1 Introduction

1.1 Overview

Patching refers to the practise of applying updates to operating systems or applications. Patches typically enhance functionality and close identified security vulnerabilities. It is important, however, to distinguish *patches* from *upgrades*. Patches typically amend the existing code to a release; upgrades may introduce entirely new code. Consequently, LSE's Architecture Board recommends that upgraded software is maintained *at least* at the current -1 upgraded version, while patches (often known formally as security releases) should be kept completely up to date.

1.1.1 Patching and security vulnerabilities

Identified security vulnerabilities are assessed using the "Common Vulnerabilities Scoring System" (https://nvd.nist.gov/cvss.cfm) metric, and consequently assigned a vulnerability rating using the "NVD Vulnerability Severity Ratings"[i] of 'High', 'Medium' or 'Low'.

Identified vulnerabilities are typically kept quiet until a patch is issued, at which point they are made public both through disclosure by the vendor and via lists such as are produced weekly by US-CERT's National Cyber Awareness System.

At the point a vulnerability is considered 'known', both by attackers seeing weaknesses in systems, and by organisations utilising the vulnerable software. Patching therefore becomes a race between attackers looking to exploit unpatched systems and systems administrators seeking to protect them.

Unpatched systems and applications are often a source of compromise, adversely affecting the Confidentiality, Integrity and Availability of LSE data.

Where it is possible, all LSE systems and applications must be updated to the latest patch releases.

1.2 Scope

All LSE systems, servers, workstations, devices and applications.

1.3 Out of Scope

LSE has no mandate to require that personally-owned devices are kept up to date. Unpatched personally-owned devices may, however, be blocked from accessing segments of LSE's network that contain sensitive data.

[i] "1. Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0-3.9. 2. Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9. 3. Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0."
From 'NVD Common Vulnerability Scoring System' https://nvd.nist.gov/cvss.cfm [accessed 11/10/16]

ISAB comprises representatives from all relevant parts of the organisation. It shall oversee the creation of information security and subsidiary policies.

The Information Security Manager will determine the appropriate levels of security measures applied to all new information systems.

3 Responsibilities

System Owners
Ensuring patching takes place or otherwise notifying Information Security that patching cannot take place.

Components of a system (e.g. a centrally-managed Operating System, or centrally-managed applications) may have the practise of patching devolved to another team (e.g. IMT systems) but the responsibility of maintaining patching remains with the system owner.

LSE-owned Laptop / Smartphone operators
Ensuring patching of operating system and applications takes place

Department of Information Management and Technology:

- Patching centrally-managed systems and applications.
- Posture checking and network quarantining as appropriate
- Recording unpatched systems
- Removing and / or quarantining noncompliant systems as appropriate

Research Lab
Responsible for the managed patching of RLAB servers, workstations and laptops.

Information Security Advisory Board
Responsible for the advising on and recommending information security policies to the Information Technology Committee, assessing information security risks, identifying and implementing controls to risks.

Information Technology Committee
Responsible for approving information security policies.

Document control

Distribution list

Name	Title	Department
Information Security Advisory Board		
Information Technology Committee		

External document references

Title	Version	Date	Author
Information Security Policy	3.12	06/10/16	Jethro Perkins
Information Classification Standard	3.0	15/03/13	Jethro Perkins

Version history

Date	Version	Comments
	0.1	Initial version
	0.2	Distributed to Architecture Board members.
	0.3	Incorporating amendments from Head of Infrastructure. Distributed to Nic Warner. Updated STICERD to Research Lab
	0.4	Incorporating amendments from the Applications Architect.
09/12/16	1	Policy approved by Information Technology Committee and moved to release.

Review control

Reviewer	Section	Comments	Actions agreed
Chris Roberts, Head of Infrastructure	2.1, 2.3, 2.4, 3	30 days may be too long for critical patches. Rename “endpoints” to “devices”. Explain BMS/SCADA. Can system owners devolve patching responsibility?	Amend 30 days. Rename endpoints. Explain SCADA. Outline that systems owners can devolve practise but not ultimate responsibility for patching.
Michael D’Urso, Applications Architect	1.0	Distinguish between patches and upgrades. Point out that upgrades should be kept at current -1, whereas patches should always be applied.	Amended as requested.