

Logging and Monitoring Policy

Table of Contents

1. Purpose.....	3
2. Scope.....	3
3. Policy Statement	3
4. Roles and Responsibilities	4
5. Event Logging	4
6. Time Synchronisation.....	6
7. Security of Logs	6
8. Monitoring	7
9. Retention of Logs	8
10. Testing	8
11. File Integrity Monitoring	8
12. Addressing Failures of Critical Security Control Systems	9
13. Log Reliability and Availability	10
14. Cloud and Managed Services	10
15. Metrics and Reporting	10
16. Policy Review Date	11
17. Document Control	11
17.1 Document Revision History	11

1. Purpose

1.1. The purpose of this policy is to ensure that:

- Access to sensitive and/or critical networks, systems, applications and facilities, and any other relevant event data, are appropriately logged and collated for investigative and audit requirements;
- Logs are appropriately protected, retained for an appropriate length of time, and regularly monitored.

2. Scope

- 2.1. This policy applies to all of the Open College of the Arts (OCA) networks, systems, services, applications and facilities that process Non-Public information. 'Non-Public' refers to any information and associated information processing facilities that are classed as being either Highly Confidential, Confidential or Internal within the [Information Classification & Handling Policy](#).

3. Policy Statement

The OCA's policy regarding logging and monitoring is as follows:

- All access to sensitive and/or critical networks, systems, applications and facilities shall be logged.
- All other event data, when deemed necessary, shall be logged and collated for investigative and audit requirements.
- All network and system components that reside on the OCA's network and cloud services shall be regularly updated with the correct time, to ensure that the log records are correct.
- Logs shall be secure and shall not be changed or deleted in an unauthorised way, or accidentally.
- Logs shall be regularly monitored for unauthorised access activities and any other suspicious occurrences.
- Logs shall be retained for an appropriate length of time; in case they are needed for further review.
- Logging and monitoring processes shall be regularly tested, to enable continuous process improvement.

- File integrity monitoring processes shall be implemented, using appropriate tools.
- Failures of critical security control systems shall be identified and addressed.

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 Department and business system owners shall comply with and monitor logs in line this policy.
- All the OCA staff shall comply with this policy and facilitate its implementation.

5. Event Logging

5.1. The OCA shall implement logging to provide an audit trail that:

- Captures access to relevant network devices, systems, services and applications that process the OCA Non-Public information;
- Captures physical access to areas that house Non-Public information, including areas that host information processing facilities, e.g. computer rooms and communications rooms;
- Links all access to each individual user or service account;
- Captures any other events relevant for monitoring of information security within those network devices, systems, services, applications and facilities.

5.2. The OCA shall implement automated logging to reconstruct the following events:

- All individual user accesses to Non-Public information;
- All actions taken by any individual with root or administrative privileges;
- Access to all logs;
- Invalid logical access attempts (e.g., access attempts by leavers);
- Use of and changes to identification and authentication mechanisms, including but not limited to:
 - Creation of new accounts and elevation of privileges;

- All changes, additions, or deletions to accounts with root or administrative privileges;
- Initialisation, stopping, or pausing of audit logs or security services;
- Creation and deletion of system-level objects for relevant devices and systems;
- Alerts from intrusion detection and anti-malware solutions;
- DNS queries;
- URL requests;
- Command-line execution;
- Cryptographic and key management operations and controls, including key lifecycle management events;
- Alerts from file integrity monitoring solutions;
- Security events which shall be retained and used in support of forensic and/or audit purposes.

5.3. The OCA shall record at least the following log entries for each event:

- Account identification;
- Account type (user, privileged, service, etc.);
- Type of event;
- Date and time;
- Success or failure indication;
- Origination of event, e.g. IP or MAC address;
- Identity or name of affected data, device or system component.

6. Time Synchronisation

- 6.1. The OCA shall use time synchronisation technology, e.g. Network Time Protocol (NTP), to synchronise clocks and times of relevant devices and systems. The high-level design of the company-wide time synchronisation solution shall be documented.

