

Network Security Policy

Table of Contents

1. Purpose.....	4
2. Scope.....	4
3. Policy Statement	4
4. Roles and Responsibilities	5
5. Network Design.....	5
5.1. Generalities	5
5.2. Logical Network Segregation.....	6
5.3. Development and Test Environments.....	6
6. Network Documentation	7
7. Connectivity.....	7
7.1. Generalities	7
7.2. Internal Local Area Networks	7
7.3. Untrusted Networks.....	8
8. Configuration of Network Devices	8
9. Network Operations.....	8
9.1. Generalities	8
9.2. Security of Network Services.....	9
9.3. Intrusion Detection / Prevention / Anti-Malware Solutions.....	9
9.4. Incident Management.....	10
9.5. Network Equipment Physical Security	10
10. Wireless Local Area Networks (WLANs)	10
10.1. Generalities	10
10.2. Roaming Environments (Outside the Office).....	11
10.3. Static Environments	11
10.4. Security Requirements for Access Points.....	12
11. Firewalls.....	13
11.1. Generalities	13
11.2. Personal Firewalls.....	14
11.3. Firewall Configuration.....	14
11.4. Firewall Administration Access Control.....	14
11.5. Firewall Rules.....	15
11.6. Firewall Logging	15

11.7. Firewall Change Control	16
12. DNS Protection	16
13. Remote Access	17
13.1. Generalities	17
13.2. Remote Access to On-Premise Networks.....	17
13.3. Remote Network Maintenance	17
13.4. Auditing and Logging.....	17
14. Penetration Testing	18
15. Capacity Management	18
16. Cloud and Managed Services	18
17. Metrics and Reporting	19
18. Policy Review Date	19
19. Document Control	19
19.1 Document Revision History	19

1. Purpose

- 1.1. The purpose of this policy is to specify and communicate requirements for the security of the Open College of the Arts (OCA) networks. Throughout this document, any references to 'network(s)' are meant to encompass both data and voice networks, except where otherwise specified. This policy is independent of any hardware and software environment and shall be used as a generic baseline for the implementation of security for any aspect of the network, across all locations.
- 1.2. A large proportion of the OCA information is stored, processed and transmitted on information technology networks, including cloud-based networks. To achieve the objectives of information security, the OCA therefore needs to include requirements for the protection of information technology networks, including infrastructure and virtualisation security requirements. This policy sets out these requirements.

2. Scope

- 2.1. This policy applies to all information technology networks under the control and management of the OCA and its suppliers. It applies to physical and logical networks, as well as on premise and cloud-based networks. The OCA suppliers are expected to comply with this policy.

3. Policy Statement

- 3.1. The policy of the OCA in regard to network security is as follows:
 - Information assets shall be protected from all threats, whether internal or external, deliberate or accidental.
 - Responsibilities for carrying out specific security processes on the OCA networks shall be clearly defined and documented.
 - Requirements for "trusted" networks are:
 - All networks that have been assessed for compliance with the OCA policies shall be classed as "trusted";
 - All other networks shall be classed as "untrusted";
 - Untrusted networks shall be segregated from trusted networks by firewalls.
 - For networks on the OCA premises, only network equipment provided, supported, and maintained by (or on behalf of) the IT Department shall be used. Installation or direct connection to the the OCA network of privately-owned network devices is forbidden, unless this has been formally approved by the IT Department.
 - Access to the OCA networks shall be controlled. All network users shall be properly authenticated and authorised.

- Non-public information shall be transmitted over secure connections. Cryptographic measures shall be applied in accordance with the [Information Classification and Handling Policy](#) and the [Cryptographic Controls Policy](#). All wireless transmissions between devices shall be encrypted.
- There shall be a managed process in place for developing and maintaining availability of networks commensurate with their criticality to the business process.
- All Wi-Fi devices shall be compliant with any Radio Frequency Identification (RFID) legislation that may exist both locally and nationally.
- Wi-Fi implementations shall ensure that there is no interference with production systems or with other electronic equipment that might create a conflict.

