Glasgow Kelvin College

ICT Security Policy

Document Control Information	
Reviewed by Financial Control Committee:	February 2020
Date of Next Review:	March 2023
Approved by the Board of Management:	March 2020

The Board of Management (or any person/group with delegated authority from the Board) reserves the right to amend this document at any time should the need arise following consultation with employee representatives.

Contents

1. Security Policy Framework

The security policy provides management direction and support for information security. It is primarily directed at staff within the College who are service owners, system procurement and general information services but more so ICT Services staff who are responsible for the development and maintenance of ICT systems. The policy will guide the creation of processes and procedures to minimise the risk of security breaches and events.

The Policy will be reviewed at least every three years and when required by modifications to the regulatory frameworks or when, in the opinion of College management or the Board's Auditors there is any significant change in the structural, legislative or operational aspects affecting the College.

2. Infrastructure, End User Computing & physical locations

2.1. Physical Security

To restrict physical access to authorised individuals, ensure that critical equipment is available when required and to prevent important services from being disrupted by loss of, or damage to, equipment or facilities.

2.1.1 Physical access to critical facilities, such as data centres, network and telecommunication equipment should be restricted to authorised personnel. Authorisation should be issued in accordance with a documented process, be reviewed regularly and revoked promptly when no longer required.

2.1.1.1 Server Room Access

Access to server rooms will be controlled by a Building Management System swipe entry locking system where only the following groups of staff will have access:

- Senior Management;
- ICT Technical Services staff;
- Estates staff;
- Health & Safety staff; and
- Security staff.

Racks and cabinets that hold key servers and storage devices will be locked at all times and the keys held by ICT Technical Services.

Switches and routers (or general networking equipment) will be held within lockable cupboards or areas. They will only be accessible by the staff groups listed above.

2.1.1.2 Staff areas

Where possible, (excluding areas such as public access, reception, advice, etc) staff areas should be locked either

with a key or an automatic door lock system when the last member of staff leaves the area. This helps to physically secure ICT equipment and any digital content on unlocked devices.

2.1.1.3 Classrooms and teaching areas

Classrooms (and similar rooms for teaching) will be secured by lockable doors. If members of staff don't have a master key to access a room they should obtain the room key from Estates. Staff should lock the rooms after they are finished with them and return the key to Estates.

PCs in classrooms will only be secured with a physical lock if the PCs are a high-value or they are deemed to have a higher risk of theft (i.e. the location may have a history of break-ins).

2.1.1.4 Outreach PCs

All outreach PCs that are owned by the College should be secured with a lockable device, thus protecting the device and its contents from theft.

2.2. Network Connection

To prevent unauthorised users or devices from gaining access to information systems and networks.

To ensure that the configuration of network devices is accurate and does not compromise the security of the network.

2.2.1 All network connected devices must be authorised by the College's ICT department and be compliant to Cyber Essentials Plus standards.

2.2.2 Must meet the appropriate security standards to protect against the compromise of confidentiality, integrity and availability of the information that they process.

2.2.3 Network attached devices should be segregated appropriately where necessary.

2.2.3.1 Network Segmentation

The College's Local Area Network (LAN) is segmented into various zones to provide a logical structure for systems, servers and endpoint devices to be best secured.

Endpoint devices are either allowed or blocked from entering the server/system zones to help secure systems and data. The table below outlines broad rules that should be followed to secure the network:

Server Zone (where servers and systems are located)	Endpoint Allowed Rules	Endpoint blocked rules
Open Access Zone *(Contains Moodle, File Servers, Mail servers, etc.)*	ICT staff PCs, General Staff PCs and Student PCs are allowed.	There are no limitations – all endpoints can access this zone without restrictions
Shielded Access Zone *(Contains Finance system, Student Records, HR, etc.)*	ICT staff PCs and General Staff PCs are allowed.	Student PC are blocked from accessing this zone.
Management Access Zone (Contains services that end users will never need to access such as Hosts, Storage, network devices)	ICT staff PCs are allowed	General Staff PCs and Student PCs are blocked from accessing this zone.

2.3. End User Computing

To ensure end user computing devices operate as intended and do not compromise the security of computer installations or other environments.

2.3.1 All end user computing devices that connect to College services and access College information/data must be actively managed by a competent authority and at a minimum comply with the following policies:

- Firewall,
- Malware Protection,
- Patch Management,
- Service Password Management,
- Encryption; and,
- Identity and Access Management.

2.3.2 System Settings and Updates

The College's endpoint devices are configured to provide a further layer of security while not impacting on the end-user experience. This provides a balance between functionality and security.

