Information Services Division

ISD Server Vulnerability Management Policy

Author: Bridget Kenyon

Date: 9 Jun 2017

Version: 1.0

Review/Revision History

This document shall be reviewed annually or more frequently if required, e.g. following changes to related requirements, or to related documents.

Revision No.	Revision Date	Summary of Changes	Who	Changes marked
1.0	9 Jun 2017		Bridget Kenyon	N/A

Approvals

This document requires the following approvals

Name	Signature	Title	Date of Issue	Version
Mike Cope		Director, ISD		1.0
James McCafferty		Director of IT Service Delivery, and Deputy Director of ISD		1.0
Bridget Kenyon		Head of Information Security		1.0

Distribution

This document has been distributed to:

Name	Date of Issue	Version
Mike Cope	9 Jun 2017	1.0
James McCafferty	9 Jun 2017	1.0
Andrew Dawson	9 Jun 2017	1.0
Paul Lamb	9 Jun 2017	1.0
Bridget Kenyon	9 Jun 2017	1.0

Contents

1. Introduction

ISD servers provide many fundamental services to UCL, such as HR management, financial management and online training courses. UCL relies upon these servers, and it is important that they are not compromised by attackers. ISD servers also contain sensitive information which must be protected from loss and inappropriate disclosure. A server with any unmanaged vulnerabilities may be compromised by attackers and damaged or misused; the data held on it may be held to ransom, stolen or made public.

This document describes how ISD shall manage security vulnerabilities on servers for which it is responsible.

2. Scope

This policy applies to:

- Any server that ISD manages[1] or is responsible for, including servers which are managed by third parties on behalf of ISD.
- Any software on these servers. In this document, "software" shall be taken to include firmware, BIOS, hypervisor, operating system, driver, library, middleware, application, service, and other digital capabilities.

3. Dependencies

Documents which rely upon this policy:

- Vulnerability Management Guidance for ISD servers.

Documents which this policy relies on:

- UCL Policy on Connecting Equipment to the College Network https://www.ucl.ac.uk/informationsecurity/policy/public-policy/Connection
- UCL Information Security Policy https://www.ucl.ac.uk/informationsecurity/policy/public-policy/Policy

4. Related requirements

The UCL Network Connection Policy Clause 1.7 requires all UCL network-connected systems to be supported and up to date with security patches (updates).

The Data Protection Act Principle 7 states that "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data…".

5. Stakeholders

The following roles, or their nominated representatives, should be involved in the review of this document.

- Head of Information Security
- Head(s) of ISD Server Management team(s)
- Service Owner(s) for Server Service(s)
- Chair of Security Working Group

[1] Including maintenance, upgrades, etc.

6. Accountable Roles

Department Heads shall ensure that servers and/or software which are managed by their staff are compliant with this policy.

Service Operational Managers shall ensure that servers and software which support their service are compliant with this policy, but may delegate operational activities to members of their Service Virtual Teams.

Service Operational Managers will ensure that the responsibilities of System Custodians as defined within the Information Security Policy, secondary policies and guidelines will be met.

Service Owners are ultimately accountable for the security of their service.

7. Definitions

See Glossary.

8. Policy statements

1. Servers shall only run currently vendor- or developer-supported software.

8.1. Monitoring

2. Service Owners shall regularly monitor the security status of their servers and/or software, including patch status, and shall use this information, along with information on mitigations in place, to update their Service Information Risk Registers.
3. Information from internal scanning, manufacturers/suppliers and/or trusted source(s) shall be used to identify vulnerabilities.

8.2. Vulnerability scanning

4. An automatic vulnerability scanning system will be operated by an independent group and will provide regular updates of identified vulnerabilities to the SOM for the service.

8.3. Mitigation

5. Within 30 calendar days of a vulnerability being identified by UCL (including through the release of a patch), either a suitable mitigation shall be applied or a dispensation be formally approved in writing by the Information Security Group. Where the risk is deemed to be very high (e.g. where attacks on UCL are known to be plausibly imminent or taking place) then the vulnerability must be addressed swiftly.
6. A security patch is the preferred approach to mitigate a vulnerability. Any security patches that cannot be applied within 20 calendar days of release must be escalated to Director of Service Delivery with an explanation about why the patch cannot be applied and a recommended course of action.
7. Where patching is not possible or not feasible, a risk-based approach (using UCL Information Risk Assessment processes) shall be used to identify the suitable alternative approach to manage a vulnerability. This may include physical or logical separation from network connectivity if no other option is available.
8. Vulnerabilities which cannot be mitigated to an acceptable level of risk shall be promptly escalated to the relevant Information Owner, and to their SIRO as required, with proposed options for resolution.

8.4. Review

9. Alternative approaches to manage a vulnerability shall be reviewed regularly to ensure that they remain suitable and effective.

9. Sanctions

This policy statement does not form part of a formal contract of employment with UCL, but it is a condition of employment that employees will abide by the regulations and policies made by UCL.