4. Roles and Responsibilities

- The IT Manager is responsible for this policy and shall ensure that this policy is up-to-date and relevant.
- Line managers are directly responsible for implementing relevant policies within their functional areas, and for adherence by their staff.
- All personnel involved in the design, configuration, maintenance or management of networks have a responsibility to adhere to this policy.
- Responsibilities for network activity shall be assigned and restricted to appropriate individuals. Responsibility shall be clearly assigned for:
 - Controlling the technical aspects of the network, such as network design, configuration management, traffic management, and network monitoring;
 - Managing the network environment, such as day-to-day operations, incident management, and change management;
 - Establishing service agreements, such as those with users or external service providers.

5. Network Design

5.1. Generalities

Networks shall be designed to:

- Incorporate technical standards, support consistent naming conventions and comply with legislation and regulations;
- Ensure that device/host naming is not indicative of purpose or capabilities;
- Minimise single points of failure and the number of entry points into the network;
- Allow for remote management of the network, where technically feasible and in line with these security requirements;

- Enable network management reports and logs to be maintained, where appropriate;
- Minimise opportunities for unauthorised access or denial of service. This shall include network architecture security, hardware and software security, and configuration and management controls.

5.2. Logical Network Segregation

The OCA's network architecture strategy shall consider, as appropriate, the following principles of segregation of networks by business area or function:

- Databases shall be placed in a network zone that is logically segregated from all other network zones.
- Security controls shall be implemented between wireless networks and sensitive business systems, including, but not limited to, systems processing confidential information.
- Where services are exposed to the Internet for accepting inbound connections, all connections shall be terminated using a system designed for this purpose (such as a reverse proxy or edge device). The device shall be deployed within a demilitarised zone (DMZ; a dedicated subnet) and firewalled on either side, i.e. the external edge and the internal edge.
- System components that store payment card data shall be within an internal network which is segregated from 'connected systems' where this is possible, and in all circumstances from the DMZ and other untrusted networks.
- Some networks may warrant segregation from other networks in their entirety, such as a network for physical security systems (e.g. CCTV). In such cases, segregation shall be achieved either by using an entirely separate physical network or through the use of isolated routing instances – virtual routing and forwarding (VRF).
- Cloud-based networks supporting multi-tenancy shall be designed to ensure that all user access is appropriately segmented and segregated, monitored and restricted, with appropriate mechanisms to ensure that tenants have access only to their own data, not to other tenants' data.
- Computing resources for administrative tasks or tasks requiring administrative access shall be segmented from the OCA's primary network and not be allowed internet access.

5.3. Development and Test Environments

- 5.3.1. Development and test environments shall be segregated from production environments.
- 5.3.2. Production data shall not be used in development or test environments, unless it has been anonymised/obfuscated using established procedures.

6. Network Documentation

- 6.1. The IT Department shall maintain under strict configuration management the documentation of groups, roles, and responsibilities for logical management of network components. Examples include firewall configuration procedures, server configuration procedures, email filtering and management guidelines, up to date logical network diagrams, and backup procedures. In addition, documentation shall be maintained for:
- The configuration of all networks (including VLANs, WLANs, etc.), including all nodes and connections; this includes network diagrams and data flow diagrams describing the network architecture;
 - Communications equipment, software, links and services, including up-to-date inventories and labelling of equipment;
 - In-house cabling, including identification of cable runs and labelling of cables;
 - Identification of high-risk environments.

7. Connectivity

7.1. Generalities

The following requirements apply with respect to network connectivity:

- All permanent network connections into and out of the OCA networks shall be documented and approved.
- All changes to network components shall be formally tested, documented and approved, in compliance with the [Change Management Policy](#).
- Where connectivity needs to be provided to transport the OCA data between sites over unsecured networks, all communications between the sites shall be encrypted in line with the [Cryptographic Controls Policy](#).
- Systems that process Confidential or Highly Confidential information shall not be directly connected to any external time source. The time synchronisation process shall be obtained by peering such systems to at least two internal time servers, each connected to reliable time sources.