- 6.2. Time synchronisation technology shall be implemented and protected from vulnerabilities in line with the [Threat and Vulnerability Management Policy](#).
- 6.3. Relevant devices and systems shall have the correct and consistent time. Only designated central time servers shall receive time signals from external sources, and time signals from external sources shall be based on Coordinated Universal Time (UTC). Where there is more than one designated central time server, the time servers shall peer with one another to keep accurate time. Relevant devices and systems shall receive time information only from designated central time servers.
- 6.4. Time data shall be protected. Access to time data and the associated configuration/services shall be restricted to only personnel with a business need to access or manage time data, i.e. authorised administrators of relevant devices and systems. Any changes to time settings on relevant devices and systems shall be logged, monitored, and reviewed.
- 6.5. Time settings shall only be received from industry-accepted reliable time sources.
- 6.6. Where it is not technically feasible to maintain time synchronisation for devices, those devices shall have the time and date regularly verified and, if necessary, manually synchronised at intervals of no less than 30 days. Where a device is found to have deviated during that period, the cause shall be investigated.

7. Security of Logs

- 7.1. Logs shall be secured so they cannot be altered or removed.
- 7.2. Viewing of logs shall be limited to those with a job-related need, e.g. by the IT Team for information security purposes.
- 7.3. Log files shall be protected from unauthorised modifications via access control mechanisms, physical segregation, and/or network segregation.
- 7.4. Log files shall be promptly backed up to a centralised log server that prevents alterations.
- 7.5. Logs for external-facing technologies shall also be written onto a centralised log server. Examples of external-facing technologies include firewall logs, Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS) alerts, URL content filtering logs, anti-malware logs, DNS logs, and e-mail logs.
- 7.6. Logs for internal and service/infrastructure technologies shall also be written into a centralised log server. Examples of internal-facing technologies include Dynamic Host Configuration Protocol (DHCP), identity and access logging, account modification and any security generated events.
- 7.7. Where the flow of log data traverses the networks where the content may be captured, measures shall be taken to ensure that the logs in question do not contain any sensitive data.
- 7.8. File integrity monitoring software – see section 10 below – shall be used on archived logs to ensure that existing log data cannot be changed without generating alerts, although new data being added shall not cause an alert. Alternatively, a solution shall be in place to ensure that existing log data cannot be changed at all.

- 7.9. Procedures shall be in place to ensure that the storage capacity of log file media is not exceeded, and therefore prevent either the failure to record events or overwriting of past recorded events. It shall also be ensured that there are no bandwidth or license limitations that could cause occurrences of these types.
- 7.10. Controls shall be in place to prevent privileged users, i.e. administrators, from being able to manipulate the logs. The centralised log server shall only be accessible to the IT Team for information security purposes.

8. Monitoring

- 8.1. Logs shall be monitored to identify anomalies or suspicious activity. Log harvesting, parsing, and alerting tools shall be used to meet this requirement.
- 8.2. The following logs shall be reviewed at least daily, with alerting to administrators where appropriate:
- All security events;
 - Logs of all system components that store, process or transmit payment card data;
 - Logs of all critical systems;
 - Logs of all servers and systems that perform security functions.
- 8.3. Other logs for all system components, including logs of external service provider activities, shall be reviewed on a periodic basis in line with the risk.
- 8.4. In addition to monitoring of logs, there shall be processes in place for regular monitoring for unauthorised personnel, connections, devices and software, in line with the [Acceptable Use Policy](#), the [Access Control Policy](#) and the [Network Security Policy](#).
- 8.5. The impact of every event shall be determined, and any exceptions and anomalies shall be identified during the review process. These shall be followed up, and actions shall be recorded, in line with the [Incident Response Policy](#).
- 8.6. The OCA shall have documented procedures in place for monitoring access logs.