Windows endpoint devices are configured with the following:

- End-users are not provided with administrator rights to the local device,
- Staff devices will be configured to auto-lock after a period of time,
- Endpoint devices will be configured to download Operating System updates automatically,
- 3rd party software (Flash, Java, browsers, etc.) will be updated as

per the ‘Vulnerability Remediation Procedure’ which is reviewed every two years; and,

- Security patches will be applied as per the Cyber Essential Plus patching standard.

2.4. Server Management

To ensure servers operate as intended and do not compromise the security of computer installations or other environments.

2.4.1 Servers should be configured to prevent unauthorised access or updates and to function as required.

2.4.2 The configuration should disable non-essential user accounts, applications, communication services, protocols and restrict access to powerful utilities, commands and system configuration settings to trusted individuals.

2.4.3 All servers must be actively managed by a competent authority and at a minimum comply with the following policies:

- Firewall,
- Malware Protection,
- Patch Management,
- Service Password Management; and,
- Identity and Access Management.

2.5. Mobile Devices

To ensure mobile devices do not compromise the security of information stored on them or processed by them and prevent unauthorised access to information in the event they are lost or stolen.

2.5.1 The College will protect information stored or processed via College owned mobile devices and prevent unauthorised access when lost or stolen.

2.5.2 Documented configuration standards will be deployed through a management system.

2.5.3 All mobile devices must use an appropriate access control mechanism (e.g. password, pin, biometric) and have a lock out time set.

2.5.4 All mobile devices must be encrypted, be capable of being remotely wiped and must be appropriately protected from malware.

2.5.5 To gain access to College systems users will require to:

- Possess a valid Active Directory username and password,
- be a member of a relevant user group,
- accept the terms of the ICT Acceptable Use Policy; and,
- Using a College issued device.

The system and firewall allow ICT to track and report on the user's internet use. This is a requirement of using the JISC provided JANET internet connection.

2.5.6 Internet Access for Personal Mobile Devices
The College offers a wireless 'on boarding system' to Staff and Students. This allows users to connect personal mobile devices to the College's Wi-Fi network and access Internet resources – most internal resources are blocked as the device is not College owned and trusted.

3. Secure Configuration

3.1. Firewall

To prevent unauthorised network traffic from gaining access to networks or leaving networks.

3.1.1 The College will operate a default inbound deny policy on all firewall devices to block unauthorised inbound connections.

3.1.2 Access to the management interface of the firewall will be appropriately restricted to authorised personnel.

3.1.3 There will be a managed process for documenting the requests for firewall changes.

3.1.4 All such requests must contain at a minimum the details of the requestor, the changes required, duration and the business need for the firewall change.

3.1.5 All firewall change requests will be subject to a review, security assessment and must be approved by a competent authority.

3.1.6 To ensure existing firewall rules are appropriate, and in line with CE+, there will be periodic reviews.

3.1.7 There will be a process where exceptions can be made due to a business need, this should be approved by a member of the SMT/OMT team.

3.1.8 Incoming traffic is scanned for viruses, spyware, vulnerabilities and malicious code unless it is encrypted or from a trusted source.

3.1.9 All internet user activity should be logged and identified using the

College's Active Directory system.

3.1.10 A Demilitarised Zone (DMZ) will be provisioned on the firewall as a 'Best Practice' measure to serve internal web resources from the College to the outside world.

3.2. Malware Protection

To protect the organisation against malware attacks and ensure malware infections can be addressed within defined timescales.

3.2.1 The College will address the malware threat by installing anti-malware software on all appropriate devices.

3.2.2 The anti-malware software will be kept up to date, with signature files updated at least daily.

3.2.3 Files must be scanned upon download and access.

3.2.4 Web pages must be scanned when accessed through a web browser, connections prevented to malicious websites.

3.2.5 There will be a documented process, including risk assessment when there is a business need for exceptions.

3.2.6 The College will utilise sandboxing technology where it is appropriate to do so and to minimise the risk of malicious files entering the organisation.

3.2.7 The College may mandate the use of application whitelisting where it is deemed necessary.

3.3. Patch Management

To address technical system and software vulnerabilities quickly and effectively in order to reduce the likelihood of vulnerabilities being exploited and serious business impact arising.

3.3.1 To help in the identification of threats that may lead to an information security incident, maintain the integrity of important security-related information and support forensic investigations.

3.3.2 The College will protect the integrity of its information and systems by gathering security logs to help identify threats and support investigations.

3.3.3 All systems will be assessed and configured to log appropriate security event information (e.g. failed login attempts), and the logs should be protected against unauthorised access and accidental or deliberate modification.

3.3.4 Security logs should be analysed/reviewed regularly, and log retention schedules are to be defined for each system.

