Configuration & Patch Management Policy

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	20/10/2016
V 0.2	Andrew Clarke	Scheduling amendments agreed as 3 months	15/11/2016
V 0.3	Andrew Clarke	End-of-life and Out-of-support caveat, clearer local ownership and responsibilities, clearer demarcation between patch and release management	17/02/2017
V 0.4	Andrew Clarke	Greater clarification of steps required to install patch – section 9	17/02/2017
V 0.5	Andrew Clarke	Technical amendments from PWG	21/02/2017
V 0.6	Andrew Clarke	CISA amendment (TY) to provide for exceptions, flexibility and risk assessment. Approved	05/04/2017
V 1.0	Andrew Clarke	Approved Information Subcommittee	27/04/2017
V 1.1	Andrew Clarke	Approved ISC	20/06/2017
V 1.1	Andrew Clarke	Annual review	02/08/2019
V 1.1	Andrew Clarke	Annual review	14/05/2020

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

Owner: Michael Jenkins	Chief Information Security Officer
Signature: MGJ	Date: 20 Jun 2017
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: PK	Date: 20 Jun 2017
Distribution:	

This document requires the approval from BUL as defined in the ISMS Compliance document.

Contents

1. Purpose of Document

This document defines the Configuration and Patch Management Policy that will need to be applied relating to the Brunel University London Systems hardware and software components to ensure a consistent approach to maintaining agreed software/hardware configuration levels.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

2. Responsibilities

Table 1 – responsibilities

Title / Role	Description
Systems Manager	Is responsible for monitoring vulnerabilities and vendors' releases of patches and fixes and installing operational software updates, patches and fixes on the operational systems Is responsible for testing software items updates and new implementations Is responsible for the Operations and Production environments, known as 'Ops' & 'Prod'
Head of Infrastructure and Operations	Is responsible for overall Patch Management on all systems managed by IS.
Head of Development and Application Services	Is responsible for monitoring vendors' releases of upgrades and new releases on server application software. Is responsible for installing server application software updates and testing software items updates and new implementations
Software tester	Is responsible for testing development software items updates and new implementations
Software Application Owners	Are responsible for tracking likely vulnerabilities in and patches available for their assets
Cyber & Information Security Manager	Is responsible for vulnerability risk assessment

3. ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A12 – Operations Security
ISO 27001:2013 Conformance Control	Information Classification Objective A.12.6 Technical Vulnerability Management

4. Background

Security Patch Management is a topic which has attracted increased attention in recent years, as organisations are affected by the increasing number of viruses, worms and other malicious software which have been developed and released. A considerable amount of this malicious software has been targeted at known vulnerabilities on unpatched systems, leading to downtime and expense as organisations respond to the attacks.

The main objective of a patch management policy, working in conjunction with the Vulnerability Management Process and the Patch Management Process, is to create a consistently configured environment that is secure against known and identified vulnerabilities within operating system and application software.

5. Scope

This document defines the University approach for managing vendor released service packs and/or bug fixes and/or single patches in between functionally upgraded Operating System releases and Service Packs.

Implementation of the policy will ensure that the University will not be left exposed to known problems or vulnerabilities for which fixes exist. Installing patches, as a precaution, is a correct and proper business requirement that will prevent operational problems, hacks, downtime, and degradation of service. This will apply to all systems in the same way, regardless of the operating system.

Major software releases:
A major upgrade or release usually supersedes all preceding minor upgrades, releases and emergency fixes normally containing large areas of new functionality, some of which may make intervening fixes to problems redundant.. A major release can be defined by the vendor usually as a renaming convention (e.g. Windows XP to Windows Vista or Windows 2012 to Windows 2016) or as an integer version release (e.g. Windows 8 to Windows 10). A major software OS or application release is usually attributed to changes made that invoke incompatible API (Application Programming Interface) changes. The deployment of these is out of scope and is covered by the Release Management policy.

