ROYAL
COLLEGE OF
PHYSICIANS
OF IRELAND

Information Security Policy (ISMS-Pol-101)

Document Title	Information Security Policy
Document Number	ISMS-Pol-101
Version	1.0
Department	IT Services
Owner/Responsible for Implementation	CTO
Approving Body	Executive Board
Effective date:	January 2021
Next Review date:	January 2023
Related Documents	DP-Pol-089 – Records Management Policy DP-Pol-090 – Data Protection Policy ISMS-Pol-102 – Acceptable Use Policy ISMS-Pol-103 – Web and Social Media Policy ISMS-Pol-104 – Remote Access Policy ISMS-Pol-105 – Access Control Policy ISMS-Pol-106 – Vulnerability and Patch Management Policy ISMS-Pol-107 – Mobile Phone Policy

1. Purpose

The purpose of this Policy is to protect the information assets of the College from all threats - internal, external, deliberate, or accidental.

The policy is aimed at:

- Safeguarding the availability, confidentiality, and integrity of the College's information.
- Protecting the IT assets and services of the College against unauthorised access, intrusion, disruption, or other damage.
- Ensuring compliance with applicable legislation and regulations.
- Providing a governance structure with clear lines of responsibility and accountability.
- The policy has been written to provide a mechanism to establish procedures to protect against security threats and minimise the impact of security incidents.

2. Scope

This Policy applies to all Users of the College's IT resources which includes, without limitation, its network (accessed on site or remotely) and/or communications devices/platforms and non-IT information assets.

3. Responsibilities

IT Services are responsible for creation and maintenance of this policy and ensuring College information is protected in accordance with this policy and other supporting documentation.

All users, learners and staff are required to demonstrate compliance to RCPI's Information Security Policy (ISMS-Pol-101) in order to protect the confidentiality, integrity, and availability of RCPI's Information Assets. This policy also extends to contractors, consultants and/or 3rd parties providing services to RCPI.

4. Definitions

- CIA Triad: Information Security aims to protect 3 main components relating to information; Confidentiality, Integrity and Availability.
- Confidentiality: Protecting information from users and other entities who not authorised to view, process or store it.

- Integrity: Ensuring that the information is protected against unauthorised deletion or manipulation intentionally or unintentionally while in transmit or where it is stored.
- Availability: Ensuring that the information is accessible when needed.

5. Data Classification & Management

5.1 College is obligated to respect the rights of individuals and to protect confidential data.

5.2 When data is classified as confidential data, appropriate access and security controls are applied in transmission and storage. Confidential data is not to be transmitted without adequate precautions being taken to ensure that only the intended recipient can access the data.

5.3 All College information is to be treated as confidential unless otherwise indicated.

5.4 Where RCPI engages the use of Cloud or external hosting services, which will host RCPI data, any proposed solutions must be evaluated and approved by the RCPI Senior Management Team.

5.5 Where data and servers on the RCPI network are accessed by 3rd parties (suppliers, contractors, consultants) for support and maintenance provided to RCPI, a 'Third Party Access form' with the accompanying Data Protection agreements must be built into the service agreement with the 3rd Party.

5.6 Information may exist in different formats (electronic or physical) in different locations (file server, emails, backup tapes etc). Proper data retention policies should be assigned to data and data should be disposed of when this time expires.

5.7 Information assets should be labelled where possible. It can be automated (i.e. adding metadata to document) or manual (i.e. stickers on equipment, footer in documents etc).

5.8 For the details of the Data Management rules, the Records Management Policy (DP-Pol-089) must be consulted

6. Network and System Security

6.1 RCPI protects its network against internal and external threats via perimeter firewall. Different zones are created to separate the assets from internet, local network and themselves.

6.2 Only necessary protocols and ports are to be allowed between sources and destinations. None of the internal or external sources should have unlimited access.

6.3 A Zero-Trust approach should be applied across the organisational network where applicable. Access to data or systems should not be solely based on the user having network access.

