

Secure Software Development Policy

Table of Contents

1. Purpose.....	3
2. Scope.....	3
3. Policy Statement	3
4. Roles and Responsibilities	4
5. Requirements Management	5
6. Change Management.....	6
7. Software Development	6
7.1. Security in the Software Development Life Cycle	6
7.2. Segregation of Environments	8
7.3. Software Documentation	8
7.4. Open-Source Code	9
7.5. Outsourced Development.....	9
7.6. Software Developed for Use by Third Parties	9
7.7. Training.....	10
8. Testing	10
9. Deployment.....	11
10. Protection of Source Code	12
11. Intellectual Property.....	12
12. Third Party Software.....	13
12.1. Generalities	13
12.2. Restrictions on Changes to Third Party Software Packages.....	13
13. Hardware	14
14. Disposal of Systems.....	15
15. Metrics and Reporting	15
16. Policy Review Date	15
17. Document Control	16
17.1 Document Revision History	16

1. Purpose

The purpose of this policy is to ensure that appropriate controls, including information security controls, are applied throughout the life cycle of all the Open College of the Arts (OCA) information systems, whether developed in house, by third parties or purchased off the shelf or via cloud services for internal production.

2. Scope

This policy covers the life cycle of all information systems within the OCA, from acquisition through to disposal, including development and maintenance. Both hardware and software components are in scope, although some of the requirements of the policy are specifically applicable to software components only.

This policy applies to all the OCA staff, including contractors and other third parties, who are involved in the acquisition, development or maintenance of the OCA's information systems.

3. Policy Statement

The OCA's policy in regard to acquisition, development and maintenance of information systems is as follows:

- All systems acquired or developed for use by the OCA shall be secure by design.
- Functional and non-functional requirements, including information security requirements, shall be defined and documented for new business information systems or enhancements to existing ones.
- All changes to systems, including implementation of new systems, shall be authorised, controlled and recorded.
- Secure development best practices shall be followed across all stages of the software development life cycle (SDLC).
- Regular reviews of approved developments shall be conducted to verify their progress and suitability for continuation, including progression between stages.
- Secure coding techniques shall be used for both new applications and enhancements to existing applications.
- All development and testing activities shall take place within environments suitably separated and secured from production systems.
- Platform components shall always be configured securely, and system hardening shall be implemented to minimise security vulnerabilities.
- Only software approved by the OCA shall be installed on the OCA devices.
- All approved third-party software installed on the OCA devices shall be appropriately licensed.
- Information systems shall always be kept up to date with respect to security patches.
- Prior to deployment, any new or modified systems shall be fully tested, including testing of information security requirements.

- System test data shall be appropriately protected and, where required, anonymised.
- Access to program source code, build and configuration documentation and files shall be controlled.
- Any outsourced software development and services shall be appropriately managed.
- Intellectual property shall be adequately protected.
- Systems shall be decommissioned and disposed of securely at their end of life.

4. Roles and Responsibilities

- The IT Manager is responsible for this policy and shall ensure that this policy is up-to-date and relevant.
- The IT Team are responsible for the validation of information security requirements.
- The Data Protection Officer (DPO) is responsible for the validation of data protection requirements.
- Line managers are directly responsible for implementing this policy within their functions/departments, and for adherence by their staff.
- All the OCA staff, including contractors and other third parties, who are involved in the acquisition, development or maintenance of the OCA's information systems shall adhere to this policy.
- See the [Change Management Policy](#) for the roles and responsibilities related with change management.

5. Requirements Management

- 5.1. Requirements for new systems and changes to existing systems shall be identified, analysed, documented and formally managed from the early stages of the SDLC, and throughout the whole life cycle.
- 5.2. Aside from other business requirements, both functional and non-functional, information security requirements shall be considered in all new systems and changes to existing systems. These include requirements for compliance with the OCA's policies and applicable regulations, including but not limited to:
 - Access control requirements;
 - Information classification and handling requirements;
 - Logging and monitoring requirements;
 - Cryptographic requirements;
 - Data protection requirements;
 - Application interoperability and portability requirements, including:
 - Communications between application interfaces;
 - Information processing interoperability;
 - Application development portability;
 - Data exchange, usage, portability, integrity, and persistence;
 - Infrastructure and virtualisation requirements;
 - Segmentation, segregation and (where applicable) multi-tenancy requirements.

- 5.3. Information security requirements that should be considered for all systems shall be identified, documented and used as a basis for the specification of requirements applicable to specific new systems or changes to existing systems.
- 5.4. Requirements shall be validated by appropriate stakeholders from the relevant business functions across the OCA. In particular:
 - Data protection requirements shall be validated by the DPO.

