Queen Mary
University of London

IT Services Policy

ITP01 - Patch Management Policy

Prepared by: < Shelim Miah>
Version: V1.0

Description & Target Audience: Policy to outline the requirement of all systems and software applications to be Patched frequently and carried out appropriately. The Policy is aimed at all in QMUL who own or manage QMUL systems and applications.			
Effective Date:	**08/06/2015**	Review Date:	**08/06/2016**

Reviewers:	**Johnathan O'Regan, Assistant Director Infrastructure** **Tavinder Jandu, Head of Network Infrastructure** **Martin Evans, Head of Data Centre Services** **Nigel Proctor, Head of Client Devices & Audio Visual** **Steve Wicks, Servers & Storage Manager** **Brian Ragunathan, Academic Applications Technical Manager** **Paul Gallagher, Head of Application Technical Support** **Ian Douglas, Head of IT Security** **Alan Hardy, Change, Release & Deployment Manager**

Authorisation:	
Name / Position	**Chris Day, IT Director**
Signature	**Chris Day**
Date	**08/06/2015**

Policy Owner:			
Name/Position	**Johnathan O'Regan, Assistant Director Infrastructure**		
Revision History			
Version	Description	Author/Updates	Date
0.1	First Draft	Shelim Miah	14/08/2014
0.2	Minor Revisions	Alan Hardy	28/08/2014
0.3	Deletion of an inventory in requirement & expansion of Software patch definition	Martin Evans	13/10/2014
0.4	Comments from Nigel Proctor	Shelim Miah	21/10/2014
0.5	Minor changes –Ian Douglas's comments	Shelim Miah	05/11/2014
0.6	Minor Changes	Shelim Miah	11/12/2014
0.7	Changes made from Ian Douglas Comments	Shelim Miah	09/01/2014
0.8	Added additional comments from Ian Douglas	Shelim Miah	09/01/2015
0.9	Changes made from Johnathan's comments	Shelim Miah	14/01/2015
0.10	Comments from by Toney Higgins	Shelim Miah	03/02/2015
0.11	Comments from Brian Ragunathan	Shelim Miah	03/03/2015
0.12	Update from Johnathan O'Regan on 5.2	Shelim Miah	20/03/2015
0.13	Updates from David Boakes	Shelim Miah	14/05/2015
V1.0	Approved by the IT Lead Team	ITLT	08/06/2015

Contents

1 Policy Statement

1.1 This Policy has been drafted by IT Services to outline the requirements for maintaining up to date software patches to ensure all software on systems, applications and devices owned and managed by IT Services are routinely updated with critical software patches, particularly security patches.

1.2 By implementing a patch management process IT Services can effectively distribute security patches automatically and can provide it's users a safe and secure environment

1.3 The Policy aims to:

- Establish a maintenance window for software patching
- Create a proactive approach to patch management
- Minimise the threat of being compromised
- Ensure a process is in place for patch management
- Establish patch management as a routine, pre-approved, regular activity
- State roles and responsibilities
- Encourage collaborative working

2 Scope

2.1 A patch, sometimes referred to as a "fix" or "hotfix" is a software update inserted (or patched) into the code of an executable program. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases or service pack of a software package.

Patches may do any of the following:

- Address security vulnerabilities
- Address software stability issues
- Fix software bugs
- Enhance functionality
- Install new drivers
- Improve Performance

2.2 This Policy covers all IT Services supported by ITS and includes all schools and faculties.

2.3 This policy applies to employees, contractors, consultants, temps, and other workers at QMUL including all personnel affiliated with third parties.

2.4 This policy applies to all IT Services managed by QMUL, but specifically the following service components:

- Servers
- Network Devices (e.g. routers and switches etc.)
- Client Devices and peripherals (e.g. Desktop, Laptop or Tablet computers, smartphones and Printers)
- All Hardware, Operating Systems, Database, Applications, Enterprise Applications, Firmware and MiddleWare.

2.5 What is deemed out of scope is upgrades, where a software is upgraded to a new version offering new functions and facilities this is considered as an upgrade and will be managed as a project.

2.6 This Policy will be effective from the date of approval until this Policy is either superseded or decided by the IT Lead Team (ITLT) that this Policy should no longer be applicable.

3 Policy Detail

Notification

3.1 All maintenance windows are to be initially agreed with the relevant stakeholders after which there will be no advanced notification to users that a patch is going to be applied other than a reoccurring entry on the Service Status page for patches regarding pre-agreed regular maintenance windows for the purpose of performing server updates, applying patches, application updates and hotfixes.

3.2 Where the facility allows, login pages of applications should have a similar message publicising the pre-agreed regular maintenance windows.

3.3 Where the facility allows, applications must be configured to redirect users to a pre-defined landing page when the application is inaccessible containing information to guide users whether it is due to known planned maintenance or not.

3.4 Where a change freeze is in effect, all scheduled maintenance windows will be superseded.

Patch Management Risk

3.5 All patch management needs to be logged as a change in the ITS helpdesk system, as part of the Change Management process.

3.6 The deployment and installation of patches where there is a risk of a service outage must follow the Change Management process for non-standard changes. Where there is no risk of service outage the patch can be applied within the maintenance window.

3.7 Any server that has the potential to impact an application service needs to reference the application and the potential impact within the ticket for the server that is to be patched. This is to alert the change manager.

3.8 Any patch that is deemed too high risk to implement, must have alternate controls in place to mitigate against the vulnerability and must be approved by the ITLT.

3.9 ITS need to align with the vendor patch releases cycle where possible to ensure that the window of vulnerability, specifically related to security, is kept to a minimum.