6.4 All Operating Systems must be maintained at a supported current version.

6.5 Quarterly malware scans must be performed on the systems to find and delete malicious codes.

6.6 User web access must be established through RCPI's official security gateways. Users are not allowed to by-pass any security systems (e.g. firewall, URL filtering etc)

6.7 Users are not allowed to change the security settings of College Operating Systems, Browsers and the applications that these are running on the systems.

7. Authentication, Authorisation & Accounting (AAA)

7.1 Authentication

7.1.1 All users, applications, web services etc must be authenticated before accessing RCPI resources.

7.1.2 Authentication must be completed with unique user accounts. Shared user accounts are not allowed.

7.1.3 Multi-Factor authentication must be applied for the critical system access (e.g. VPN) where available.

7.1.4 The account credentials assigned to users must not be shared with any others and must be kept confidential.

7.1.5 All users are responsible for activities that are performed via their assigned accounts (non-repudiation)

7.1.6 multiple applications. Even when SSO mechanisms are used, users must be still identified uniquely.

7.1.7 Users should not cache the credentials on the devices those don't belong to RCPI.

7.1.8 Strong password policy rules are applied during the authentication on the systems where possible. The password policy rules are defined below:

7.1.9 RCPI may provide federated authentication to provide Single Sign-On (SSO) for easy authentication to

7.1.10 Have a length of 10 – 14 characters

7.1.11 Apply password history rules (remembering specific number of old passwords and not allowing re-use of them).

7.1.12 Be a combination of three (3) of the following character sets: Upper- & Lower-case letters, Numbers and Symbols

7.1.13 Have a maximum lifetime of 90 days

7.1.14 For the systems where the above password policy is not applicable, they should be configured as stated in Access Control Policy.

7.1.15 Users must follow best practices to prevent misuse, loss or unauthorised access to systems:

7.1.16 Choose password which is unpredictable. Do not use your or family member name, birthdate, marriage date, sports team etc.

7.1.17 IT Administrators may send temporary account passwords via encrypted email to HR during the New Starter process

7.1.18 Change temporary passwords at first logon

7.2 Authorisation

7.2.1 Need-to-know basis and Least Privilege Principles must be followed for authorising users to access to the systems. Therefore, staff are granted with limited access to allow them to carry out their job functions.

7.2.2 If any user changes department, the previous access rights must be revoked based on (Joiners, Movers & Leavers) JML Process and new job definition requirements should be assigned to the user.

7.2.3 When a user leaves RCPI or a contract ends for a third party, all user accounts must be disabled and deleted immediately. (Leavers Process)

7.2.4 Users should not have administrative access rights on their computers. Only an authorised, limited number of staff can have these access rights in alignment with their job definitions.

7.2.5 Users who have administrative access to the systems must have two separate accounts. Normal account which is used for daily activities (such as logging on the PC and working on spreadsheets etc) must not have administrative rights on systems

7.2.6 Privileged Identity Manager must be used to managed privileged accounts

7.3 Accounting

7.3.1 All activities including logon/logoff must be logged.

7.3.2 Failed logon attempts must be logged on systems to get notified about brute force/dictionary attacks.

7.3.3 Audit logs must be protected against manipulation and digitally signed where available.

7.3.4 Security logs must contain at least following information:

7.3.5 Username

7.3.6 Date/time

7.3.7 Activity

7.3.8 Source and Destination IP Address

7.3.9 Success/Fail information

7.3.10 Targeted object (i.e. Password reset on which account name)

7.3.11 Time synchronisation systems (i.e. NTP servers) must be used to synchronise all system times for accuracy of the event logs.

7.3.12 Privileged accounts must be monitored more detail

7.3.13 Security logs should be sent to a separate system (e.g. SIEM) to collect, correlate and store. Access to these logs should be restricted to prevent log corruption, deletion, modification.

8. Encryption

8.1 All College owned laptops must have their internal hard drive encrypted and protected with a boot PIN. This is a service supported by the IT Services

8.2 Where sensitive information is transmitted through a public network to an external third party the information must be encrypted and sent via secure channels (SFTP, SSH, HTTPS, VPN etc.)

8.3 WIFI networks advertised for staff business use (e.g. EDUROAM) must be encrypted using WPA2 or better.

8.4 All SSL versions as well as TLS versions prior to 1.1 are not allowed. TLS 1.2 or higher should be used during secure communications.