9. Retention of Logs

- 9.1. Log history shall be retained for at least one year, with a minimum of 90 days immediately available for analysis, e.g. using a combination of online logs, indexing, archived logs, and backups.

10. Testing

- 10.1. Tests to check the efficiency of the logging and monitoring processes shall be undertaken regularly – at least annually. Such tests shall include the simulation of attacks and unusual activities, both with and without previous knowledge by the teams responsible for monitoring that such simulations are taking place. Third party specialists may be commissioned where deemed useful.
- 10.2. The outcomes of tests shall be recorded, retained and used for lessons learned activities, to enable continuous improvement of the logging and monitoring processes.

11. File Integrity Monitoring

- 11.1. The OCA shall deploy file integrity monitoring tools to alert personnel to unauthorised modification (including changes, additions, and deletions) of critical system files, configuration files, or content files. This includes relevant operating system and application settings.
- 11.2. Examples of files that shall be monitored include:
 - System executables;
 - Application executables;
 - Configuration and parameter files;
 - Centrally stored, historical or archived, log and audit files;
 - Web pages used for payment by card;
 - Other critical files identified by the OCA to be at risk.
- 11.3. For file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File integrity monitoring tools usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, shall be evaluated and defined.
- 11.4. File integrity monitoring tools shall:
 - Monitor any changes to access log data that shall not be changed;
 - Be actively running and up to date;
 - Be configured to perform critical file comparisons at least on a weekly basis.

- 11.5. Alerts shall be generated – and centrally recorded and responded to – when components that are being monitored are altered, excluding when information is added to the end of log files.
- 11.6. Records of file integrity monitoring checks, alerts and resulting actions shall be retained for one year.

12. Addressing Failures of Critical Security Control Systems

- 12.1. Processes shall be implemented to monitor the availability of critical security control systems and to enable timely detection and reporting of failures of those systems, including but not limited to:
 - Firewalls;
 - IDS / IPS;
 - File integrity monitoring;
 - Anti-malware;
 - Physical access and monitoring controls;
 - Logical access controls;
 - Audit logging mechanisms;
 - Segmentation controls, if in use.
- 12.2. Any failure of, or alert against a critical security control shall be considered as an information security incident and responded to in a timely manner, as prescribed in the [Incident Response Policy](#).

13. Log Reliability and Availability

- 13.1. Where the network between a system/service and the centralised log server(s) may be unreliable or at risk of being impacted by network capacity exceeding available bandwidth, the logging method used shall be such that there is a reliable caching and confirmed delivery of the log data.
- 13.2. Any centralised log servers shall have system and service availability and performance SLAs in line with the systems and services that they capture log data from.

14. Cloud and Managed Services

- 14.1. Where the OCA uses cloud or managed services, the responsibilities for logging and monitoring can be shared between the cloud service provider (CSP) and the cloud service customer (CSC), in line with the Shared Security Responsibility Model and with the Managed Service Provider (MSP) in line with contractual terms.
- 14.2. The split of responsibilities for logging and monitoring may vary depending on the delivery model of the cloud services consumed by the OCA. The following applies:
- In the case of Software as a Service (SaaS), all responsibilities for logging and monitoring shall generally sit with the CSP;
 - Responsibilities for the monitoring of physical access to the data centres that host the cloud services shall sit with the CSP, irrespective of delivery model;
 - In the case of Infrastructure as a Service (IaaS), responsibilities for log monitoring and alerting shall generally sit with the CSC;
 - In the case of Platform as a Service (PaaS), responsibilities for time synchronisation shall generally sit with the CSP.
- 14.3. In all cases, the split of responsibilities shall be clearly documented in contractual terms.

15. Metrics and Reporting

- 15.1. Relevant metrics for logging and monitoring shall be defined, and regularly obtained and reported to the OCA Board.
- 15.2. Analysis of metrics shall be used to assess the efficiency of the logging and monitoring processes and continuously improve them.

16. Policy Review Date

17. 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.

18. Document Control

Document Control	
Title:	Logging and Monitoring 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