

Threat and Vulnerability Management Policy

Table of Contents

1. Purpose.....	3
2. Scope.....	3
3. Policy Statement	3
4. Roles and Responsibilities	3
5. Vulnerability Risk Levels.....	4
6. Asset Register.....	4
7. Vulnerability Management.....	5
7.1. Generalities	5
7.2. Testing and Scanning.....	6
7.3. Response to Results	6
8. Patch Management	7
8.1. Generalities	7
8.2. Sourcing Information on Threats, Vulnerabilities and Patches.....	8
8.3. Patch Exemptions	8
8.4. Identifying Patch Priorities	8
8.4.1. Patch Risk Level.....	9
8.4.2. Relevance of Impacted Systems	9
8.4.3. Patch Priority	9
8.5. Testing Patches	10
8.6. Production Implementation of Patches	11
8.7. Emergency Patches	11
8.8. Operating System and Application Major Version Upgrades	11
8.9. End-of-Life Operating Systems and Applications.....	11
9. Cloud Services	12
10. Metrics and Reporting	12
11. Policy Review Date	12
12. Document Control	13
12.1 Document Revision History	13

1. Purpose

- 1.1. The purpose of this policy is to specify and communicate the requirements for vulnerability and patch management, for all of The Open College of the Arts (OCA)'s IT network devices and systems.

2. Scope

- 2.1. This policy applies to all software components that are used by the OCA on all IT network devices and systems¹, including systems hosted in the cloud.

3. Policy Statement

- 3.1. The OCA's policy in regard to vulnerability and patch management is as follows:
 - The OCA shall regularly monitor threat, vulnerability and security patch information published by vendors and other recognised security industry sources.
 - Vulnerabilities shall be identified and managed using a formal, regular programme of vulnerability scanning and penetration testing, supported by appropriate tooling and including testing by trusted third parties.
 - The implementation of software security patches shall be managed in a structured and controlled way to ensure that the OCA is constantly protected against the impact of software vulnerabilities.
 - Patches shall be applied within timeframes commensurate to the vulnerability risk level and the relevance and data classification of the impacted systems and data.
 - Where the OCA uses cloud services, responsibilities for vulnerability and patch management shall generally be shared with the cloud service providers, with the split of responsibilities documented in contractual terms.

4. Roles and Responsibilities

- The IT Manager is responsible for this policy and shall ensure that this policy is up-to-date and relevant.
- Information Security is responsible for continually assessing the latest threats, vulnerabilities and security patch requirements using security industry recognised sources and relevant vendor sources.
- The IT Department is responsible for addressing vulnerabilities and applying security patches in line with analysis and direction provided by the IT Manager.

¹ Where relevant, software also includes firmware.

- Where relevant, business system owners are responsible for ensuring that security vulnerabilities are removed and security patches are applied to the systems that they are responsible for, e.g. application and database servers.
- Where the OCA uses cloud services, split responsibilities for vulnerability and patch management shall be established in contractual terms. (See section 9 for details.)

5. Vulnerability Risk Levels

- 5.1. Vulnerabilities shall be categorised with a risk level based on likelihood and potential impact, using a 3-point scale: High, Medium and Low.
- 5.2. Tools used by the OCA for vulnerability scanning may have their own built-in criteria for assigning vulnerability risk levels. Where that is the case, those criteria can in practice be used directly by the OCA. The table below should therefore only be used in cases where a rating provided by a vulnerability scanning tool seems inaccurate for the OCA systems that could be impacted – either in terms of likelihood or potential impact.

Risk	Description
High	The vulnerability is easily exploitable, widely known and/or it has a high impact on systems affected or the overall network infrastructure. There could be potential malware infection or significant damage to data, the network and computer systems.
Medium	The vulnerability requires some skill, software or tools to exploit it, is less widely known or understood and/or it has a medium level of impact on affected systems. There is likely to be no malware infection, though there may be some limited (but not overly significant) damage to data, the network and computer systems.
Low	The vulnerability is difficult to exploit, is partially addressed by other security mechanisms and/or has a low or negligible impact on affected systems. There is no immediate threat to data, the network and computer systems.

6. Asset Register

- 6.1. The IT Department shall maintain an up-to-date asset register of all information and IT assets that belong to the OCA. This register shall include all the appropriate information to support vulnerability and patch management. See the [Asset Management Policy](#) for more information.

7. Vulnerability Management

7.1. Generalities

- 7.1.1. Security effectiveness shall be tested and measured through a formal and regular programme of vulnerability scanning and penetration testing. This

shall only be conducted either by designated Information Security personnel or by a trusted and certified third party².

