ICT CoP 05: System Security

1. Introduction

1.1 This Code of Practice defines the requirements, procedures and provides advice for managing systems that are used to connect to the Imperial network and/or access organisational data.

2. Scope

2.1 This Code of Practice applies to all members of Imperial, including staff, students, visitors and third-party contractors, who wish to connect any device to the Imperial network and/or access organisational data.

3. Roles and Responsibilities

3.1 This applies to Imperial owned devices.

3.2 The primary user of a system is the named individual who uses it for the majority of the time.

3.3 A custodian is a named individual who is responsible for ensuring that a system meets the requirements defined in the Information Security Policy and Code of Practice 5: Systems Security. Every system must have one and it must be a named member of staff. If a custodian is not defined, it will default to the Director of Operations for the Department.

3.4 A system administrator is either a named individual or a Team who performs administrative functions on a system. By default, systems will be administered by ICT.

4. Devices must

4.1 By default, be enrolled into ICT's management platforms.

4.1.1 Self-management of devices is permitted on request following a standard opt-out process. Opt-outs will be reported to the relevant Department. The named individual who approved the request will then become the custodian of the device and will be responsible for ensuring that the device complies with the Information Security Policy and Code of Practice 5: Systems Security.

4.2 Be protected by authentication methods as defined in Code of Practice 4: Account Security Management.

4.3 Be configured to automatically lock after 15 minutes of inactivity.

4.4 Require users to reauthenticate when waking from sleep mode.

4.5 Run supported operating systems & applications – i.e. still receiving security updates.

4.6 Be configured to automatically install security updates to both the operating system & applications by default.

4.7 Install applications from ICT provided or approved application store(s).

4.7.1 If an application is not available, then installed from trusted/approved locations/official stores.

4.8 Not undermine the built-in security features – e.g. jail breaking or rooting.

4.9 If available have endpoint protection (antivirus) installed, configured to automatically update and have real-time protection enabled.

4.10 If available, devices should be encrypted; preferably using tools built into the operating system.

4.11 If available have a software firewall installed/configured and enabled; preferably using tools built into the operating system.

4.12 If available, be configured to automatically wipe if incorrect passwords are repeatedly entered.

4.13 If available, devices should be configured to use remote wipe tools/capabilities.

4.14 When an individually assigned device (i.e. a laptop) is transferred to another primary user they must be securely wiped and configured for said new primary user.

4.15 Be configured so that a standard user account does not have administrative privileges; access to administrative privileges is limited to individuals with a business need.

4.16 Log authentication attempts – this is applied by default for ICT managed devices.

5. Vulnerability Management

5.1.1 Vulnerabilities should be remediated within the expected timelines:

- Security updates marked as Critical or High or with a CVSS (Common Vulnerability Scoring System) v3.0 base score of 7.0 or higher shall be patched within 14 days or less.
- Security updates marked as Medium or with a CVSS v3.0 base score between 4.0 or 6.9 shall be patched within 90 days or less.
- Security updates marked as Low or with a CVSS v3.0 base score between 0.1 or 3.9 shall be patched within 180 days or less.

5.2 If a vulnerability is being actively exploited, then these timeframes will be shortened.

5.3 If a vulnerability is not able to be mitigated within the defined time window, the risk will need to be recorded within Imperials risk management platform with mitigations identified and implemented.

6. Public Facing Servers

6.1 Public facing servers (i.e. web servers) are permitted upon request via the web exception process where there is a clear business need.

6.2 Must be hosted either within an Imperial approved data centre or an Imperial approved public cloud provider.

6.2.1 Public facing servers/services are not permitted on the campus/edge network.

6.3 Will be subject to routine vulnerability scanning.

6.4 Will be subject to routine web application vulnerability scanning – if applicable.

6.5 Will be protected by ICT's intrusion detection system (IDS) and intrusion prevent system (IPS) service.

6.6 The requirement for a server to be public facing should be reviewed every 6 months by the custodian.

7. Removeable Media

7.1 The use of removable media shall be avoided where possible and only used where there a clear business need and more secure, alternative options are not feasible (e.g., Imperial-provided collaboration solutions). Members of Imperial wishing to use removable media for storing university data should first consult with the ICT department to ensure more secure, alternative solutions are not available.

7.2 Imperial provided removable media devices shall be encrypted, in line with Imperial's Information Security and Data Protection policies.

7.3 Non-Imperial provided removable media devices should be encrypted, in line with Imperial's Information Security and Data Protection policies.

7.4 Removal of personal data, or devices containing personal data (or which can be used to access it), from Imperial's premises without appropriate security measures being in place (as set by Imperial's ICT Department) shall not be allowed.

7.5 Removable media must not contain the only copy of data.

7.6 As per the Information Governance Policy Framework. Sensitive or Special Category data, otherwise considered under the framework to be deemed 'Confidential' or 'Certified Environment', shall not be transferred to removable media devices, except where explicitly approved and provided by Imperial's ICT department and IAOs (Information Asset Owners) of the data. Where removable media is used for storing sensitive data, this will be managed as an exception.

7.7 Non-Imperial provided removable media devices shall not be used for storing university data considered to be Confidential or 'Certified Environment' under the Information Governance Policy Framework.

7.8 Imperial provided removeable media shall not be marked in such a way as to indicate the origin of the information (i.e. Imperial) nor its contents.

7.9 The threats and risks associated with the use of removable media for a given product or service will be identified, assessed and managed as part of the design process and will take into consideration the sensitivity and quantity of data that could be accessed or lost.

7.10 Loss or suspected loss of any Imperial provided removable media, or any non-Imperial provided removable media that contains or may contain university information, is to be raised as a cyber security incident with the ICT department and reported as a data breach.

7.11 Any Imperial data held on a removable media device, whether Imperial provided or not, is to be securely deleted in line with the Information Security and Data Protection policies, when no longer required, or when the device is passed to another party.

Document Control

Document title:		ICT CoP 05: System Security	
Version:	V1.0	**Date:**	September 2025
Initially approved by and date:		Chief Information Security Officer / 04-09-2025	
Version approved by and date:		Chief Information Security Officer / 04-09-2025	
Version effective from:		September 2025	
Originator:		Information and Communication Technology	
Contact for queries:		Chief Information Security Officer	
Cross References:		Information Security Policy CoP 01 – Hardware and Software Asset management CoP 02 – Electronic Messaging CoP 03 – Inspection of Electronic Communications and Data CoP 04 – Account Security Management CoP 06 – Conditions of Use of IT Resources	
Notes and latest changes:		May 2025 V0.0 Initial Draft developed V1.0 reviewed by the Joint Cyber Security Group	