7.2. Internal Local Area Networks

- 7.2.1. Connection shall not be made between two Local Area Networks (LANs) within the OCA until it is established that both LANs are compliant with the relevant OCA information security policies.
- 7.2.2. Where the networks are of differing security classification, controls shall be put in place to ensure that only authorised users and approved traffic traverse the point where the networks are linked.

7.3. Untrusted Network

- 7.3.1. An “untrusted” network is any network that is not:
- Owned and managed by the OCA IT or its approved suppliers, or;

- A cloud network approved by the OCA IT.
- 7.3.2. Connectivity with “untrusted” networks shall be protected through the use of firewalls. The following shall apply:
- Direct public access between external untrusted networks and the OCA resources that process the OCA information classified as Non-Public is strictly prohibited.
 - Logical or physical network connections to untrusted networks shall be subject to contractual agreements between the OCA and the network owners.

8. Configuration of Network Devices

- 8.1. All network devices shall be configured such that they are protected from security threats. The secure configuration baselines that are required for these devices shall be based on industry-accepted system hardening standards. This includes configuration of the network device to:
- Highlight overload or exception conditions;
 - Log events in a form – e.g. Common Event Format (CEF) – suitable for review and capable of being copied to a separate log collecting system for review;
 - Disallow non-essential services;
 - Close or disable network ports which are not in active use, or which are in public areas and exposed;
 - Prevent unauthorised or incorrect updates (for network devices that perform traffic routing).
- 8.2. Network devices shall be reviewed at least annually against approved configuration standards and by checking parameters, settings and activity logs.
- 8.3. Access to network devices, such as routers, shall be strictly controlled. All physical and logical access to these devices shall be authorised through established change management procedures, in line with the [Change Management Policy](#).

9. Network Operations

9.1. Generalities

9.1.1. The following requirements shall be met:

- All changes for external connections to the OCA network shall follow the [Change Management Policy](#).
- All administrative or configuration changes to network devices shall be managed through change management processes and records shall be maintained.

- Access control rules for all network devices (physical or virtual) that have a security function shall be formally reviewed by IT on, at least, a six-monthly basis.

9.2. Security of Network Services

9.2.1. All networked devices on the OCA network shall be synchronised to a single time source. Time synchronisation shall:

- Be configured to an approved the OCA time source or service, whether hosted on premise or within the cloud;
- Be authenticated;
- Be such that if an Internet time source is used, then this shall be via a connection to the DMZ (a dedicated subnet).

9.2.2. Where insight for security controls is required, the OCA ingress/egress points shall inspect encrypted traffic to meet the requirements of other policies.

9.3. Intrusion Detection / Prevention / Anti-Malware Solutions

9.3.1. Intrusion detection / prevention / anti-malware solutions shall be strategically deployed and implemented as follows:

- Solutions shall be implemented at all Internet ingress and egress points to on premise networks and cloud environments, and at all points where the networks change security classification within the OCA (e.g. moving from general access to data centre, server farm or to privileged networks in their own segment).
- Ingress / egress points shall have appropriate anti-malware controls in place to ensure that traffic is inspected for access to, or transfer of, malicious content (including but not limited to inappropriate or malicious websites).
- Critical devices, including, but not limited to, those processing confidential information, shall have Host-based Intrusion Detection/Prevention System (HIDS/HIPS) controls whenever possible; where this cannot be implemented (i.e. not supported by the vendor), then compensating mechanisms shall be implemented (e.g. Network Intrusion Detection, robust firewall rules).
- Implementation shall include:
 - Solutions actively running, and configured, maintained and updated per vendor instructions to ensure optimal protection;
 - Detection of known attack characteristics;
 - A process for regular update to incorporate new or updated attack characteristics;

- Provision of alerts when suspicious activity is detected and formal procedures for responding to suspected intrusions as per the [Information Security Incident Response Policy](#);
 - Backing up of alerts to a secure, centralised log server, in line with the [Logging and Monitoring Policy](#);
 - Retention of alert logs for a defined period of time, in line with the same policy.
- 9.3.2. The use of powerful analysis / monitoring tools, such as protocol analysers, shall be restricted to authorised users.
- 9.3.3. For more information on event logging, see the [Logging and Monitoring Policy](#).