- 7.1.2. Prior to scanning / testing, discussions shall be held with the business and system owners regarding:
- Scope and level of intensity of the scanning / testing activity, from a basic assessment to complete exploitation and information gathering;
 - Whether it will be conducted by the OCA or a third party company;
 - The requirement to keep knowledge of the scanning / testing activity appropriately restricted;
 - Planning and agreement to minimise disruptions to business processes;
 - Creation of an informed stakeholders list to ensure penetration testing does not affect or alert other parts of the business unintentionally, who will be updated at the beginning of the test, and advised of any issues / critical risks identified during the test;
 - Creation, both for applications and operating systems service packs/patches, of a current and updated target test environment and/or access to the live environment with appropriate approvals such that any testing and assessment is relative to the target in the live platform and service connections thereof;
 - The requirement for any testing which is intended to address or emulate Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks to be:
 - Clearly documented;
 - Only executed against the OCA or third party infrastructure with prior approval from appropriate stakeholders and subject to third party constraints where appropriate.
- 7.1.3. Vulnerabilities discovered outside of the regular programme of vulnerability scanning and penetration testing shall be reported and responded to as information security incidents, in accordance with the Information Security Incident Response Policy.
- 7.1.4. It shall be ensured that the tools used by the OCA for vulnerability scanning are regularly updated with the latest threat signatures and indicators of compromise.
- 7.1.5. The OCA shall maintain contact with special interest groups or other specialist security forums and professional associations, as a means to receive early warnings of alerts, advisories and patches pertaining to threats, attacks and vulnerabilities.

² For certified suppliers of penetration testing and scanning services, see the [NCSC Check scheme](#) and [PCI ASV](#) web pages.

- 7.1.6. Relevant information about the efficacy of the vulnerability and threat management processes shall be shared where appropriate, both with internal stakeholders and with peer organisations.

7.2. Testing and Scanning

- 7.2.1. Penetration testing and vulnerability scanning of business-critical systems shall be conducted by a trusted third party on, at least, an annual basis and after any significant change.
- 7.2.2. Where penetration testing and vulnerability scanning is conducted by a third party, the following specific requirements shall be met:
- All tests and scans shall be agreed by management together with a formal document of authorisation. The aim, scope and methods of the testing and scanning shall be clearly defined within the document.
 - Any accesses required to meet the scope of the test shall be approved beforehand.
 - Any equipment that is added to the network shall be approved by stakeholders and network operational management beforehand. (IT Infrastructure management may reject the installation of equipment if it is considered to place the operational environment stability at risk and shall facilitate a new design with the third party which meets the required scope, security and stability requirements).
 - Designated Information Security personnel shall have access to all the testing / scanning activity.
 - A formal debrief shall be provided by the third party to all relevant personnel.
 - The third party shall provide a deliverable that includes solutions for the vulnerabilities identified.
 - Penetration testing shall only be performed by accredited personnel.
 - Where a third party wishes to assess or perform a penetration test of the OCA's infrastructure and/or services, this shall only be done with prior approval from the IT Manager.

See also:

- [Network Security Policy](#);
- [Access Control Policy](#).

7.3. Response to Results

- 7.3.1. Results from penetration testing and vulnerability scanning shall be evaluated and appropriate measures taken to address the associated risk, as follows:

- The results shall be securely communicated to the system owners and/or the relevant IT teams, as applicable, to facilitate identifying a fix for the software³ and when/how it can be implemented.
- A root cause analysis shall be performed, to evaluate the underlying issues that cause vulnerabilities in code and allow development teams to do more than just fixing individual vulnerabilities as they arise.
- The vulnerabilities identified shall be addressed following the information security risk management process.
- If a system or application is deemed to be high risk, the execution of additional tests shall be considered.
- Identified high risks may require remedial action such as patching or the turning off / removal of services affected by the vulnerability.
- Any remedial actions shall be implemented in accordance with the [Change Management Policy](#).
- Where a vulnerability cannot be resolved, alternative risk treatment actions or compensating controls shall be implemented.
- Where possible, remediation of identified vulnerabilities shall be automated.

8. Patch Management

8.1. Generalities

8.1.1. The implementation of software security patches shall be managed in a structured and controlled way to ensure that the OCA is constantly protected against the impact of software vulnerabilities. Patching also encompasses implementation of routine service packs.

8.1.2. The following requirements shall be met:

- All patch implementations shall be done in accordance with the [Change Management Policy](#).
- All patches shall be sourced from the vendors and verified as being legitimate by methods such as checksum matching.
- Where patches are downloaded automatically, the update mechanism shall use methods to ensure the authenticity of the patches received, including but not limited to secure transport, checksums and digital signatures. Shall any of these checks fail the patch download shall be rejected.
- Relevant and necessary security patches shall be identified on a continual basis. For assessment and prioritisation, vulnerabilities shall be assessed in terms of risk and criticality of the affected systems.

