IT-POL-101 - Information Security Policy

Policy title:	**Information Security Policy**
Policy reference:	**IT-POL-101**
Department:	**IT Services**
Owner:	**Michael Hughes**
Approving body	**SMT**
Effective date:	**01/01/2023**
Next review date:	**30/09/2026**
Version Control	**5.0**
Related Policy and/or Procedures	• IT-POL-101-Information Security Policy • IT-POL-102-Acceptable Use Policy • IT-POL-103-Web & Social Media Policy • IT-POL-104-Remote Access Policy • IT-POL-105-Access Control Policy • IT-POL-106-Vunerability & Patch Management Policy • IT-POL-107-Antivirus & Malware Policy • IT-POL-108-Business System Owner Policy • IT-POL-109-Asset Management Policy & Procedure • IT-SOP-120-Business Health & IT Security Cloud Assessment Questionnaire • DP-POL-089-Records Management Policy • DP-POL-090-Data Protection Policy • DP-POL-083-Breach Management Policy & Procedure

ROYAL COLLEGE OF PHYSICIANS OF IRELAND

Contents

1. Purpose

The purpose of this Policy is to protect the information assets of the RCPI from all threats - internal, external, deliberate, or accidental. The policy is aimed at:

- Safeguarding the availability, confidentiality, and integrity of the RCPI's information.
- Protecting the IT assets and services of the RCPI 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 RCPI'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

- Senior Leadership Team (SLT)
    - The SLT is responsible for distributing the IT Information Security Policy to all heads of Departments & Faculties and for supporting the Chief Technology Officer in the enforcement of the policies where necessary.

- Line Managers
  Each Line Manager is responsible for:
    - The implementation of this policy and all other relevant RCPI policies within the business areas for which they are responsible.
    - The ownership, management, control, and security of the information processed by their team or service on behalf of the RCPI.
    - The ownership, management, control, and security of RCPI information systems used by their team or service to process information on behalf of the RCPI.
    - Ensuring that all members of staff who report to them are made aware of and are instructed to comply with this policy and all other relevant RCPI policies.
    - Consulting with the HR, IT, Legal and Data Protection Department in relation to the appropriate procedures to follow when a breach of this policy has occurred.

- IT Services
  The I.T. Department is responsible for:
    - Creation and maintenance of this policy and ensuring RCPI information is protected in accordance with this policy and other supporting documentation.
    - The management, control, ownership, security, and integrity of all RCPI network domain (LAN/WAN/Wi-Fi) on behalf of the RCPI.
    - Ensuring adequate procedures are in place to ensure compliance with this policy and all other relevant policies.
    - Ensuring adequate technologies are in place to ensure compliance with this policy and all other relevant policies.
    - Providing information owners or their nominees with audit reports and user access lists for information systems which are directly managed by the IT Services.

- User
    - All users, trainees and staff are required to demonstrate compliance to RCPI's Information Security Policy 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.
    - Respecting and protecting the privacy and confidentiality of the information systems and network they access, and the information processed by those systems or networks.
    - Complying with instructions issued by designated information owners, system administrators, network administrators and/or the I.T. Department on behalf of the RCPI.
    - Reporting all misuse and breaches of this policy to their Line Manager.
- CTO

  Is responsible for:
    - the management of the College Network and for the provision of support and advice to all nominated individuals with responsibility for discharging these policies
    - Advising the SMT, the College officers, Line Manager, Administrators, and other appropriate persons on compliance with this policy and its associated supporting policies and procedures.
    - Reviewing and updating the Security policy and supporting policies and procedures.
    - The promotion of the policy throughout College.
    - Periodical assessments of security controls as outlined in the Security Policy and supporting policies and procedures.
    - Investigating security Incidents as they arise.
    - Maintaining records of Security incidents. These records will be encrypted and stored securely for six months after which time information pertaining to individuals will be removed. The records will then be held in this anonymous format for a further two years for statistical purposes.
    - Reporting to the SLT, the College officers, Administrators, and other appropriate persons on the status of security controls within the College.

4. IT Security Policy - Guiding Principles

4.1 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 authorized 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.

4.2 Data Classification & Management

4.2.1 RCPI is obligated to respect the rights of individuals and to protect confidential data.

4.2.2 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.

4.2.3 All RCPI information is to be treated as confidential if not otherwise indicated.

4.2.4 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.

4.2.5 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.

4.2.6 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.

4.2.7 Information assets will 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).

4.2.8 For the details of the Data Management rules, Records Management Policy must be consulted.

4.3 Network and System Security

4.3.1 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.