Traceability of requirements to design, build and testing shall be maintained across all stages of the SDLC.

6. Change Management

- 6.1. All changes to systems, including implementation of new systems, shall be formally approved and controlled, in line with the [Change Management Policy](#).
- 6.2. As part of the change management process, all changes shall be subject to risk assessment – including the assessment of information security risks.
- 6.3. When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organisational operations or security.
- 6.4. Any changes that could have a data protection impact shall be subject to a Data Protection Impact Assessment (DPIA).

7. Software Development

7.1. Security in the Software Development Life Cycle

Information security shall be considered across all stages of the Software Development Life Cycle (SDLC):

- Planning and Analysis:
 - Information security requirements, to ensure compliance with the OCA's information security policies and applicable regulations, shall be defined, analysed and documented before software development begins.
 - Information security requirements shall be validated:
 - By the IT Team;
 - Where involving personal data, by the DPO;
 - By relevant stakeholders from other business functions, as applicable.
 - The analysis of requirements shall include the assessment of associated information security risks.
- Design:
 - Information security requirements shall be appropriately incorporated into the system design.

- Threat models shall be used to identify key system interfaces, data flows, threats and countermeasures.
 - Applications and databases that use access controls to protect confidentiality and integrity of data shall comply with the [Access Control Policy](#).
 - Where relevant, encryption techniques shall be used to protect the confidentiality and integrity of data, in line with the [Cryptographic Controls Policy](#).
 - Applications and databases that process personal data shall be designed to enable compliance with data protection regulations; this shall include appropriate mechanisms for effective disposal of personal data and to address data subject requests.
 - Applications and databases shall be designed with appropriate logging and auditing capabilities, in line with the [Logging and Monitoring Policy](#).
 - Secure configuration shall be incorporated into the system design.
 - Consideration shall be given, in the design, to the use of data masking, anonymisation or pseudonymisation techniques to protect data that should be hidden from (some) users.
 - Where feasible:
 - Existing, well-secured software shall be reused (either created in-house or acquired from third parties), instead of duplicating functionality;
 - Support for using standardised security features and services (e.g., integrating with log management, identity management and access control) shall be built into the system instead of creating proprietary implementations of such features and services.
- Build:
 - Information security requirements shall be appropriately incorporated into the system build.
 - Secure coding principles and techniques shall be applied, aligned to industry best practices.
 - Software developers shall be familiar with threats and vulnerabilities guidelines published by recognised sources¹ and check them regularly for updates.
 - Tools and libraries used in software development shall be compliant with the OCA's information security policies.
 - Approved static code analysis tools shall be regularly used to scan source code for known vulnerabilities.
 - Code reviews shall be:
 - Conducted regularly, by individuals knowledgeable in code review techniques and secure coding practices and who have not been involved in the development of the code being reviewed;
 - Evaluated against OWASP vulnerabilities;
 - Appropriately documented.

¹ Including the Open Web Application Security Project (OWASP) and the Build Security in Maturity Model (BSIMM).

- The use of open-source code shall be restricted and appropriately controlled – see subsection 7.4 below for more information.
- Outsourced development shall be appropriately controlled – see subsection 7.5 below for more information.
- Testing:
 - All information security requirements shall be subject to testing; see section 8 below for more information.

The requirements above also apply in the case of outsourced development; see also subsection 7.5 below.

Version control, configuration baselines and other configuration management techniques shall be applied to all software development.

7.2. Segregation of Environments

Environments used for development and testing shall be segregated from production environments but shall provide the same degree of security as the latter, in terms of access control and system configuration.

Software developers and test analysts shall not have access to production environments.

7.3. Software Documentation

Software documentation shall be created, and kept up to date, for all systems developed by or for the OCA, including but not limited to:

- Requirements documentation;
- Design documentation (high-level and low-level);
- Data flow documentation to identify what data is processed, stored or transmitted where;
- Technical specifications for configuration (including security configuration) and operation;
- User manuals.

All software documentation shall be:

- Stored in appropriate repositories with access restricted to designated individuals on a 'need to know' basis, in line with the [Access Control Policy](#);
- Backed up;
- Subject to version control.

An inventory of all software components used by the OCA in the development of applications shall be created and kept up to date by the relevant teams.