9.4. Incident Management

- 9.4.1. In order to identify and resolve incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring, all types of incidents (including malfunctions, loss of power / communications services, overloads, mistakes by users or IT Department personnel, and access violations) shall be recorded, investigated and resolved in accordance with the [Incident Response Policy](#).

9.5. Network Equipment Physical Security

- 9.5.1. The physical security controls for network equipment shall be in accordance with the [Physical Security Policy](#).

10. Wireless Local Area Networks (WLANs)

10.1. Generalities

- 10.1.1. WLANs transmit and receive data over the air, minimising the need for wired connections. Thus, WLANs combine data connectivity with user mobility. Although there is a reduction in the requirements for physical infrastructure, use of wireless significantly increases three major risks:
- Interception – Since wireless signals are radio transmissions, they can be easily intercepted;
 - Unauthorised access – As wireless transmissions circumvent traditional perimeter security; access control is weakened. Further, not only can an attacker gain access to the the OCA network, but the attacker can also create unauthorised “rogue” gateways (access points) to deceive legitimate users;
 - Denial of service – Since wireless network devices operate using radio signals, their use can cause, and be vulnerable to, Radio

Frequency Interference (RFI). This can result in significantly degraded performance and can lead to denial of service.

- 10.1.2. The OCA shall have controls in place to minimise these risks.
- 10.1.3. Firmware on wireless devices shall support strong encryption for authentication and transmission over wireless networks.
- 10.1.4. Only secure wireless protocols shall be used, in line with current security industry best practices (e.g. Wireless Application Protocol version 2.0 (WPA2) or later).
- 10.1.5. Before authorised WLANs are used, all default passwords and encryption keys shall be changed. In addition, only secure Simple Network Management Protocol (SNMP) community strings shall be used, as applicable.
- 10.1.6. Passwords and encryption keys for access to WLANs shall be changed whenever anyone with knowledge of the keys leaves the OCA or moves into a different role which does not require access to the WLANs.

10.2. Roaming Environments (Outside the Office)

- 10.2.1. Connection to the OCA resources over third-party wireless facilities, such as a public wireless “hotspot”, may be enabled using approved laptops and mobile devices – via the Mobile Device Management (MDM) solution, in accordance with the [Acceptable Use Policy](#).
- 10.2.2. Users shall check the name of the wireless network they are connecting to, to determine whether it appears to be genuine. If in doubt, users shall not connect to the network.
- 10.2.3. Where users use their own device to access the OCA applications/data, they shall abide by the [Acceptable Use Policy](#) in relation to how they access and store corporate data.
- 10.2.4. When connecting to the OCA on-premises devices from a third-party wireless network, all communications shall be encrypted. This shall be done using client Virtual Private Network (VPN) technology.

10.3. Static Environments

- 10.3.1. In physically static OCA office environments, wireless connectivity to corporate networks shall be restricted to specified sets of devices only. Connection of mobile devices shall only be allowed if approved and enabled by the IT Department. Corporate devices shall automatically connect to the corporate wireless network, and not use any shared / public networks.
- 10.3.2. Devices that have not been approved for use with the corporate network shall not be connected to the corporate wireless network but shall use either the guest or public wireless network – which shall not provide access to the on-premises corporate environment.
- 10.3.3. The following controls shall be in place for corporate devices connecting to the OCA wireless network:
 - Every device shall be authenticated to the access point, using a certificate/Network Access Control (NAC).
 - All communications over the wireless network shall use an established encryption method in line with the [Cryptographic Controls Policy](#).