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

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

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

4.3.4 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)

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

4.4 Authentication, Authorisation & Accounting (AAA)

4.4.1 Authentication

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

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

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

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

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

4.4.1.6 RCPI may provide federated authentication to provide Single Sign-On (SSO) for easy authentication to multiple applications. Even when SSO mechanIT are used, users must be still identified uniquely.

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

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

- Have a length of 10 or more characters.
- Apply password history rules (remembering specific number of old passwords and not allowing re-use of them).
- Be a combination of three of the following character sets: Upper- & Lower-case letters, Numbers and Symbols
- Have a maximum lifetime of 90 days.

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

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

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

4.4.1.12 IT Administrators or MSP (Managed Services Provider) IT Personnel may send temporary account passwords via encrypted email or Teams message to HR and starter Manager during the New Starter process.

4.4.1.13 Change temporary passwords at first logon.

4.4.2 Authorization

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

4.4.2.2 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.

4.4.2.3 When a user leaves RCPI or a contract ends for a third party, all user accounts must be disabled immediately and follow the default 6-month period before account is deleted following existing (Leavers Process).

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

4.4.2.5 Users who have administrative access to the systems must have 2 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.

4.4.2.6 Privileged Identity Manager must be used to managed privileged accounts.

4.4.3 Accounting

4.4.3.1 System activity logs, including logon and logoff events, are maintained to help ensure the security and reliability of our IT environment. These logs are used solely for safeguarding organisational assets, supporting incident investigations, and meeting compliance requirements. Individual privacy is respected, and access to logs is strictly controlled.

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

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

4.4.3.4 Security logs must contain at least following information:

- Username
- Date/time
- Activity
- Source and Destination IP Address
- Success/Fail information.
- Targeted object (i.e., Password reset on which account name)

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

4.4.3.6 Privileged accounts must be monitored more detailed.

4.4.3.7 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.

4.5 Encryption

4.5.1 All RCPI owned laptops must have their internal hard drive encrypted and protected with the latest Hardware encryption available. This is a service supported by the IT Services/ MSP.

4.5.2 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.)

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

4.5.4 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.

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

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

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

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

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

4.6 Cloud Security

4.6.1 Identity & Access Management

4.6.1.1 **Azure AD Tenant:** All identities are managed via Azure AD (Tenant ID: 4bdbc99f-14d5-40ac-8220-5a85d6b6fe7d).

4.6.1.2 **Directory Synchronisation:** Hybrid identity is enabled via AZDCPRD02 sync server. Sync health is monitored regularly.

4.6.1.3 **Hybrid Device Registration:** Windows devices with domain controller visibility are auto registered with Azure AD.

4.6.1.4 **Multi-Factor Authentication (MFA):** Required for all external access to Office 365 services.

4.6.1.5 Apply the **principle of least privilege,** review access quarterly.

4.6.1.6 Privileged accounts must use **Privileged Identity Management (PIM)**.

4.6.2 Device Management

4.6.2.1 **Mobile Device Management (MDM):** Microsoft Intune is deployed for Windows devices. Enrolment is mandatory for all staff devices.

4.6.2.2 **Mobile Application Management (MAM):** Conditional access policies enforce MFA and app protection policies.

4.6.2.3 **Legacy Policies:** The legacy mailbox policy (RCPI default) will be deprecated post full Intune rollout

4.6.3 Data Protection

4.6.3.1 **Data Loss Prevention (DLP):** DLP policies must be configured for Exchange, SharePoint, and OneDrive to detect and prevent leakage of sensitive data (e.g., PPS numbers, banking details).

4.6.3.2 **Policy Tips and Activity Tracking:** Policy tips and activity tracking are enabled to help inform and guide users about security best practices, and to generate audit trails that support the protection of organisational data. These features are designed to assist users in making secure choices and to ensure compliance with legal and regulatory requirements. All activity tracking is handled in line with our commitment to privacy and is only used for legitimate security and compliance purposes.

4.6.3.3 **Encryption:** SSL/TLS for data in transit; BitLocker for data at rest.

4.6.3.4 **Backups of critical workloads** must be performed regularly and tested quarterly.

