

IT-POL-105-Access Control Policy

Policy Title:	Access Control Policy
Policy reference Number:	IT-POL-105
Department:	IT Services
Owner:	Michael Hughes
Author:	Eduards Jutanovs Michael Hughes
Approving body	SLT
Effective date:	01/01/2023
Next review date:	30/09/2026
Version Control:	5.0
Related Policy and/or Procedures	<ul style="list-style-type: none"> • IT-POL-101-Information Security Policy • IT-POL-102-Acceptable Use Policy • IT-POL-104-Remote Access Policy • IT-POL-107-Antivirus & Malware Policy • IT-POL-108-Business System Owner Policy • IT-SOP-120-Business Health & IT Security Cloud Assessment Questionnaire • IT-SOP-305-Presidio Access Management Procedure • IT-SOP-306-Presidio GDAP Access Management Procedure • DP-POL-089-Records Management Policy • DP-POL-090-Data Protection Policy • DP-POL-083-Breach Management Policy & Procedure

Contents

1. Purpose.....	3
2. Scope	3
3. Responsibilities.....	3
4. Policy Principles.....	4
4.1 Access Rights and Privileges	4
4.2 Access control	5
4.3 Third Party Access	6
4.4 Password Policy	7
5. Compliance & Breach of Policy	9
6. Review and Approval	10
7. Reference Documents.....	10

1. Purpose

This policy outlines the RCPI's approach to access control of its computing facilities. It provides the guiding principles and responsibilities to ensure the RCPI's access control objectives are met.

The objectives for this policy are to:

- safeguard the RCPI's information from security threats that could have an adverse effect on its operations or reputation.
- fulfil the RCPI's duty of care toward the information with which it has been entrusted.
- protect the confidentiality, integrity, availability, and value of information through the optimal use of controls.

2. Scope

This policy is applicable across the RCPI and applies to:

- all individuals who have access to RCPI information and technologies.
- all facilities, technologies and services that are used to process RCPI information.
- all information processed, accessed, manipulated, or stored, in any format, by the RCPI pursuant to its operational activities.
- internal and external processes used to process RCPI information.
- external parties that provide information processing services to the RCPI.
- access to 'private' and 'confidential' data/information is governed by this policy.

There are no restrictions on access to 'public' information.

The policy will be communicated to users and relevant external parties.

3. Responsibilities

The following groups of people will have responsibilities for managing different aspects of this policy.

- RCPI IT Services
 - RCPI IT Services department is accountable for the effective implementation of this policy, and supporting information security rules and standards, within the RCPI.
- Business System Owners
 - Overall responsibility for the management of the system and its data.
- Business System Admin/Managers
 - Implement access requests ensuring that each user must only be able to access the information or resources necessary to do their job ("least privilege" or "least authority").
 - Ensure that the information resources are secured according to RCPI IT security policies.
 - Regularly review users' permissions.

- Line Managers
 - Approve access requests ensuring that each user must only be able to access the information or resources necessary to do their job (“least privilege” or “least authority”).
 - Regularly review their team’s permissions.
 - In the absence of an automated process, inform system owners of leavers to ensure that leavers’ accounts are disabled.
- All Staff (as users of digital systems) must
 - Know and comply with published policies and procedures.
 - Request appropriate permissions through line management.
 - Notify line managers when permissions are no longer needed.
 - Not share access credentials and, in this regard, take responsibility for all activity under their account.
- Users must
 - Be responsible to making informed decisions to protect the information that they process.
 - Familiarise themselves with the relevant policies governing the information and systems they access.
- Managed Service Providers (MSPs):
 - Must comply with all relevant access management procedures and policies.

