Royal College
of Physicians

Cyber Information Security

Policy

Document control

Cyber Information Security Policy

Current version	0.5	
Date of current version	11/05/2018	
Document status	Draft	
Document classification	Cyber Information Security	
Owner	IT Services	
Approved by	Name	
	Role	
	Date	

Document revision history

Version	Date	Author	Summary of changes
0.1		NCC Group	Initial draft template for client use
0.2	21/04/2018	Awesta Sepahbod	Modified/updated
0.3	26/04/2018	Awesta Sepahbod	Updated
0.4	10/05/2018	Awesta Sepahbod	Updated
0.5	11/05/2019	Awesta Sepahbod	External

Table of contents

1 Purpose

- This policy defines requirements for information security within the Royal College of Physicians (RCP) for confidential or private data including cardholder data.
- This policy sets out the high-level objectives that must applied to RCP systems and behaviours that must be adopted by RCP users. The Information Security Policy does not define *how* objectives should be met, it only describes the expected, minimum security requirements. RCP users must refer to other supporting procedures and standards when determining how to achieve the policy objectives set out below.
- The Information Security Policy is issued and managed under the authority of the senior information risk owner (SIRO).

2 Scope

This policy defines expected controls all for users, processes and IT systems within the RCP.

3 Introduction

- Protection of information assets is the primary goal of cyber information security. This includes practising behaviours to reduce the overall occurrence of theft, loss or misuse of information assets.
- A breach in information security or loss of information assets can have serious consequences, depending on the sensitivity and value of the information and the extent of the breach. The consequences can include:
    - disclosure of personal information
    - interruption in the company’s ability to deliver services
    - financial losses related to correcting the situation
    - threats to public safety or individuals’ health and wellbeing
    - regulatory fines
    - legal actions
    - erosion of the public trust in the company.
- Individual actions and behaviours of RCP users are critical to protecting the information assets. Technology and policies are only effective if users are aware of their responsibilities, policies and supporting procedures. Education and awareness are essential to promote an understanding of the importance of information security.

4 Roles and responsibilities

4.1 Personnel

- RCP users are responsible for understanding their responsibilities as defined in the Acceptable Use Policy.
- RCP users must know their responsibilities for the protection of information and information assets.
- RCP users must protect credentials, eg personal identifiers, passwords, access cards, keys and tokens.
- RCP users must attend information security awareness, education and training offerings.
- RCP users must be aware of and understand security policy and practices.
- RCP users must obtain management approval for personal use of information resources.
- RCP users must understand what constitutes an actual or suspected breach of information security, and raise a service desk ticket within 24 hours of a security incident.

4.2 Line management

- Line managers must ensure their RCP users attend awareness training upon hire and annually thereafter.
- Line managers must ensure their RCP users have access to applicable policies and procedures, and are aware of where they are located.
- Line managers must ensure their requests for access are limited to the privileges needed for the RCP users' role.
- Line managers must ensure that upon leaving RCP employment, their RCP users' access is immediately revoked by informing HR, site security and IT.

4.3 Senior management

- The senior information risk owner (SIRO) is responsible for cyber information security within the RCP.
- The SIRO must approve any exceptions to this policy.
- The SIRO is responsible for distributing this policy, and supporting policies, procedures and standards to the relevant users.
- The head of Cyber Information Security is responsible for ensuring that this policy complies with the latest version of the Payment Card Industry Data Security Standard (PCI DSS), Cyber Essentials plus and ISO 27001.
- The head of IT Services is responsible for ensuring that systems and resources are available for monitoring and responding to security alerts.
- The head of Cyber Information Security is responsible for creating and distributing incident response procedures.
- The head of IT Services is responsible for ensuring user accounts and authentication is securely managed.
- The head of IT Services is responsible for ensuring access to private and confidential data including cardholder data is suitably monitored.

5 Network Security

5.1 Firewall management

- All firewalls must be managed with documented roles and responsibilities for:
  - approving changes
  - implementing changes
  - operational management.
- All changes to firewall or routers must be a documented process, and must include:
  - testing any network and configuration changes
  - approving any network and configuration changes.
- Firewall and router rules must be reviewed by suitably qualified personnel at least every 6 months and the results must be documented.
- All outbound traffic to the internet must be explicitly authorised by the head of IT services.
- Insecure services must be justified and approved by the head of IT services who must implement suitable technical controls to secure the service depending on the data involved, the application in question and the associated risks.
- All system components that provide publicly accessible services must be authorised by the head of IT services and be documented in design documentation.
- Firewall documentation.
- All networks must be documented in a version-controlled network diagram, which accurately describes the network environment.
- All network diagrams must be updated following significant changes to the network, system or application architecture.
- All firewall and routers must be built following the documented configuration standards.

