University of Aberdeen

Vulnerability & Patch Management Policy

Version 1.7 – September 2019

Table of Contents

Document Control

File Name	Patch Management Policy.DOCX
Document Version	1.7
Document Owner	M. Marooth
Date Released	[Publish Date]
Readership	DDIS, IGC, System Owners and Service Owners
Location	[SharePoint][Policy Zone]

Amendment History

Version	Date	Comment	Author
1.0	12th April 2018	Initial draft	M Marooth
1.1	10th December 2018	Updated to reflect latest changes to IASME Cyber Essentials criteria	M Marooth
1.2	8th January 2019	Review Updates	M Marooth
1.3	4th February 2019	Further Review Updates	M Marooth
1.4	5th February 2019	Comments D Dawson & A Matthews	M Marooth
1.5	5th March 2019	Comments Katie Wilde & CISO Change	M Marooth
1.6	3rd April 2019	Review of Accountabilities	M Marooth
1.7	19th September 2019	Publish	M Marooth

Review and approvals

Function	Name	Date
Reviewed:	Distribution	
Approved:	Information Governance Committee	June 2019

Distribution

Role	Name
Director of Digital and Information Services	Brian Henderson
CISO	Mark Mair
IT Security Manager	Garry Wardrope
Assistant Director (Service Management)	Richard Lynch
Assistant Director (Applications Management)	Ian Robotham
Server Infrastructure Manager	Derek Dawson
Network Infrastructure Manager	Alastair Matthews
Desktop Manager	Ian Rowley
Data Centre Manager	Martin Fraser
Service Desk Manager	Iain Cameron
Research IT Manager	Katie Wilde

Purpose

The University of Aberdeen IT Infrastructure must be properly maintained with the most up to date patches and updates. This is to minimize system vulnerability and to ensure the confidentiality, integrity and availability of its systems and data (including third party data) stored on its systems. IT Systems across the institution are critical to the objectives of the University to deliver on its Foundational Principle. Without, strong, protected and robust IT Systems, the University faces significant loss of Revenue, Reputational Damage and impact to Research.

This policy establishes a standard framework and procedures for the implementation of Business as Usual software patching as well as the identification of vulnerabilities and mitigation of such vulnerabilities and the methods by which those vulnerabilities are prioritised for mitigation.

Scope

This policy applies to all software, servers, desktops, laptop computers, mobile phones and IT appliances owned and operated by the University of Aberdeen.

Common Terms

Term	Definition
DDIS	Directorate of Digital and Information Services
IGC	Information Governance Committee
Patch	A set of changes to a computer program or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities and other bugs.
Vulnerability	A weakness which can be exploited by a Threat Actor, such as an attacker, to perform unauthorised actions within a **computer** system.
Vulnerability Management	https://en.wikipedia.org/wiki/Vulnerability_management
Patch Management	https://en.wikipedia.org/wiki/Patch_(computing)
SCCM	A systems management software product developed by Microsoft for managing large groups of computers.
Satellite	A systems management product by the company **Red Hat** which allows system administrators to deploy and manage large groups of **Red Hat** Enterprise Linux hosts.
System Owner	The designated DDIS resource(s) responsible for the operational service of a device or devices.
Service Owner	The designated DDIS or Business resource(s) responsible for the operational delivery of business services underpinned by IT Infrastructure

Overview

The process of patch management has been developed worldwide over many years to ensure the safe implementation of operating system enhancements, bug fixes and security updates. Best practice recognises the following patch management steps:

- Discover and Assess
  - Feeds from Industry Sources
  - Internal Scans
  - Networking with Industry/Sector Peers
  - Internal Reviews
  - Assess Risk, Liaise with System Owners
- Identify and Test
  - Locate Devices
  - Liaise with System Owners
  - Obtain Patch or Vulnerability Detail/Software
  - Assess Implementation
  - Apply to Test Environment (If Possible)
  - Test Outcomes
- Evaluate and Plan
  - Assess Risk
  - Assess Test Implementation
  - Plan Deployment
  - Change Control
- Deploy and Remediate
  - Deployment direct to Device or Deployment Channel (SCCM, Satellite)
  - Test
  - Validate

Categorisation

It is recognised and accepted that not all vulnerabilities or patches have the same intrinsic priority for deployment. Some may be of a cosmetic nature or affect low risk systems/services whilst others will be critical to the continued operation of the University, often-remediating exposed security flaws or because of an attack or hacking elsewhere.

The University, through Digital and Information Services will employ the following sources of Information to ascertain the priority for implementation of patches or rectification of vulnerabilities:

1. Vendor Severity Rating – External Measure
2. Exploitability Index – External Measure
3. CVSS Score – External Measure
4. Institutional Impact Index – Internal Measure
5. Service Recovery Priority – Internal Measure

Policy

1. Vulnerability assessment and patching will only be carried out by designated roles. These roles are:
    a. Server Infrastructure Team – Assessment & Patching
    b. Network Infrastructure Team – Assessment & Patching
    c. Applications Management Team – Assessment & Patching
    d. Desktop Management Team – Assessment & Patching
    e. Audio Visual Team – Assessment & Patching
    f. Digital Research Services – Assessment & patching
    g. Data Centre & Monitoring – Assessment & Patching
    h. System Owners (Where not in the preceding teams) - Assessment
    i. IT Security Team - Assessment

2. All End User devices must be accurately listed in CART whilst all Server, Network and Appliance devices must be recorded in the Server Database.