7.4. Open-Source Code

Use of open-source code in the development of solutions can bring a number of benefits but entails risks that shall be appropriately managed. The following requirements shall be met:

- Only open-source code of reputable origin shall be considered for use in applications developed by or for the OCA.
- The open-source licence shall not put the OCA under the obligation to disclose any code which could expose or highlight any security controls or mechanisms implemented by the OCA.
- Open-source code libraries shall be assessed and tested before being rolled out in the development of applications to ensure that they:
 - Are current and compatible with the existing software;
 - Do not negatively impact on the functionality and security of the network infrastructure and systems;
 - Are free from malware;
 - Do not cause security monitoring solutions in place to see them as malicious / generate false positive alerts.
- Updates required for applications which use open-source libraries shall be identified and applied, in line with the [Threat and Vulnerability Management Policy](#).
- All open-source code libraries used by the OCA shall be appropriately documented, inventoried and managed.

7.5. Outsourced Development

In circumstances where software development is outsourced to a third-party, the following requirements shall be met:

- The third party shall be subject to the supplier management process as defined in the [Third-Party Vendor Management Policy](#).
- Third party custom software development shall comply with this policy, and this shall be confirmed in contractual terms.

7.6. Software Developed for Use by Third Parties

Software developed for use by any third party shall follow secure development as defined in this policy. Additionally, the following requirements shall be met:

- Mechanisms shall be provided and communicated to the recipients for verification of the software release integrity.
- The software shall be protected from reverse engineering (e.g., by using obfuscated object code).
- The software shall only be distributed after recipients have signed an agreement stating they shall not disassemble, reverse engineer, or modify software provided by the OCA.

- All system documentation for use by third parties shall be reviewed and authorised prior to release.

7.7. Training

The OCA staff involved in software development shall receive training in secure software development, as appropriate to their role. This shall include annual training in how to avoid common coding vulnerabilities such as those identified in The Open Worldwide Application Security Project (OWASP) and Building Security in Maturity Model (BSIMM).

8. Testing

All new or modified systems shall be subject to system testing prior to deployment, using established, formal processes. The following requirements shall be met:

- Testing shall:
 - Include the testing of all documented functional and non-functional requirements, including information security requirements;
 - Employ recognised best practices of software testing, with documented test plans, test exit criteria, test cases, etc.;
 - Be conducted by dedicated testing teams, segregated from the development teams and with an appropriate degree of knowledge of software testing techniques, including testing of information security requirements;
 - Be appropriately documented and ensure traceability of test cases to the corresponding requirements;
 - Be automated when applicable and possible.
- Whenever feasible, system testing by the dedicated testing teams as described in the previous point shall be supplemented by user acceptance testing (UAT), conducted by designated users of the system being tested. Where UAT is conducted, the relevant dedicated testing teams shall provide support to the designated users for this activity.
- New external-facing systems, or modifications to such systems entailing significant changes in terms of information security controls, shall be subject to penetration testing prior to deployment (and to UAT where conducted). See the [Threat and Vulnerability Management Policy](#) for more information on penetration testing.
- The use of live production data, especially when it contains information classified as Confidential or Highly Confidential, shall be avoided. Where such data is required for testing purposes:
 - It shall be, whenever possible, anonymised or obfuscated before use;
 - When anonymisation/obfuscation is not possible, authorisation shall be sought in advance from data owners, and the associated risk shall be managed;
 - It shall be securely erased from the test environment immediately after testing is complete.

- Access control requirements that apply to production environments shall also apply to test environments.

9. Deployment

Before the deployment of new or modified software, the following criteria shall be met:

- Development or test account information, such as user account information or password, shall have been removed.
- Data used for testing shall have been removed.
- Outstanding issues following software testing shall have been fully resolved.

Deployment of new or modified systems shall be done using established, formal processes. The following requirements shall be met:

- Mechanisms shall be in place – and automated as much as possible – to ensure that all the correct, required components are deployed (software and/or hardware).
- Deployment in production environments shall be subject to authorisation by the Change Advisory Group (CAG), following review of documented outcomes of previous delivery gates.
- Deployment shall be appropriately documented.
- All affected users shall be forewarned of the deployment timetable and of any possible disruption to normal services.
- Any unsuccessful deployment shall trigger the implementation of the corresponding rollback plan.
- In the case of software to be used by third parties, mechanisms shall be provided and communicated to the recipients for verification of the software release integrity – see subsection 7.6 above.
- Deployment processes shall be automated when applicable and possible.

See the [Change Management Policy](#) for more information.

10. Protection of Source Code

All source code developed by or for the OCA constitutes Confidential information and shall be accordingly handled, as prescribed in the [Information Classification and Handling Policy](#).