- Extensible Authentication Protocol / Transport Layer Security (EAP/TLS) shall be used to provide credential protection and mutual authentication.
- Posture checking of devices connecting to the wireless network shall be applied to ensure that they are patched to an acceptable level and that anti-malware software is up to date. Until this is addressed, the devices shall not be permitted access to the corporate network.
- Unless specifically required for business purposes and approved by the IT Department, peer-to-peer wireless capabilities on end user devices shall be disabled.

10.3.4. Where there is a requirement for enhanced security, multi-factor authentication (MFA) shall be used. Service Set Identifier (SSID) broadcasting shall be turned off.

10.4. Security Requirements for Access Points

10.4.1. The following requirements shall be met for Access Points (APs):

- Only APs implemented by IT shall be deployed within the OCA. Unapproved (rogue) APs are not permitted.
- All APs shall be registered and properly accounted for.
- APs shall be located such that unauthorised physical access is prevented and located away from external sources of electromagnetic interference.
- APs that can be reset to factory default settings with a reset button on the device shall not be used.
- Software programs that can be used to configure APs shall not be installed on users' devices.
- The built-in Communication or COM (serial interface) ports of APs shall be password-protected to prevent any unauthorised access to the APs. All unnecessary services and ports on the APs shall be removed or disabled. Any default passwords shall be changed before use.
- APs shall be connected to a dedicated network segment reserved for wireless devices and not to the core corporate network. Access controls shall be in place between these networks and the core corporate network.
- APs shall be assigned static Internet Protocol (IP) addresses, where feasible.
- Processes shall be implemented to test for the presence of rogue APs, and detect and identify all authorised and unauthorised APs on a regular basis – at least once a year.
 - Methods that may be used in the process include, but are not limited to:
 - Wireless network scans;

- Physical/logical inspections of network devices and systems;
 - Network access control (NAC);
 - Wireless Intrusion Detection Systems or Intrusion Prevention Systems (IDS/IPS);
- If automated monitoring is utilised, e.g. NAC or wireless IDS/IPS, the configuration shall generate alerts when unauthorised wireless access devices are detected;
 - The rogue wireless detection process shall be recorded for audit purposes and any detected rogue AP shall be addressed in line with the [Incident Response Policy](#).

11. Firewalls

11.1. Generalities

11.1.1. The following requirements shall be met for firewalls¹:

- The firewall shall be configured to deny all services except those that are specifically permitted.
- A comprehensive set of rules shall be established to enforce this configuration, and changes to the rule base shall be processed through established change management procedures.
- The firewall software shall run on a dedicated device. All non-firewall related software, such as compilers, editors, communications software, etc., shall be deleted or disabled. The only exceptions are services which are integrated into the recommended product.
- Consideration shall be made to configure services for high availability using a risk-based approach – all decisions on implementation shall be made by the service owner.
- Details of the OCA internal networks shall not be visible from outside the firewall (i.e. internal network addressing shall not be displayed to “untrusted” networks).
- Firewalls shall be used to inspect all network traffic at the perimeter of the internal network for protocol non-compliance, malware, spam, intrusions, or other unwanted traffic. The placement of firewalls shall include:
 - Between the internal network and the DMZ;
 - Between the DMZ and “untrusted” networks;

¹ The requirements for firewalls described in this policy apply both to physical or logical firewalls, and also, as relevant, to other network security controls such as routers configured with access control lists (ACLs), and cloud virtual networks.

- Between wireless networks and business systems²;
 - Between the public hosting zones and the private hosting zones within the cloud provider.
-
- Consideration shall be given to the level of traffic that requires inspection, including whether controls against web application attacks are necessary (e.g. via implementation of a web application firewall). This shall be performed via a formal risk assessment, as necessary.

11.2. Personal Firewalls

- 11.2.1. Any mobile device that accesses the corporate network while connected to an untrusted network such as the Internet shall have personal firewall software activated which the user cannot disable.