3.4. Identity & Access Management

To ensure that only authorised individuals gain access to business applications, systems, networks and computing devices, that individual accountability is assured and to provide authorised users with access privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

3.4.1 The College will utilise an Identity and Access Management (IAM) system.

The following procedures outline the creation and decommissioning processes:

- Creating GKC Staff Accounts - Procedure
- Staff leaver - mail and file retention - Procedure

3.4.2 The IAM ensures that unique account credentials are approved and created in a timely manner to allow access to information, services and locations necessary for the roles function.

3.4.3 That access permissions are granted on a need only basis and removed when no longer required.

3.4.4 That accounts are disabled or removed when no longer needed.

3.4.5 Standard user accounts are to be assigned by default, with a documented approval process for administrative accounts.

3.4.6 Administrative accounts must be used for administrative activities only, the Administrator Accounts Procedure outlines this.

3.4.7 Multi – Factor Authentication will be implemented for staff where there is an elevated risk (i.e. Management and staff who process key data).

3.4.8 The above principles should also be adhered to when providing access to non-ICT administered systems including:

- Student Records Systems,
- Timetabling system,
- Finance systems; and,
- Estates Building Access systems.

3.5. Password Service Management

To restrict access to business applications, systems, networks and computing

devices to authorised users.

3.5.1 All users should adhere to the College's 'Password Change Procedure'.

3.5.2 All users should be authenticated using a unique username and password before accessing College resources.

3.5.3 Password should never be requested in the form of clear text (e.g. via email, http).

3.6. Encryption

To protect the confidentiality of sensitive information, preserve the integrity of critical information and confirm the identity of the originator of transactions or communications cryptographic solutions should be approved, documented and applied throughout the organisation.

3.6.1 All mobile devices must be appropriately encrypted and use authorised services to ensure the protection of information at rest and in transit.

3.6.2 Encryption technologies used must be managed to ensure that they remain secure and have documented key management processes.

3.6.3 There will be a documented approval process, including risk assessment and risk management process when there is a business need for an exception.

3.6.4 Due to the multi-user use of Student laptops and the decreased sensitivity of data they access there is no benefit to encrypting learner devices.

4. Service Lifecycle

4.1. Asset Management

To help support risk-based decisions regarding hardware / software, reduce the risk of information security being compromised by weaknesses in hardware / software, protect assets against loss, support development of contracts and meet compliance requirements for licensing.

4.1.1 To assist risk-based decisions, reduce risk of compromise by weaknesses in hardware and software, protect assets against loss, meet compliance requirements and inform contracts, all hardware and software should be recorded in an accurate and up-to-date asset register.

4.1.2 There should be regular checks for discrepancies, and these should be investigated and resolved.

4.1.3 The asset register must be protected against unauthorised change and be independently reviewed.

4.2. Configuration Management

To ensure that changes are applied correctly and do not compromise the security of business applications, computer systems or networks.

4.2.1 Changes should be tested, reviewed and be part of a documented change management process.

4.2.2 The change management process covers all types of change, such as upgrades, changes to systems and networks, software or application and to business information.

4.2.3 Any request for change must:

- Be accepted by an authorised individual,
- Approved by an appropriate business representative,
- Tested; and,
- Include a back-out plan.

4.2.4 Once the changes have been made the following must happen:

- Changes are communicated to relevant stakeholders,
- System documentation is updated to reflect changes,
- Changes are reviewed to ensure only changes that have been authorised have taken place; and,
- System and information reviewed to ensure that security classifications have not changed.

4.3. Service Development Lifecycle

4.3.1 To ensure that business applications (including those under development) meet business and information security requirements. System development activities should be performed in specialised development environments, which are isolated from the live and testing environments, and protected against unauthorised access.

4.3.2 Quality assurance of key security activities should be performed during the system development lifecycle.

4.3.3 Information security requirements should be documented and agreed before detailed design commences.

4.3.4 Information security requirements for systems under development should be considered when designing systems.

4.3.5 System build activities (including coding and package customisation) should be carried out in accordance with industry good practice; performed by individuals provided with adequate skills / tools; and inspected to identify unauthorised modifications or changes.

4.3.6 Systems under development (including application software packages, system software, hardware, communications and services) should be tested in a dedicated testing area that simulates the live environment, before the system is promoted to the live environment.

4.3.7 Systems under development should be subject to security testing, using a range of attack types (including vulnerability assessments, penetration testing and access control testing).

4.3.8 Rigorous criteria (including security requirements) should be met before new systems are promoted into the live environment.

4.4. Disposal

To ensure the secure disposal of information assets and comply with legal, regulatory and contractual obligations.

4.4.1 When Technology assets have reached the end of their useful life they should be securely disposed.

4.4.2 Asset management processes must be updated with the final disposition of the technology asset's media and hardware.

4.4.3 All storage mediums will be securely erased in accordance with current industry best practices.

4.4.4 Approved third-party disposal service must render all data / information unreadable and provide a certificate of destruction. These certificates must be retained and asset registers updated with the locations of the certificates.