Source code shall be protected from unauthorised disclosure and modification during and after distribution using appropriate logical and physical security controls:

- The security of system files, program source code, load modules and object libraries shall be protected with approved access controls and encrypted where technically feasible.
- Source code, library products, system tools and system documentation shall reside in protected repositories.
- Code distribution within the OCA shall employ strong logical and physical access controls to ensure authenticity.
- External code distribution (where applicable) shall also employ digital signatures to ensure authenticity.

Production code shall not be modified except through a documented and approved change procedure, in line with the [Change Management Policy](#).

Consideration shall be given to placing source code into a commercially provided software escrow repository.

11. Intellectual Property

- 11.1. All software created by the OCA, or by a third party on behalf of the OCA under contract, constitutes intellectual property owned by the OCA.
- 11.2. All matters regarding creation, ownership or transfer of intellectual property shall be done so under legal guidance.

12. Third Party Software

12.1. Generalities

In circumstances where third party software is used by the OCA², the following requirements shall be met:

- Only the OCA-approved third-party software shall be installed on or accessed from the OCA devices; this includes “Software as a Service” (SaaS).
- The third party who provides the software shall be subject to the supplier management process as defined in the [Third-Party Vendor Management Policy](#).

² Other than open source code – see subsection 7.4 above.

- Updates required for applications which use third party libraries shall be identified and applied, in line with the [Threat and Vulnerability Management Policy](#).
- The software shall be licenced, and licences shall be appropriately managed.
- Where remote maintenance of software by a third-party provider is required, this shall be done with appropriate control of access, including granting temporary access where appropriate, in line with the [Access Control Policy](#).
- The OCA should not run any end-of-life operating systems or applications in a production environment – see the [Threat and Vulnerability Management Policy](#) for more information.

12.2. Restrictions on Changes to Third Party Software Packages

Modifications to third-party software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled. As far as possible and practicable, third-party software packages shall be used without modification or customisation.

Where a software package needs to be modified the following shall take place, in addition to the normal requirements of the change management process:

- A risk assessment of built-in controls and integrity processes being compromised;
- Obtaining consent from the vendor, as relevant;
- Where feasible, obtaining the required changes from the vendor as standard program updates;
- An impact assessment of the OCA becoming responsible for the future maintenance of the software as a result of changes;
- A review of compatibility of the changes with other software in use.

If changes are necessary, the original software shall be retained, and the changes applied to a designated copy. A software update management process shall be implemented to ensure the most up-to-date approved patches and application updates are installed. All changes shall be fully tested and documented, so that they can be reapplied, if necessary, to future software upgrades.

13. Hardware

13.1. The following requirements shall be met for the acquisition of IT equipment:

- IT equipment shall be appropriate to satisfy the OCA's information security requirements.
- IT equipment shall only be acquired from the OCA-approved third-party suppliers.
- Suppliers of IT equipment to the OCA shall be subject to the supplier management process defined in the [Third-Party Vendor Management Policy](#).
- Where applicable, IT equipment shall be configured in line with established baselines and supporting standards.
- Where hardware components are an integral part of the implementation of an OCA system³:
 - Information security requirements pertaining to those hardware components shall be identified, analysed and documented;
 - The requirements pertaining to those hardware components and to software components implemented in them shall be reviewed and tested using appropriate tools and methodologies; this could be outsourced to an accountable and capable third party where the OCA does not have the required capability.
- Hardware shall be reviewed for integrity before deployment into production.
- Maintenance and repair of hardware shall be performed using an established process.

14. Disposal of Systems

- 14.1. When reaching their end of life, OCA systems shall be securely disposed of. The following requirements shall be met:
- Users shall be notified with sufficient advance of the impending end of systems support and the date of systems end of life.
 - Software shall be effectively uninstalled from the devices where it is hosted; this shall as much as possible be done by automated procedures.
 - Data shall be securely removed from the devices where it is stored, in line with the [Information Classification and Handling Policy](#).
 - Equipment shall be securely disposed of in line with the [Asset Management Policy](#).

15. Metrics and Reporting

- 15.1. Technical and operational metrics referring to systems acquisition, development and maintenance, including application security metrics, shall be defined, obtained and reported to the OCA Board, in alignment with business objectives, security requirements, and compliance obligations, and enabling processes improvement.

³ Including, but not limited to, 'Internet of Things' (IoT) systems.

16. Policy Review Date

- 16.1. 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.

17. Document Control

Document Control	
Title:	Secure Software Development Policy
Reference:	
Version:	1.0
Date:	
Status:	Draft
Owner:	IT Manager
Classification:	Internal

17.1 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