³ Including, where applicable, vulnerabilities identified in external libraries used by applications.

- Security patches shall be tested in a controlled environment to ensure that they do not undermine the functionality and security of the OCA network infrastructure and systems.
- Security patches shall be approved and rolled out to all relevant network components and systems within an appropriate time, commensurate to the assessed risk levels.
- Software that is no longer supported and maintained by the vendor shall not be used, given that patches and service packs will cease to be available.
- The integrity of security patches shall be verifiable against a trusted source.
- Mechanisms shall also be implemented to ensure that, where relevant, mobile devices are updated with the latest patches as soon as they connect to the OCA network infrastructure.

8.2. Sourcing Information on Threats, Vulnerabilities and Patches

8.2.1. The OCA is primarily dependent on external sources to obtain information about security threats and vulnerabilities, and particularly on the vendors of its network and systems software components to provide timely information about new security patches. Therefore, the OCA shall:

- Regularly monitor threat, vulnerability and security patch information⁴ published by vendors and other well recognised information security industry sources;
- Ensure that service providers allocate appropriate resources to regularly check for new security patches for the relevant software components⁵;
- Ensure that all formal notifications are received from each vendor, e.g. via subscription services; this shall be done by providing relevant Information Security personnel with regular updates, e.g. via a 'group' e-mail account set up for this specific purpose; the mechanism implemented shall ensure that any staff absences, e.g. due to holidays or sickness, do not degrade or delay the ability to regularly check for new security patches;
- Analyse the information collected about threats to produce threat intelligence, which can then be used in risk assessment and threat modelling activities⁶.

8.3. Patch Exemptions

8.3.1. Patches shall only be applied to software functions, utilities, services and protocols that are in use. There may also be situations where patches need not be applied for one or more of the following reasons:

⁴ Including cloud security vulnerabilities.

⁵ For example, for Microsoft patches which are released on a monthly basis.

⁶ See the [Information Security Risk Management Policy](#) and the [Systems Acquisition, Development and Maintenance Policy](#).

- The patch is not relevant to the network infrastructure and systems;
- The patch is not compatible with the technical infrastructure;
- The patch will have a significant negative impact on the OCA operations;
- The OCA has implemented a change freeze.

8.3.2. In all circumstances, such exemptions shall be subject to a risk assessment, discussed with the IT Manager, recorded and approved.

8.4. Identifying Patch Priorities

The following approach shall be used to consistently identify important and necessary security patches, based upon:

- Risk level – how vulnerable the OCA is if security patches are not applied;
- Relevance of the impacted systems (in terms of sensitivity / criticality).

8.4.1. Patch Risk Level

- 8.4.1.1. For each patch, the risk of not applying it shall be evaluated, based on the risk level of the corresponding vulnerability, as per the categories defined in section 5 above.
- 8.4.1.2. Information Security shall maintain a register of all identified patches and associated risk assessment, including the following elements:
 - Patch ID (unique);
 - Patch description;
 - Risk level (High / Medium / Low);
 - Whether the patch is exempt (Yes / No), and reasons for exemption where applicable.

8.4.2. Relevance of Impacted Systems

- 8.4.2.1. As well as the risk level of the vulnerability associated with each patch, the relevance of the impacted network components and systems (in terms of sensitivity / criticality) shall also be taken into account when determining priorities for patch implementation. As a general rule, the following applies, although exceptions can be considered:

- **Relevance 1:**
 - Firewall devices;
 - Externally accessible systems;
 - Internet facing systems;
 - Business critical applications;
 - Database servers;
 - Domain controllers;

- **Relevance 2:**

- Other internal servers and network devices;
- User PCs, laptops and mobile devices.

8.4.3. Patch Priority

8.4.3.1. The following matrix defines the patch priority according to risk level and system relevance:

Patch Priority	System Relevance	
Risk	Relevance 1	Relevance 2
High	High priority	High priority
Medium	High priority	Medium priority
Low	Medium priority	Low priority

Note: A lower priority as defined in the above table does not mean that the patch shall not be implemented. Rather, it defines the relative urgency in terms of the timing of patch implementation.

8.4.3.2. The chosen mechanism for selecting and implementing patches shall be able to record the systems and priorities associated with each required patch.

8.5. Testing Patches

8.5.1. The following requirements shall be met:

- Patches shall be tested before being rolled out to production systems to ensure that the patches:
 - Are compatible with existing software;
 - Are free from malware;
 - Do not cause security solutions to generate a false positive or see them as malicious / alert against them;
 - Do not negatively impact on the functionality and security of the network infrastructure and systems.
- Testing requirements shall be decided on the basis of the perceived level of risk in the application of the patch, the criticality of the systems affected and the urgency in terms of the likelihood of exploitation if the implementation of a patch is delayed.
- The change management process shall be formally applied as appropriate, including impact assessment and formal sign-off for patch implementation, and keeping records of the outcomes of the tests executed.