8.5 Weak encryption and hashing algorithms should not be used e.g. DES, RC4, SHA1. This evaluation must be done based on current status of these algorithms.

8.6 Cleartext communication channels must not be used and disabled on system access like Telnet, HTTP etc.

8.7 Private keys of PKI must be protected properly, and the passwords of these key must be kept secret.

8.8 SSL Certificate lifecycle must be followed effectively and must be renewed with the most current algorithms.

8.9 Passwords must be stored in one-way encryption formats (hashing). Hash salting should be used where available.

9. Information Security Awareness

9.1 IT Security awareness strategy is delivered through multiple methods with the aim of raising user awareness and highlighting end user responsibilities.

9.2 Scheduled targeted Security Awareness Training sessions are available on demand in conjunction with Data Protection training.

9.3 During staff induction new hires are briefed on all policies.

9.4 User awareness must be assessed via different methods like quiz, phishing campaigns, competitions etc.

9.5 Security awareness materials must be provided where available (i.e. posters, Logon messages etc)

9.6 Users must follow the Clean-Desk & Clean-Screen Policy which covers:

- Do not leave your computer unattended without locking your computer or logging off.
- Do not write down your passwords

- Do not leave sensitive documents unattended on your desk, printer and communal areas
- Shred the documents that need to be disposed of
- Do not leave your mobile phone unattended and always use screen-lock

10. Business Continuity & Disaster Recovery Strategy

10.1 Main goal is to provide the Business Continuity before it turns to a Disaster Recovery phase.

10.2 Highly available systems and infrastructure should be setup and maintained where available (i.e. cluster systems, backup lines etc) to support the approach cited above.

10.3 It is the responsibility of the business owner of each service to ensure that an adequate business continuity plan is in place in the event that the service is affected by the non-availability of the relevant servers, network or other elements of the IT infrastructure. Prevention of data loss should be ensured through data back-ups.

10.4 IT Services maintains Disaster Recovery plans for all RCPI centrally managed infrastructure and critical services.

10.5 Disaster Recovery plans and processes are tested regularly

10.6 The IT Services manage data and system backups for critical systems

11. Incident Management

11.1 Formal incident management procedures are in place for IT Security incidents and procedures relating to personal data breaches. Please reference IT Policy' for policy breach process

11.2 All staff are responsible to report incidents or suspicious activities to IT Services.

11.3 Proper incident response handling guidelines and playbooks must be created to be prepared to handle any future incidents.

11.4 All incidents must be recorded with the information below:

- Notification Time
- Notifying staff/party
- Location
- Details of incident
- IT Services is responsible to perform Triage to the reported incidents and appropriate actions must be taken to deal with the incident. IT Services is responsible to record the following information

- Incident criticality
- Actions taken
- Closure time

11.5 Appropriate preventive actions should be taken to prevent the occurrence of similar incidents in the future

11.6 The details should be recorded as part of a knowledgebase as Lessons-Learned for future staff.

12. Physical Computer Storage Environmental Provisions

12.1 All hardware used for the storage of College data is to be purged of data and securely destroyed once it is no longer to be used.

12.2 When tapes and other secondary storage devices reach the end of their useful life, they are to be purged of RCPI Data and securely destroyed.

12.3 This security policy is intended to ensure an effective IT infrastructure for the benefit of all users. Where necessary, support will be provided by IT Services to assist users in complying with the policy.

12.4 IT Security Governance

12.5 IT Security is governed in RCPI through

12.6 Yearly External Audit for financial systems

12.7 RCPI Risk Register

12.8 IT Risk Register

12.9 To be able to complete the tasks above, RCPI should create Asset Inventory which may guide to create Risk Registers.

12.10 Proper Risk Management Process must be documented and followed.

12.11 Risks must be reviewed, and Risk Registers must be approved by senior management formally.

12.12 Appropriate risk management techniques must be applied to the risk with the following options:

- Risk Mitigation
- Risk Acceptance
- Risk Avoidance
- Risk Transfer