5.2 Firewall architecture and configuration

- Firewalls must be placed between internal RCP networks and public networks including (but not limited to) the internet.
- Firewalls must be placed between internal RCP networks and demilitarised zone (DMZ) networks. All firewalls must be configured to a default 'deny-all' so that any network traffic not specifically authorised is blocked.
- Router configuration files must be stored on systems that restrict access to personnel with a need to access the files.
- All inbound traffic from public networks including (but not limited to) the internet must route through firewalls into a DMZ and must not directly route into internal networks.
- All firewalls must be configured with anti-spoofing settings or technology.
- All outbound traffic to the internet must be explicitly authorised by the head of IT services.

- All firewalls must permit only established connections into the network and deny any inbound connections not associated with a previously established session by performing stateful inspection of traffic or similar means.
- All systems that store confidential or private data must be located on internal network zones, segmented from other untrusted networks such as DMZs.

5.3 Wireless networks

- All wireless networks must only connect to other RCP networks through a firewall that restricts traffic in accordance with sections 5.1–5.3.
- Wireless keys must be changed from the default factory setting value before a wireless access point can be used.
- Simple Network Management Protocol (SNMP) Community strings of wireless access point must be removed before a wireless access point can be used.
- All vendors default passwords must be changed before a wireless access point can be used.
- The wireless access point firmware must be updated in accordance with section 9 of this policy and support strong encryption as defined in the Information governance policy.

System builds

6.1 Configuration build standards

All systems must have vendor default settings removed or changed including but not limited to:

- Default passwords.
- SNMP settings.
- All systems must be built to documented configuration standards.
- All configuration standards must be aligned with external standards from the SANS Institute or the National Institute of Standards and Technology (NIST).
- All configuration standards must be updated as new vulnerabilities are identified following the procedures described in section 9 of this policy.
- All new systems must be deployed with the latest up-to-date configuration standard.
- Configuration standards must document necessary protocols and network services that are enabled on the system.
- Configuration standards must document unnecessary software, scripts, drivers, features and subsystems removed from systems.
- Configuration standards must document security parameters that must be defined on the systems.
- All servers must be deployed with only one primary function.

6.2 System management services

- All management ports and services must be configured to use strong encryption over protocols as defined in the RCP's Encryption Standard.
- Insecure management protocols (eg telnet, rlogin) must be disabled on all systems.

7 Data security

7.1 Data storage

- All data must be handled in accordance with the information governance policy.
  - Sensitive authentication data (SAD) must never be stored post authorisation.
  - Cardholder data must only be stored, processed or transmitted with the approval of the executive director of Corporate Services.
  - If full primary account numbers (PAN) are stored, any digits beyond the first six and last four must only be visible to personnel or teams who have explicit authorisation and a validated business requirement from the executive director of Corporate Services.
  - All cardholder data must be protected via strong cryptography as defined in the RCP Encryption Standard.
  - If encryption is used to protect confidential or private data including cardholder data then encryption keys must be managed following the RCP Encryption Standard

7.2 Data transmission

- All confidential or private data including cardholder data must be encrypted across public networks using strong cryptography as defined in the RCP Encryption Standard.
- Confidential or private data including cardholder data must never be sent via messaging technologies (eg email, link or Skype) unless protected in accordance with the RCP Encryption Standard.

8 Anti-virus

8.1 Anti-virus configuration

- Anti-virus software must be deployed on all systems that are commonly affected by malware including Windows operating systems and Mac OS desktop.
- Systems considered to be not commonly affected by malicious software must be periodically re-evaluated to confirm whether such systems continue to not require anti-virus software.
- Anti-virus software must be centrally managed.
- The anti-virus management server must have anti-virus client software deployed.
- All anti-virus clients must be active, running and be tamper proof.
- All anti-virus clients must be configured to update signatures automatically.
- All anti-virus client software must be kept up to date.

9 Patching and vulnerability management

9.1 Patch management

- Patches must be applied following a documented procedure; the patch management procedure.
- Updates from vendors of all systems (off-the-shelf applications, payment applications (including those that are payment application (PA)-DSS validated and those that are not), middleware, operating systems and network devices) must be reviewed fortnightly to identify patches and apply critical security updates.
- Critical security updates from vendors must be applied to all systems within 10 days of being released by the vendor.

