Patching Policy

Contents

1 Introduction .................................................................................................................. 2
2 Scope .......................................................................................................................... 2
3 Policy statements ........................................................................................................ 2
   3.1 Types of IT Service patch ..................................................................................... 2
   3.2 Goldsmiths University IT Service patching prioritisation .................................... 3
4 Sanctions ...................................................................................................................... 3
5 Monitoring .................................................................................................................... 3
6 Exceptions .................................................................................................................... 3
7 Definitions ..................................................................................................................... 4
8 Related documents ....................................................................................................... 4
9 Related requirements ................................................................................................... 4
10 Review plan .................................................................................................................. 4
11 Revision history ......................................................................................................... 4

Ownership
Chief Information Officer

Contact
Information Security Manager

Protective Marking
Unclassified

Policy Unique ID
POL0001_Patching_v1.0

Last review date
March 2019

Next review date
March 2021
1 Introduction

1.1 Keeping IT operating systems and applications as up to date as possible is a vital activity in the prevention of loss of data or services due to an information security incident.

1.2 The process of applying software to any device is often generically known as “IT Service Patching”, which is typically to enhance functionality and protect against exploitation of identified security vulnerabilities.

1.3 Unpatched systems and applications are often a source of compromise, adversely affecting the Confidentiality, Integrity and Availability of Goldsmith’s data. Where possible, all Goldsmith’s systems and applications must be updated to the latest patch releases.

1.4 Security vulnerabilities are assessed using the Common Vulnerabilities Scoring System (CVSS) and consequently assigned a vulnerability rating of Critical, High, Medium or Low.

1.5 Identified vulnerabilities are not publicised until a similar rating of patch is issued, at which point they are made public both through disclosure by the vendor and via security lists such as those produced weekly by the National Institute of Science and Technology (NIST).

1.6 At the point a vulnerability is publicised, organisations utilising the vulnerable software must instruct systems administrators to patch their IT systems before all potential attackers exploit unpatched systems.

2 Scope

2.1 All Goldsmiths servers, workstations, network equipment, printers, scanners, devices and applications.

2.2 Out of scope of this policy are non-Goldsmiths owned equipment. However, it is strongly recommended this equipment is patched as up to date as possible.

3 Policy statements

3.1 Types of IT Service patch

3.1.1 Patch: minor adjustment to existing software.

3.1.2 Updates: potentially introducing significantly new software and functionality.
3.2 **Goldsmiths University IT Service patching prioritisation**

3.2.1 Patches if CVSS rating Critical (security related) should be kept completely up to date but must be within 15 days.

3.2.2 Patches if CVSS rating High should be within 15 days but must be within 30 days.

3.2.3 Patches if CVSS rating Medium and Low vulnerabilities must be installed within 30 days of availability, unless mitigating controls are in place to prevent the exploit being realised.

3.2.4 Updates to software should be maintained at least at the current -2 version.

3.3 Where specific procedures have been provided by IT&IS for patching different types of system i.e. servers, desktops, network equipment and applications they must be followed.

3.4 Patching of systems will be centrally managed wherever possible, unless there are clear business reasons for patching to be performed locally.

3.5 In certain instances, the severity of the potential or actual impact, may require the Information Security Manager mandate a shorter timeframe for any particular patch to be applied and communicate through appropriate channels.

4 **Sanctions**

4.1 Unpatched devices may be disconnected from the network and prevented from accessing Goldsmiths data and services if perceived as a significant risk to Goldsmiths data and services.

5 **Monitoring**

5.1 Goldsmiths will routinely monitor equipment connected to the network to identify non-compliant systems in accordance with the Information Security Policy and IT Service Patching Policy.

6 **Exceptions**

6.1 Some systems cannot be patched, either because they are end of life, rely on a precise software version, or are impossible to update. Exceptions must be reported to the Information Security Manager, who will assess the risk and advise if other controls can be employed.
7 Definitions

Patch: Minor software revision.
Update: Significant software revision.

8 Related documents

- Information Security Policy
- IT&IS Server Patching Procedure

9 Related requirements

- Goldsmith’s auditor reports
- Information commissioner's office - GDPR guidance
- National Cyber Security Centre - Cyber Essentials guidance
- International Standards Organisation - ISO27001 guidance
- University and Colleges Information Systems Association - Information Security Management Toolkit Edition 1.0 Volume 1

10 Review plan

10.1 This policy shall be updated regularly to remain current in the light of any relevant changes to UK law, Goldsmiths policies or contractual obligations and reviewed by the Information Security Steering Group at least every two years.

11 Revision history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Details</th>
<th>Author</th>
<th>Approved</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>07/03/19</td>
<td>Submitted to ISSG</td>
<td>Peter Hircock</td>
<td>Approved</td>
</tr>
<tr>
<td>1.0</td>
<td>11/11/19</td>
<td>Submitted to E&amp;IC</td>
<td>Peter Hircock</td>
<td>Noted</td>
</tr>
</tbody>
</table>