Minor software releases and hardware upgrades, normally containing small enhancements and fixes, some of which may have already been issued as emergency fixes.
A minor upgrade or release usually supersedes all preceding emergency fixes. A minor release by a vendor is usually identified in the naming convention as prefixed by the exiting naming convention followed by a decimal point (e.g. Windows 8 to Windows 8.1 or Advanced Aircraft Analysis 3.6 to Advanced Aircraft Analysis 3.7) and is within scope of the Patch Management Policy
Emergency software and hardware fixes, normally containing the corrections to a small number of known problems and is within scope of the Patch Management Policy

It may be that a change to a business process or procedural measures is the preferred solution for minimising a risk, rather than implementing a patch. These solutions are excluded from this document.

The scope of this document covers:

- All the University's information systems are within the scope of this procedure;
- Server Hardware including SAN storage devices, server chassis mounted fibre channel and Ethernet switching, on-board remote management devices and applications;
- Desktop PCs, Workstations and Laptops;
- Firewalls, Encryption Devices, Routers and Secure Access Solutions;
- LAN Switching Equipment;
- Wi-Fi Equipment;
- Mobile Devices / Laptops *(pending MDM deployment)*
- Server Applications both local and IS managed;
- Printers;

6. Out of Scope

- Bring Your devices (BYOD)

7. Overview

The process for deployment of security patches is described in the following paragraphs. This approach is based on information from key vendors, Microsoft, Linux and VMware.

8. Identification and Assessment

The first stage in the patch management process is the initial identification of the critical or security patch or vulnerability. This information is triaged from a number of sources such as vendor specific tools, vendor security bulletins and third party sources.

Information Services are responsible for providing a list of recommended Windows, Linux, Application and VMware patches throughout the University environment. Vulnerability scans are performed regularly by a vulnerability scan tool run by the CSIRT team to assist in identifying the necessary critical patches to apply. IT applications are responsible for providing a list of recommended business application patches.

Vulnerabilities will be grouped into two categories based on advice provided by the vendor and information collated from relevant third parties (CPNI, SANS Institute).

Critical/Security: The patch should be raised for review and approval, test and deployment completed within a timely and managed fashion. The testing should ensure the integrity of the released patch along with the integrity of the servers and applications the patch is applied to. This should be deployed throughout the live environment within a quarterly schedule (3 months) with patching being scheduled on a monthly basis.

Low /Important/Moderate. The patch should be raised for review and approval, test and deployment completed within a timely and managed fashion. The testing should ensure the integrity of the released patch along with the integrity of the servers and applications the patch is applied to. This should be deployed throughout the live environment within 6 months with patching being scheduled on a monthly basis.

N.B – a third category – **Emergency/Out of Band** – should be reserved for extreme cases where for example a Denial of Service attack is imminent. In this extreme case an Emergency Change Approval Board should be convened with the intention of approving, testing and deploying the patch within 14 days, note this does not preclude earlier deployment if the circumstances permit such a rapid deployment. It is possible that such changes may need to be authorised retrospectively.

It will be taken into account the risk of applying the patch (as well as that of not applying) – for example there may be a risk that a patch could cause an application to fall over, or could compromise the integrity of an imminent application release.

9. Ownership and responsibilities

Regarding local peripheral devices (handheld devices such as mobile phones and local acquired printers), the maintenance and patching of these remain the responsibility of the relevant IT service unit attached to the Business Unit that acquired them.

With regard to local applications, these also, will remain the responsibility of the relevant IT service unit attached to the Business Unit that acquired and uses the application. However, advice and guidance can be sought from both Information Services and the Cyber and Information Services Team (CIST) with regard to best practice.

Concerning end-of-life and out-of-support devices and applications, consideration must be given to refreshing these to a supported level. These remain a significant risk to the University Cyber Security as vulnerabilities can be exploited for malicious gain without any capabilities of remediating or mitigating these risks.

Any such devices and applications must be identified and actions taken to mitigate the risk where possible (e.g. reducing access, removing Internet capabilities)

10. Testing

General

The patch must be obtained either directly from the vendor or downloaded from a reputable source (vendor only - not from cnet, filehippo etc. and never a torrent).

If the applications are Open Source and available only via a torrent, extra care must be taken and additional precautions taken during the download to ensure that the system is isolated and potential malware is not introduced into the University network (see below).