11.3. Firewall Configuration

- 11.3.1. The following requirements shall be met for firewall configurations:
- The firewall shall be built and configured to an approved security specification.
 - The configuration standard shall include a documented list of all services, protocols and ports with a business justification and approval for each.
 - No insecure services, protocols or ports shall be used within the configuration.
 - Where relevant, only authorised business traffic shall be allowed between the wireless environment and the cardholder data environment.
 - Running and start-up configurations shall be synchronised after each change.
 - Anti-spoofing measures shall be implemented to detect and block all forged source IP addresses from entering the network.
 - Outbound traffic from a cardholder data environment shall be explicitly authorised.
 - The firewall build and configuration shall be validated on at least an annual basis to ensure security has been maintained.
 - The firewall shall failover to a configuration that denies all services and requires a firewall administrator to re-enable services after a failure.
 - The firewall shall be configured to implement transparency for all outbound services. Unless specifically authorised and approved, all in-bound services shall be intercepted and processed by the firewall.
 - Source routing shall be disabled on the firewall hosts and external routers.

² This is the recommended approach as a firewall will provide additional protection (e.g. anti-spoofing, attack detection etc.) that basic network ACLs / switch functionality cannot provide.

11.4. Firewall Administration Access Control

11.4.1. The following administration access control requirements shall apply:

- Accounts used to access the firewall shall explicitly be only for firewall administration purposes and shall be accountable to a specific individual. Shared accounts or group or demonstration accounts shall be removed or disabled from the firewall where possible.
- There shall be no remote login capability for Root / Administrator.
- “Trust” configurations shall not be used to permit access to the firewall.
- Administrative access to cloud-based resources providing firewall capabilities shall be limited through the use of granular Role Based Access Control (RBAC) and MFA or privileged access management.
- Firewall access passwords shall be immediately changed, in line with the [Access Control Policy](#), when they are known or suspected of being compromised.

11.5. Firewall Rules

11.5.1. The following requirements shall be met for firewall rule management:

- Only protocols that are needed for a service to function shall be allowed to pass through a firewall. Explicit justification shall be obtained, with an associated risk documented and accepted for any insecure protocols used by connections originating from insecure networks.
- Egress network connectivity shall be routed through a Network Address Translation (NAT) control.
- A firewall rule that allows either “From any” or “To any” may only be used when it is justified and shall be explicitly approved through change control procedures.
- Firewall rules shall be documented including, but not limited to:
 - Services and ports opened in the firewall;
 - Business justification for rules including the business process owner;
 - Source and destination network addresses for rules;
 - Date the rule was created;
 - Any change management references.
- Firewall rule sets shall be reviewed on at least a six-monthly basis.

11.6. Firewall Logging

11.6.1. The firewall shall comply with the logging requirements within the [Logging and Monitoring Policy](#). In addition, the following shall be logged:

- All administrative access changing the firewall configuration;

- System access logs – all traffic denied by the firewall and not specifically excluded from logging as “noise”.

11.7. Firewall Change Control

11.7.1. The following requirements shall be met for firewall change control:

- All changes to firewall configurations, including the creation, modification and deletion of rules, shall go through the formal change management process, in line with the [Change Management Policy](#). This includes minor changes, for example, IP address changes, or extending existing filters/rules to include new servers. Substantive changes such as upgrades, architectural design, and use of new products or services, shall be documented and approved in line with the [Change Management Policy](#).
- All desired services shall be described and defined by the business unit requiring a change of a firewall’s rule set. Requests for all services shall additionally include business justification for the service.
- All connectivity requests shall be reviewed to ensure that the request and solution are consistent with the OCA policies and that no conflicts occur.
- Review, authorisation, testing and formal approval of all firewall rule changes shall be accomplished prior to implementation.
- When testing access requests, the logs shall be checked to ensure the correct rules are being triggered.

12. DNS Protection

12.1. Measures shall be taken to limit the potential impact to the OCA of attacks to Domain Name System (DNS) servers. The following measures shall be implemented:

- DNS servers shall be fully patched, and updates shall be applied in line with the [Vulnerability and Patch Management Policy](#).
- Only internal users/systems shall be allowed to access the DNS servers.
- DNS entries shall be proactively monitored to ensure they correspond with the correct IP addresses.
- The use of recursive DNS shall be avoided.
- It shall be ensured that the DNS provider does not permit zone transfers or directory listings.
- It shall be ensured that the DNS provider has distributed denial-of-service (DDoS) protection in place.
- Checks of the public DNS listings shall be conducted at regular intervals (e.g. every 30 minutes) to ensure that they are correct.