9.2 Vulnerability management

- A vulnerability management program must be maintained by IT Services, which identifies new vulnerabilities for all systems (off-the-shelf applications, middleware, operating systems and network devices).
- Vulnerabilities must be tracked and managed using the Common Vulnerability Scoring System (CVSS).
- Sources of vulnerability information must include vendors, independent researchers and the results of network testing activities.

10 Software development

All software application must be developed as defined in the Secure Software Development Policy. This includes writing code securely following the secure development lifecycle and performing code review for all software that is created by the RCP.

11 Change management

All changes within the RCP environment must follow the System Configuration and Change Management Policy.

12 Access control

12.1 Access control policy

All access to RCP systems must be managed following the Access Control Policy.

13 Physical security

13.1 Physical site access and security policy

All access to RCP sites must follow the Physical Security Policy.

13.2 Media security

All physical media in the cardholder data environment must conform to the Physical Security Policy.

14 System logging

14. 1 System log configurations

All systems must have active and enabled logging features in line with System Configuration and Change Management Policy.

14.2 Time settings

- All systems must receive time updates from authorised internal time servers.
- Authorised internal time servers must only receive time updates from industry accepted external sources.
- Access to time / network time protocol (NTP) configurations on systems must be limited to personnel with a need to access time / NTP settings.
- Changes to time / NTP configurations on systems must be detected and alert monitoring personnel, and be investigated.

14.3 Audit trail security

- Access to audit trails must be limited solely to users with a job related need to view audit logs.
- Modifications to stored audit logs must be detected, alerted and investigated by Cyber Information Security.
- Audit trails must be stored on a centralised server or be backed up.
- Logs to externally facing systems (eg webserver firewalls) must be written to internal systems.
- All logs must be monitored and reviewed regularly.
- Log data must be stored for 12 months and 3 months of data must be immediately available for online review.

15 Network testing

15.1 Wireless testing

- All sites storing, processing or transmitting confidential or private data, including cardholder data, must be subject to wireless security tests on a quarterly basis.
- Wireless tests must follow a documented methodology that is that is capable of detecting all types of wireless devices and must include a physical inspection of server rooms, data centres and racks.
- The detection of an unauthorised wireless access point within RCP premises must be reported and be managed through the security incident management process.

15.2 Network vulnerability scanning

- Vulnerability scans must be conducted within networks storing confidential or private data, including cardholder data, on a quarterly basis.
- External vulnerability scans must be completed by an approved scanning vendor on a quarterly basis.
- All significant changes, as defined in the System Configuration and Change Management Policy must be followed by an internal and external scan of the affected system components.
- All vulnerabilities identified during scans must be managed through the vulnerability management programme and be remediated.
- Following remediation, all scans must be repeated against systems where vulnerabilities were identified to confirm the vulnerability no longer exists.
- All scans must be completed / initiated and results reviewed by knowledgeable users.

15.3 Penetration testing

- Penetration test must be completed against networks storing confidential or private data, including cardholder data, on an annual basis.
- Penetration tests must follow an industry-accepted penetration testing approach.
- Penetration tests must include all systems within the defined scope including operating systems and network components.
- Penetration tests must include tests covering layers 2–7 of the open system interconnection (OSI) model.
- Penetration tests must be completed by an approved scanning vendor.
- Where a penetration test is carried out by an internal resource, the resource must be organisationally independent of the systems being tested.
- All significant changes, as defined in the System Configuration and Change Management Policy, must be followed by a penetration test of the affected system components.

16 Monitoring tools

16.1 Intrusion detection and prevention systems

- Intrusion detection systems (IDS) / intrusion prevention systems (IPS) must be deployed within networks storing confidential or private data, including cardholder data.
- IDS / IPS must be configured to monitor all traffic within the network and alert on suspected attacks to IT Services and Cyber Information Security.
- IDS / IPS systems must be maintained by applying vendor patches following the patch management procedure.
- IDS / IPS systems should ideally have signatures applied immediately and must have signatures applied within 72 hours of release by the vendor.

16.2 File integrity monitoring

- File integrity monitoring (FIM) or other change detection mechanisms must be deployed on systems storing confidential or private data, including cardholder data.
- Change detection solutions must monitor all critical files.
- Change detection solution must scan critical files weekly at a minimum.
- Change detection solution must alert the IT Services of any unauthorised changes to critical files.

February 2019