3.10 A log or record of patches that have been applied to a server or service need to be held by the team that are responsible for the server/service

Service Interruption

3.11 Routine patch management cycles may require servers/services to be restarted, occasionally multiple restarts maybe required and some may require to be restarted in a particular sequence, which all should be done during the maintenance window.

3.12 The maintenance window should be arranged for a time when there is minimal impact on the users of the service unless agreed with stakeholders.

3.13 As per 3.1 to 3.3 regarding notification, users should be able to find out when a service has been, or is scheduled to be, unavailable and when the service is available.

Release Approaches and Deployment Methods

3.14 The following release approaches and deployment methods should be considered and the most appropriate chosen depending on the type and criticality of the patch, the service it affects and the type of service component as listed within the scope of this policy detailed in section 2.4.

- Big Bang or Phased Release
- Push or Pull Deployment
- Automated or Manual Deployment

Standard Testing and Troubleshooting Expectations

3.15 Where a User Acceptance Testing (UAT) environment exists; patches should be applied to the UAT environment and tested successfully before being implemented in production. For critical Enterprise Applications this is mandatory.

3.16 Updates should be tested and documented in the UAT environment to ensure the issue(s) listed section 2.1 has been addressed and no new issues have been introduced and performance has not been compromised.

3.17 Once installed in the production environment any tests carried out in UAT should be repeated.

3.18 Where no UAT environment exists documented testing needs to be carried out to ensure that the Issue (s) have been addressed and no new issues have been introduced and performance has not been compromised.

3.19 As per normal Change Management procedures, in cases where errors or issues arise during testing, irrespective of environment there needs to be a roll back plan in place that can be executed, to ensure business continuity whilst the errors or issues are rectified.

Preferred Patch Schedules and Maintenance Windows

3.20 Preferred patch management schedule and maintenance windows will be owned by the Change Management process to ensure that there is a co-ordinated approach that minimises disruption to the users but at the same time enables IT Services to carry out the essential work in a timely manner.

3.21 The schedule is published on the ITS website and is maintained by the ITS Change Manager:

Emergency Patching

3.22 There may be circumstances where a patch maybe required to be implemented outside of the normal maintenance windows and at short notice for example to restore the service or address a high risk security vulnerability. These must follow the Emergency Change process but testing outlined in 3.16 to 3.19 must be carried out.

Enterprise Application

3.23 Before any patch is applied the impact of installing the patch should be understood and risk assessed for all Enterprise Applications.

3.24 Where a patch being implemented and has an effect on applications (e.g. .NET & Java updates, IIS changes etc.) then the following should be carried out:

a) Check with vendor to see if they have tested this patch
b) Does it require a restart (need approval from business for outage)
c) Can it be tested in UAT first

3.25 Restarts for Enterprise Applications should be carried out in a way to ensure that no data is lost, this may require restarts to be done in a specific way, therefore should be carried out by the appropriate team member in the Applications team.

3.26 Enterprise Application updates should not be carried out as part of a patch release unless there is a requirement and it is needed. After the implementation of a patch, tests should be carried as per 3.16 to 3.19.

3.27 All Enterprise Application patches must go through the UAT first before being applied to the Production environment.

3.28 Assessments should be made to ascertain the level of risk exposed by delaying the implementation of a patch, as they can and do get recalled. If the risk is unacceptable the patch should be applied with a roll back plan in place in the event of a recall.

Keeping Patches Up to Date

3.29 Where a particular service has been risk assessed and the patch poses minimal risk, automated patching should be considered. Checks, manual and or automated should be made to ensure patching is up to date and being deployed appropriately.

3.30 Service owners must ensure that their teams are carrying out patch installations and that the appropriate individuals are monitoring the release of new patches.

3.31 Regular contact should be established with vendors to identify the release of new patches, this could be in the form of mailing lists or checking vendor noticeboards and websites.

3.32 Subscription to a third party security advisory website which is not affiliated with any particular vendor, may provide information on the latest vulnerabilities and fixes. This information should also be verified with vendors for accuracy.

4 Roles & Responsibilities

4.1 Heads of Departments or Services and Assistant Directors will ensure that patch management is given sufficient priority to allow IT Services to carry out patch management.

4.2 IT Services will make every effort to keep all patching and updates to the maintenance windows specified.

4.3 Application and infrastructure owners will each be responsible for monitoring the release of new vendor patches.

4.4 The Change, Release & Deployment Manager will liaise with the operational service owners to ensure appropriate due process is followed.

4.5 ITS staff must ensure that adequate communications are provided to the users where appropriate.

4.6 All ITS teams and stakeholders must work together to ensure that patching is carried out in the appropriate order to minimise disruption to the service.

5 Monitoring

5.1 Compliance

5.2 Periodic assessments will be undertaken to ensure compliance with this Policy. KPI reports will be generated and corrective actions taken where appropriate.

6 Exceptions

6.1 In the event of an exception that is not addressed by this Policy. The matter will be firstly referred to the ITLT for a decision via the appropriate Assistant Director.
The ITLT will then make a decision or refer this to ITSIB for guidance.

7 References

- SANS institute
- Trinity University
- Tech Republic
- NIST Guide to Enterprise Patch Management - http://csrc.nist.gov
- Wikipedia

8 Appendix

8.1 Appendix A - Definitions

Term	Meaning
ITLT	IT Lead Team – Team of Senior Managers consisting of the Assistant Directors of IT, Faculty Relationship Managers and Chaired by the IT Director.
ITSIB	IT Strategy Implementation Board – Team of Executive managers consisting of Vice Principals and the IT Director, who oversee the delivery of the IT Strategy.