4.6.4 Network Security

4.6.4.1 Use **Azure Firewall, Network Security Groups (NSGs)**, and **conditional access policies** to restrict access.

4.6.4.2 No direct exposure of administrative ports (e.g., RDP, SSH) to the internet.

4.6.4.3 Apply **Zero Trust principles** for all connections.

4.6.5 Logging and Monitoring

4.6.5.1 Enable **Azure Security Centre** and **Microsoft Defender for Cloud/Office 365.**

4.6.5.2 Log all administrative actions; retain logs for a minimum of **12 months.**

4.6.5.3 Enable **alerting and automated responses** for suspicious activity.

4.6.6 Compliance and Monitoring

4.6.6.1 **Ensure compliance with** GDPR, ISO 27001 (and/or latest), and Irish Data Protection Commission guidance**.**

4.6.6.2 **Review third-party cloud providers for compliance certifications annually.**

4.6.6.3 **Conduct regular** penetration testing **and** vulnerability scans**.**

4.6.6.4 **Microsoft Compliance Manager**: RCPI maintains a compliance score (currently 69%) with ongoing remediation of high-risk items.

4.6.6.5 **Activity Policies**: Custom policies to detect suspicious usage patterns.

4.6.6.6 **Customer Lockbox**: Enabled to control Microsoft engineer access during support cases.

4.6.6.7 **Legacy Authentication**: Blocked via Conditional Access policies.

4.6.6.8 **OAuth App Monitoring**: Automated alerts for high-permission apps.

4.6.6.9 **Cloud Discovery**: Alerts for new/trending apps and anomalies.

4.6.6.10 **Sign-in and User Risk Policies**: Enabled to challenge suspicious activity and compromised accounts.

4.6.7 Email and Communication Security

4.6.7.1 **Exchange Online Protection (EOP)**: Hardened configurations for connection, policy, and content filtering.

4.6.7.2 **Mail Flow Connectors**: Configured for TLS, SMTP relay, and app integrations. Regular reviews ensure no misconfigurations.

4.6.8 Collaboration and Sharing Controls

4.6.8.1 **OneDrive & SharePoint**:

- Default sharing link type set to “Specific People”.
- Links expire after 30 days.
- External sharing restricted via domain whitelisting.

4.7 Information Security Awareness

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

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

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

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

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

4.7.6 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.

4.8 Business Continuity & Disaster Recovery Strategy

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

4.8.2 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.

4.8.3 It is the responsibility of the business owner of each service to ensure that an adequate business continuity plan is in place if 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.

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

4.8.5 Disaster Recovery plans and processes are tested regularly.

4.8.6 The IT Services manage data and system backups for critical systems.

4.9 Incident Management

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

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

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

4.9.3 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.

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

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

4.10 Physical Computer Storage Environmental Provisions

4.10.1 All hardware used for the storage of RCPI data is to be purged of data and securely destroyed once it is no longer to be used by the IT Department.

4.10.2 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 by IT Services.

4.10.3 Unallocated hardware that is found in the office (laptops with no tags, USB devices, strange electronics etc) will be flagged with IT Services for this to be investigated, checked and purged if necessary to ensure no malicious content harming the network and security in RCPI infrastructure. The test will be conducted on a laptop that is off the domain, off the network and not connected to the internet to be scanned before it is checked for malicious content or in a similar safe manner.

4.10.4 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.

4.11 IT Security Governance

4.11.1 IT Security is governed in RCPI through

- Yearly External Audit for financial systems
- RCPI Risk Register
- IT Risk Register

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

4.11.3 Proper Risk Management Process must be documented and followed.

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

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

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

5. Compliance & Breach of Policy

The RCPI will conduct cyber security compliance and assurance activities, facilitated by the RCPI IT security staff to ensure cyber security objectives and the requirements of the policy are met. Wilful failure to comply with the policy will be treated extremely seriously by the RCPI and may result in enforcement action on a group and/or an individual, may result in disciplinary action in accordance with RCPI procedures [for Staff] or reduction or withdrawal of services [for non-staff users]. If you have any questions or concerns about this policy, please discuss them with your line manager.

6. Review and Approval

This policy, and supporting documentation, will be reviewed, and updated annually or more frequently when best practice or the legislative/regulatory environment changes to ensure that they:

- remain operationally fit for purpose.
- reflect changes in technologies.
- are aligned to industry best practice.
- support continued regulatory, contractual, and legal compliance.

Changes to this policy will be presented to the RCPI SMT for review prior to publication.

Version	Date	Author	Approver	Notes
1.0	27/05/2020	Omer Altundal (Evros)	Joe Brady (Evros)	
2.0	15/01/2021	Alan O'Mahony	Michael Hughes	
2.1	01/01/2023	Shane O Neill	Michael Hughes	
3.0	28/03/2023	Shane O Neill	SMT	
4.0	27/12/2023	Eduards Jutanovs & Michael Hughes		Updates to reflect RSM May'23 Data Protection Audit comments and as part of the annual review process
5.0	08/08/2025	Eduards Jutanovs & Michael Hughes		Updated to reflect improvement in our cloud security

7. Reference Documents

- Cybersecurity (sharepoint.com)