnight	Week	Day
<b>Secure</b>	Normal cycle	Fortnight	Week	Day	Immediate

<b>Microsoft Recommended Timeframe for Patch Deployment</b>		
<b>Severity Rating</b>	<b>Recommended</b>	<b>Maximum</b>
<b>Critical</b>	Within 24 hours	Within 2 weeks
<b>Important</b>	Within 1 month	Within 2 months
<b>Moderate</b>	Depending on expected availability, wait for next service pack or patch rollup that includes the patch, or deploy the patch within 4 months	Deploy the patch within 6 months
<b>Low</b>	Depending on expected availability, wait for next service pack or patch rollup that includes the patch, or deploy the patch within 1 year	Deploy the patch within 1 year, or choose not to deploy at all.

### 3.7 Patch Cycle

The Manager Systems Administration and ICT Service Coordinators will document a standard patch cycle for systems under their administration. The procedure will incorporate details of the testing regime required with respect to the information system classification, and/or the specific software being updated where required.

### 3.8 Assurance Testing

The Security Officer (operational) will verify correct installation of patches by performing periodic network and host vulnerability scanning in accordance with USQ Policy and Standards.

### 3.9 Responsibility for Patch Installation

System, Database and Application Administrators:

- Are accountable for patching information systems under their control;
- Will have final approval regarding the application of workarounds and patches;
- Will advise the Patch Management Team in cases where it is not possible to implement a recommended workaround or patch in the suggested timeframe;
- Will test patches before applying where possible;
- Will assist with the identification of patches applying to operating system, database and application software that is currently not being included in the list of software monitored by the Patch Management Team;
- Will assist {Some central group} to maintain the operating system and application software inventory with details pertaining to software that is either of a critical nature or is in broad use across the University.

DRAFT

## 4 Related Documents

Document (Electronic)	
Document (Hardcopy)	

DRAFT