At present there is not a test environment to perform like for like testing prior to live deployment. As such there are additional risks associated with applying patches to servers running business applications.

If a test server is available the patch will be deployed onto the test server first. If no test server is available it is recommended that the patch be deployed to at least one non-critical server in the live environment prior to deployment on servers running critical University applications.

Ensure the Patch Update is Safe

All files relating to a patch update should be reviewed in an isolated environment where possible (remove the server from the network unless connectivity is required during installation), in order to prevent malicious code from entering the University infrastructure, and to confirm their digital authenticity.

The first component of patch testing will thus be the verification of the patch's source and integrity. This step helps ensure that the update is valid and has not been maliciously or accidentally altered. Digital signatures or some form of checksum or integrity verification should be a component of patch validation. This signature should be regularly verified, especially as an update is passed through an organization's technology operations (e.g. on the update server, in build images, in software repositories). Seek advice from Information services on how to do this.

It should be noted that auto-update mechanisms such as WSUS and VMWare Update include vendor patch verification.

If integrity checks are not possible as the vendor does not provide a checksum, then the minimum integrity check should be on whether the patch contains malware, right click the downloaded file and scan for viruses.

Installation

The method used to install patches during a test should be the same as that used in the live environment – servers used for the tests should be rebooted both before and after the tests are performed. Rollback and uninstall options should be tested by removing the patch and rebooting the server. When the patches have been installed and tested, the server must be tested to ensure that its functionality has not been altered in any unexpected manner – there may be standard monitoring tests which can be executed to perform this task.

User Acceptance Testing (UAT)

This testing will include making sure the system reboots as expected along with test procedures comprising executing the application to ensure that the new release/features are installed as expected or advised and that no undocumented failures are observed. The execution of test scripts should be used to perform UAT that validate continued system and application functionality for larger application deployments and are only required for applications that are used across a spectrum

of departments. The extent of testing is dictated by system criticality and availability requirements, available resources, and patch severity.

Evaluation
When the tests have been completed the outcome should be recorded, including details of any rollback tests.

Backup
All servers must have a full backup taken prior to LIVE patch deployment, including the server system state where possible.

Schedule
The schedule for deploying updates will vary depending on the platform and type of update. Server patches will be applied out of hours over weekends during scheduled maintenance windows. Clusters and other resilient solutions need to be reviewed to ensure that an active node is always available.

The IS Customer Services and University Departments must be informed that a deployment is taking place, so that they have advance warning should there be a cluster of identical incidents.

Installation
Installation should take place in an identical manner to the tests, including the operation of uninstall and rollback options. While applying patches, and especially security updates, in a timely manner is critical, these updates must be made in a controlled and predictable fashion.

Review
The University Sanity Check process will be applied to any servers that form part of a business application architecture. Feedback from each patch deployment should be reported to the Service Delivery Team to ensure that future deployments gain from experience, and provide input to help update this policy document. Feedback should include:

- Success and failure stats, showing number of devices affected;
- Timings, showing how long the exercise took so that future deployments can be more accurately forecast;
- Remedial action for devices where updates did not take place;
- Lessons learnt;
- Cost;
- Recommendations.

Standard Builds

Any deployed patches must be included in future standard builds, which may only be updated at longer intervals.

Patch Exception
Exceptions to the Patch management policy require formal documented approval from the Head of Infrastructure and Operations and the Cyber & Information Security Manager. Any servers or workstations that do not comply with policy must have an approved exception on file.
An applicable patch that cannot be implemented by the implementation deadline is an exception and requires a Security Exception Letter.
The table below describes how this form is completed and approved.

When a patch exception may occur.	Who completes the form and obtains approvals.
During the initial assessment.	Functional Support.
During testing or implementation.	Functional Support or Software Application Owner.
At any time for business reasons.	Software Application Owner.

Note: Functional Support is defined as the group responsible for identifying and assessing patches and performing Functionality Testing.

11. Deployment

10.1 Microsoft Servers

A fundamental element of Microsoft patch deployment is for the server to be registered within the Windows Server Update Services **(**WSUS) management system. WSUS will be responsible for scanning the servers on a quarterly basis and providing a list of Microsoft patches to be applied on a server by server basis.