- DNS validation / anti-spoofing solutions shall be enabled on the OCA DNS servers and in lookups on behalf of the OCA users.
- Log monitoring shall be implemented on the DNS server to include administrative access and changes to the configuration.

13. Remote Access

13.1. Generalities

- 13.1.1. Remote access is defined as any connection made to the OCA corporate network using remote access technologies such as VPN.

13.2. Remote Access to On-Premise Networks

- 13.2.1. Where remote access is required to services and/or data located on the OCA networks, the following shall be in place:
- The OCA's primary method of MFA shall be used to authenticate users in addition to their network credentials.
 - Connectivity shall be via an approved secure client VPN installed on the user device.
 - Only the OCA approved devices shall be able to access the VPN.
 - Other remote access tools from an external location (e.g. TeamViewer) shall not be used without prior approval.
 - The VPN shall be configured such that the session terminates automatically after a set period of inactivity. The period of inactivity shall be set commensurate to the level of risk associated with the remote access.
 - Access via VPN shall be regularly audited by IT and access removed when not needed.
 - Any banner information presented upon connection to the Internet shall be removed and replaced with an unobtrusive login prompt which includes a warning relating to unauthorised access. The warning shall also clearly communicate to the user that their activities on the network will be monitored and that, by logging on, they grant permission for such monitoring.

13.3. Remote Network Maintenance

- 13.3.1. To prevent unauthorised access to the network through the misuse of remote maintenance facilities, remote maintenance shall be tightly managed and in strict compliance with the above requirements.

13.4. Auditing and Logging

- 13.4.1. All remote access activity shall be logged and monitored, in line with the [Logging and Monitoring Policy](#), so that unusual activity such as failed login attempts and abnormal usage patterns can be identified.

14. Penetration Testing

- 14.1. Where network access is required for penetration testing by a trusted third party, the following specific requirements shall be met:
- All tests shall be agreed by management together with a formal document of authorisation.
 - The aim, scope and methods of the testing shall be clearly defined and documented (including any source IP addresses which may need whitelisting, duration, estimated bandwidth and emergency contact information).
 - Knowledge of testing shall be appropriately restricted.
 - A formal debrief shall be provided by the testers that includes all relevant personnel.
 - The testers shall provide a deliverable that includes remediation requirements and solutions.
 - The information security risk management process shall be applied to the findings documented in the test deliverables, with agreed remediation actions and timelines.

15. Capacity Management

- 15.1. There shall be tools and processes in place to:
- Monitor and tune the use of network resources;
 - Generate alerts when defined thresholds are close to being exceeded;
 - Make projections of future capacity requirements to ensure that systems remain performant at the required levels.

16. Cloud and Managed Services

- 16.1. Where the OCA uses cloud and managed services, the responsibilities for network security management 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. Most of those responsibilities shall generally sit with the CSP; however, the following specific responsibilities shall generally be split between the CSP and CSC:
- In the case of Infrastructure as a Service (IaaS), responsibilities for capacity planning;

- Responsibilities for secure migration to cloud environments³ (irrespective of the delivery model of the cloud services).

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

17. Metrics and Reporting

- 17.1. Relevant metrics for network security shall be defined, and regularly obtained and reported to the OCA Board.
- 17.2. Analysis of metrics shall be used to assess the efficiency of the network security processes and continuously improve them.

18. Policy Review Date

- 18.1. 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.

19. Document Control

Document Control	
Title:	Network Security Policy
Reference:	
Version:	1.0
Date:	
Status:	Draft
Owner:	IT Manager
Classification:	Internal

19.1 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

³ See [Cryptographic Controls Policy](#).



The Open College of the Arts



The Open
University