- In line with the change management process, testing shall, as much as practical, be carried out in a segregated test environment.
- The testing shall also establish the roll-back process for the patch. In simple cases, this might be to uninstall the patch. However, some updates (e.g. Windows service packs or router firmware updates) may require a full rebuild. Any roll-back facilities included with a hot fix, firmware or service pack shall be tested before implementing the fix into production.

See also:

- [Change Management Policy](#).

8.6. Production Implementation of Patches

8.6.1. The process for selecting and implementing patches shall include recording the intended and actual dates of patch implementation per system. Timeframes for implementing patches into production according to priority – see subsection 8.4.3 above – shall be established. The following timeframes shall be considered as a guideline:

Patch Priority	Timeframe
High	30 days
Medium	60 days
Low	90 days

8.7. Emergency Patches

8.7.1. Emergency patches are sometimes issued in cases where a vulnerability that poses an imminent threat has been identified. In such cases, the patch implementation shall be treated as an emergency change and fast tracked, as described in the [Change Management Policy](#). In all instances:

- Testing of the patch shall be done before implementation and documented for auditing and tracking purposes.
- A risk assessment and deployment of an emergency patch shall be done within 3 days of availability to the impacted system(s).

8.8. Operating System and Application Major Version Upgrades

8.8.1. Vendors will regularly update their operating systems and applications bringing new functionality to their products but also engineering new ways to increase performance, to mitigate risks or threats and to provide more effective logical interfaces enabling information security vendors to have the necessary programmatic access to the system architecture to detect and mitigate threats and/or vulnerabilities.

8.8.2. The relevant business owners within the OCA shall ensure that, wherever possible, the versions of operating systems and applications are maintained at a minimum of N-1 for major operating system and application

releases (i.e., the version in place shall be either the latest released major version or the one immediately before that, but not an older version).

8.9. End-of-Life Operating Systems and Applications

- 8.9.1. The OCA should not run any end-of-life operating systems or applications⁷ in a production environment.
- 8.9.2. Where this is unavoidable for a given operating system and/or application, Information Security shall perform a risk assessment and vulnerability testing and document it for auditing, mitigation and tracking purposes. Additional threat mitigations shall be applied and regularly tested to ensure that the system is not vulnerable. Where feasible, the system should be moved to a segregated sub-set and internet access removed.
- 8.9.3. The relevant business owners shall be accountable for extended support, and for justifying the acceptance of the risk in maintaining the system, against options of updating or replacing it with a supported solution.

9. Cloud Services

- 9.1. Where the OCA uses cloud services, the responsibilities for vulnerability and patch management can be shared between the cloud service provider (CSP) and the cloud service customer (CSC), in line with the Shared Security Responsibility Model.
- 9.2. The split of responsibilities for vulnerability and patch management may vary depending on the delivery model of the cloud services consumed by the OCA. At the infrastructure and virtualisation levels, those responsibilities shall generally sit with the CSP; at other levels, the following applies:
 - In the case of Infrastructure as a Service (IaaS), those responsibilities shall generally sit with the CSC;
 - In the case of Software as a Service (SaaS), those responsibilities shall generally sit with the CSP;
 - In the case of Platform as a Service (PaaS), those responsibilities shall generally sit with the CSC at the application level, but with the CSP at the middleware and host levels.

In all cases⁸, the split of responsibilities shall be clearly documented in contractual terms.

10. Metrics and Reporting

- 10.1. Relevant metrics for vulnerability and patch management shall be defined, and regularly obtained and reported to the Finance, Employment, Audit and Risk (FEAR) Committee and The OCA Board as appropriate.

⁷ Including any software that is no longer supported and no longer receives regular updates for security problems.

⁸ Including other cloud computing service models, if used by the OCA.

- 10.2. Analysis of metrics shall be used to assess the efficiency of the vulnerability and patch management processes and continuously improve them.

11. Policy Review Date

- 11.1. This policy shall be reviewed and appropriately updated on an annual basis. It shall also be reviewed and appropriately updated when there are any changes to relevant regulations on information security and/or data protection.

12. Document Control

Document Control	
Title:	Threat and Vulnerability Management Policy
Reference:	
Version:	1.0
Date:	
Status:	Draft
Owner:	IT Manager
Classification:	Internal

12.1 Document Revision History

Version	Date	Author	Summary of changes
0.1			Initial draft
1.0	06/11/2025	Dean Humphreys	Final revisions approved and version updated to 1.0 for release