3. Vulnerability scanning will have a minimum frequency of being run monthly. As the maturity of Institutional Scanning develops, the frequency of scans will increase in line with that maturity. Vulnerability reports will be distributed to the list in Appendix A within 2 working days of the end of scanning. The IT Security Manager is responsible for the efficient and effective running of scans to time and for the distribution of reports. The IT Security Manager is also responsible for the development of Scanning Maturity.

4. Threat Analysis will be undertaken by the IT Security Team, working with System Owners and Service Owners. The IT Security Team has responsibility for ensuring that threats are evaluated in a timely manner. Where necessary, due to risk or time, threats will be escalated to the Digital and Information Systems Senior Management Team for prioritisation.

5. Threat Analysis (Discover and Assess) will determine whether the Patch or Vulnerability Mitigation is progressed to implementation. Priority is determined using the attached Priority Schedule(s).

6. Patches and Vulnerability Mitigation packages must be obtained from the relevant vendor or other trusted source. Each package must be authenticated, and its integrity verified using the method provided by the source. Credible sources will always provide such an authenticity method such as MD5Sum, Digital Signature, Encrypted Certificate and finally, Internal Testing. No package must be deployed unless its authenticity has been established.

7. All devices must run the latest supported and patched versions of software prior to being released as a live service."

8. No RFC pertaining to patching or updates should be permitted to proceed without following the complete RFC process through to and including approval.

9. Manual patches and updates will be tested prior to implementation into any live (or representative) environment to avoid unacceptable side-effects. Where this is not possible, the relevant authority to proceed must be obtained from either the Service Owner or Assistant Director. This authority must be included in any Request for Change (RFC) as one of:
    - RFC Change Approval (SO or AD a member of the Change Accountable Board)
    - Copy of email approval embedded in the RFC
    - Free text approval included in the RFC.

10. A back-out or recovery plan that allows safe restoration to pre-patch state must be devised prior to any patch or update.

11. Patches will be applied according to the Digital and Information Services defined schedule and established patch windows or via Request for Change. These schedules are held within the distribution systems, SCCM and Satellite. Manual patching schedules are to be held and managed by the local teams responsible, i.e. Server Infrastructure Team, Network Infrastructure Team and Desktop Team.

12. Team audits must be carried out to ensure that patches and updates have been applied as required or notified by vendors and are functioning as expected. Team audits must be led by the respective Team Manager undertaken on at least a bi-annual basis. Outcomes of the audit must be reported to the IT Security Manager. Where it is identified that teams are unable to meet patching and update objectives, Team Managers should consult with the IT Security Manager for assistance with remedial actions.

13. Exceptions to this policy require formal documented approval from the Director, designated depute or relevant Assistant Director. Any device which does not comply with policy must have approved exceptions on record.

Monitoring

Compliance refers to the percentage of devices that have been successfully patched or otherwise remediated such that they are no longer vulnerable.

Compliance is recorded and maintained in a set of reports, produced by each responsible team and reported to the Operational Security Group. Key metrics are in turn reported to the Digital and Information Services Senior Management Team and the Information Governance Committee. Compliance status should be maintained by each team with reports presented to the Operational Security Group (OSG) which precedes the Information Governance Committee (IGC). The IGC Schedule is listed in Appendix B.

These Reports are found here:
https://365abdn.sharepoint.com/sites/instres/infosecurity/osg/Shared%20Documents/Restricted%20Circulation/Compliance%20Reporting

Compliance

Where non-compliance due to human or other factors are identified, the following actions should be taken:

- Review institutional and team processes and procedures
- Review staff skills and training

Any staff member found to have deliberately violated this policy may be subject to disciplinary action.

Guidelines and other Links

National Vulnerability Scoring Calculator	https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator
Common Vulnerability Scoring System	https://www.first.org/cvss/cvss-v30-specification-v1.8.pdf
CVSS Scoring Calculator	https://www.first.org/cvss/calculator/3.0
Vulnerabilities Reference Database	https://www.cvedetails.com/cvss-score-distribution.php
Patch Priority Schedule	Located in Policy Zone with this Policy

Review and Development

This policy shall be reviewed on an annual basis by the IT Security Team and, if required, recommendations for amendment made the Digital and Information Services Director. Recommendations for amendment will then be taken to the Information Governance Committee for approval.

Appendix A – Vulnerability Scanning Results Distribution

Role	Designated Contact
IT Security Manager	Garry Wardrope
Infrastructure Server Manager	Derek Dawson
Infrastructure Network Manager	Alastair Matthews
Desktop Manager	Ian Rowley
Data Centre Manager	Martin Fraser
Research IT Manager	Katie Wilde
Research IT Team Lead	Naveed Khan
Assistant Director (Service Management)	Ian Robotham or Designate
Assistant Director (Applications Management)	Richard Lynch or Designate
CISO	Via IT Security Team

Appendix B – Information Governance Committee Meeting Schedule

Month
February
April
June
August
October
December

Title	Vulnerability & Patch Management Policy
Author / Creator	Mark Marooth
Owner	Garry Wardrope IT Security Manager
Date published / approved	Approved June 2019 Published September 2019
Version	1.7
Date for Next Review	September 2020
Audience	All staff, partners, suppliers and contractors who work for or on behalf of the University and have responsibility for ensuring that IT Systems are patched.
Related	Conditions for using IT Facilities Information Security Policy Cyber Essentials +
Subject / Description	Purpose of this policy is to ensure that all University of Aberdeen IT Infrastructure is properly maintained and patched to minimise vulnerabilities and ensure the confidentiality, integrity and availability of the IT Infrastructure.
Equality Impact Assessment	N/A
Section	Digital and Information Services
Theme	IT Infrastructure Protection
Keywords	IT Infrastructure, Vulnerability, Patch, Vulnerability & Patch Management, Patch Schedule, Compliance, CVSS