The integrity of all Microsoft patches is checked within WSUS prior to deployment. If a server is not being managed by WSUS it will be highlighted as a remedial action in the quarterly patch report.

Rollback
Should a problem arise on a server after a patch has been deployed one of two methods will be used to recover the server.

1. Driver or application not working;

WSUS has a built in rollback feature that will undo the patch that was last applied.

2. Server blue screen;

The server will be returned to its last known good configuration using the system state backup taken prior to patch deployment.

A standard build image of the server OS will be used to deploy new or replacement machines. (Reference BUL-POL-10.13 Configurations v0.1) Once the new machine is

joined to the domain it will be updated (via WSUS) to the latest patch levels as in the existing server farms or workstations. Updates to the “Base Image” will be covered under the Brunel University London Change Management Process.

Patch levels, image versions and machine specific configuration of the new machine will be verified against current levels on the existing machines or against server documentation for IP addresses/ naming conventions.

10.2 Linux/Unix Servers

An essential element of Linux/Unix patch deployment is for the servers to be registered within the third party patching management system. This management system automates and simplifies the scanning of the servers on a quarterly basis and the automatic deployment of vendor patches to be applied on a server by server basis.

The integrity of all vendor provided patches is checked prior to deployment.

Rollback

Should a problem arise on a Linux or Unix server after a patch has been deployed it is possible to roll back the patch using patchinstall with -r and specify the build number of the last patch installed (the patch to be removed).

Patches that affect running daemons require you to restart manually.

10.3 Microsoft Workstations

For Microsoft workstation patch deployment it is necessary for each workstation to be registered within the Windows Server Update Services **(**WSUS) management system. WSUS will be responsible for scanning the workstations on a quarterly basis and providing a list of Microsoft patches to be applied on a device by device basis.

The integrity of all Microsoft patches is checked within WSUS prior to deployment. If a server is not being managed by WSUS it will be highlighted as a remedial action in the quarterly patch report.

Rollback
Should a problem arise on a workstation after a patch has been deployed WSUS has a built in rollback feature that will undo the patch that was last applied.

10.4 Server Applications

General

In order to maintain the stability of critical University systems it is recommended that applications only be patched to:-

- Deploy Security or critical vendor provided update;
- Fix a specific problem without a workaround or;

- A support or license issue.

Testing
There are additional risks associated with applying patches to servers running University applications. The patch will be deployed onto a TEST server first and users will be asked to perform UAT.

In addition to UAT, the execution of test scripts from a pre-configured user account with access to all business applications must be run for sanity check purposes. Once the application owner confirms UAT is successful the patch will be deployed to the LIVE server.

Upgrades to a new version of a business application should be managed by the Release Management function.

Rollback
Should a problem arise on a server after a patch has been deployed the server will be returned to its last known good configuration using the full backup taken prior to patch deployment.

10.5 VMware

General
VMware use three mechanisms to provide bug fixes for their products;

Maintenance Releases or Updates
A maintenance release is provided on an as needed basis, for example when a bug or a set of bugs are affecting a number of customers severely and one cannot wait for the next product update.

Minor Releases or Updates
Minor Releases are released regularly to provide fixes for bugs identified in current releases, and may include some minor enhancements.

Major Releases or Upgrades
A major release will normally include all the bug fixes provided by releases for the previous version. In addition, it will contain fixes for critical and serious bugs discovered since the last release, and as many fixes for non-critical. This type of update will be handled by the Release Management function.

Deployment
Currently installing a patch or update on an ESX host server is a manual process which requires all Virtual Machines running on the physical ESX host server to be shut down or migrated [Vmotion] to another physical ESX host server. Extra planning will be required for VMware patches in order to minimise the downtime required.

Rollback
Should a problem arise on an ESX host server after a patch has been installed; the server will be rebuilt to its last known stable patch version using the snapshot taken prior to deployment.

12. Deployment review

10.1 Monthly reports on patch deployment should be executed and distributed to both the CSIRT team and the Cyber & Information Security Manager to review and ensure that exceptions are identified and risks reviewed.