4.4.5 No computer equipment should be disposed of via skips, dumps, landfill etc.

5. Detection

5.1. Monitoring

To assess the performance of business applications, computer systems and networks, reduce the likelihood of system overload and detect potential or actual malicious intrusions.

5.1.1 The College has regulatory and operational requirements to monitor activity across its network and systems.

5.1.2 Information relating to this monitoring (e.g. logs) should be retained long enough to meet these requirements.

5.1.3 All monitoring activities must be authorised, and regularly performed to help identify suspicious or unauthorised activity.

5.1.4 All personnel authorised to perform monitoring functions must do so in accordance to the relevant ethics, procedures and safeguards.

5.1.5 Monitoring activities include scanning systems for known vulnerabilities, this activity must be restricted to authorised individuals and the results presented to the system owners.

5.1.6 Any misuse of ICT Systems or Equipment will be managed in line with the Acceptable Use Policy and Disciplinary Policies and Procedures.

5.2. Logging

To help in the identification of threats that may lead to an information security incident, maintain the integrity of important security-related information and support forensic investigations.

5.2.1 The College will protect the integrity of its information and systems by gathering security logs to help identify threats and support investigations.

5.2.2 All systems will be assessed and configured to log appropriate security event information (e.g. failed login attempts), and the logs should be protected against unauthorised access and accidental or deliberate modification.

5.2.3 Security logs should be analysed/reviewed regularly, and log retention schedules will be defined in the College's Document Retention policy.

6. Response & Recovery

6.1. Incident Response

To identify and resolve information security incidents quickly and effectively, minimise their business impact and reduce the risk of similar incidents occurring.

The College's Incident Response Procedure should be followed and will ensure the following principles:

6.1.1 The College / College will identify, respond to and recover from security incidents to minimise the business impact and reduce the risk of similar incidents occurring.

6.1.2 The incident response team is responsible for managing information security incidents.

6.1.3 A review will take place after each incident to identify the root cause and highlight any improvements that can be made to the process.

6.2. Business Continuity

To provide relevant individuals with a documented set of actions to perform in the event of a disaster or emergency affecting business applications and technical infrastructure, enabling critical business processes to be resumed within critical timescales.

6.2.1 The Business Continuity procedures should be followed with the following principles adhered to: Business continuity plans should be documented for each key service and provide a set of actions to perform when enacted.

6.2.2 Each plan should be prepared by or in conjunction with the service owner and relate to likely scenarios.

6.2.3 Roles and responsibilities should be defined and documentation/training available.

6.2.4 Business continuity plans should be reviewed and tested on a regular basis.

6.3. Disaster Recovery & Backups

To enable critical business processes to be resumed to an agreed level, within an agreed time following a disruption, using alternative processing facilities.

The Disaster Recovery procedures should be followed with the following principles adhered to:

6.3.1 Due to Virtual Machine technology a general documented backup and restore procedure will be sufficient for Disaster Recovery and backups.

6.3.2 Critical business information and software require a backup schedule to ensure restoration can occur within an agreed time.

6.3.3 Backups should be protected from loss, damage, unauthorised access and subject to the same level of protection as the live information e.g. encrypted.

6.3.4 Backups should be regularly verified by successfully testing restoration.

6.3.5 Alternative facilities must be ready for immediate use.

7. External Partnerships

7.1. Third party

To protect critical and sensitive information when being handled by external suppliers or when being transmitted between the organisation and the supplier.

7.1.1 To protect College information when being transmitted between or handled by an external third party, information security requirements need to be considered at all stages of the relationship.

7.1.2 All third parties should be identified and recorded in a register which assigns a business owner, security contact and is categorised High, Medium, Low in terms of information security.

7.1.3 All third parties should agree a baseline of security arrangements for any information held, and specialised controls put in place which meet business and security needs as a result of a risk assessment.

7.1.4 Termination of third-party relationships should ensure the revocation of physical and logical access, and the return or secure destruction of information assets.

7.1.5 A Business Continuity Plan (BCP) may also be required depending on the nature of the third-party service.

8. Remote access

8.1. VPN Access

A Virtual Private Network (VPN) is a service that is offered by the College for staff. This allows staff on College owned laptops to connect to the College's VPN service and access most network resources from a remote location.

The VPN system is provided by an enterprise class security vendor and is secured with the following:

- Enterprise standard SSL encryption,
- a proprietary application (i.e. standard Operating System clients will not work with the system),
- network rules which only allow the user to access the network resource or server that they require,
- Active Directory group membership – only members of the VPN security group will be allowed to connect to the system; and,
- all requests must be made through the ICT Helpdesk and approved by a relevant authority.