4. Policy Principles

4.1 Access Rights and Privileges

- 4.1.1 All users must have a unique identifier that is assigned to them to perform their daily activities on the systems.
- 4.1.2 Users must not share any of the credentials which are assigned to them with any other internal or external party.
- 4.1.3 All users are responsible for the consequences of the actions undertaken by using the accounts assigned to them.
- 4.1.4 All access must be logged on the systems in detail where possible.
- 4.1.5 Users are not allowed to try to gain access to the systems where they are not authorized.
- 4.1.6 All access rights must be given after a formal request-approval process.
- 4.1.7 Least privileged and need-to-know basis principles must be followed while giving access to any user on any system.
- 4.1.8 Generic or group IDs will not normally be permitted as means of access to RCPI data but may be granted under exceptional circumstances if sufficient other controls on access are in place and the control is auditable.

- 4.1.9 Generic identities will never be used to access confidential data or personally identifiable data.
- 4.1.10 The allocation of privilege rights (for example, local administrator, domain administrator, super-user, root access) will be restricted, controlled, and not provided by default.
- 4.1.11 Authorisation for the use of such accounts will only be provided explicitly, upon written request from a head of function, and will be documented by the system owner.
- 4.1.12 No access to any staff IT resources and services will be provided without prior authentication and authorisation of a user's account.
- 4.1.13 Multi-factor authentication (MFA) will be required for all privileged access where it can be practically implemented.
- 4.1.14 Access to IT resources and services will be given through the provision of a unique user account and complex password.
- 4.1.15 Usernames and passwords are for individual use only, and must not normally be disclosed to third parties, whether within or outside the RCPI.
- 4.1.16 Any user knowing or believing that they have disclosed their account details, or who knows or suspects that their email account has been compromised, must contact the IT Service Desk immediately to outline the situation.

4.2 Access control

- 4.2.1 Access to confidential, restricted, and internal information will be limited to authorised persons whose job or study responsibilities require it, as determined by law, contractual agreement, and applicable RCPI policies and regulations. The responsibility to implement access restrictions lies with the data and systems owners.
- 4.2.2 Role-based access control (RBAC) will be used as the method to secure access to all resources.
- 4.2.3 An access control matrix must be created for critical systems to create a formal process. Access rights on these systems must be given by default based on the job titles or departments. All other extra access request must be handled as explicit access; business requirements and the risk of authorization must be considered during the approval decision process.
- 4.2.4 Access for remote users will be subject to authorisation and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access will be permitted to any network device or networked system.
- 4.2.5 The use of cloud-based systems must meet the access control provisions laid out in this policy.

- 4.2.6 Evaluation of access controls implemented in any cloud system is performed during the vendor assessment and implementation stages of any project, via the Business Health & IT Security Cloud Assessment processes.
- 4.2.7 Access rights will be reviewed regularly.
- 4.2.8 The Joiners, Movers, Leavers Procedure must be followed to revoke accesses from the systems when a user moves to another department or leaves the College. On the other hand, necessary access rights must be assigned to the user when a new employee joins College or moves to another department.

4.3 Third Party & Managed Service Provider (MSP) Access

- 4.3.1 Third parties are provided with accounts that solely provide access to the systems and/or data they are contracted to handle, in accordance with least privilege and need-to-know principles. The accounts will be removed at the end of the contract or when no longer required.
- 4.3.2 Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.
- 4.3.3 Third party access must be set with a defined expiry date provided at the time of the original request and any extension of this must be supported by a new request.
- 4.3.4 Managed Service Provider (MSP) Access
 - Named user accounts only; no generic accounts permitted (except for emergency “Breakglass” accounts, which are strictly controlled)
 - RBAC for all systems and services
 - Two-factor authentication (2FA) for all remote and privileged access
 - Regular review and auditing of permissions
 - Password management via approved password management systems (e.g., PassPortal), with strict complexity requirements
 - Segregation of duties and least privilege principles
 - Customer sign-off required for access management reports
 - All access requests and changes must be logged and approved
 - MSP engineers must complete specialised training for privileged access
- 4.3.5 GDAP (Granular Delegated Admin Privileges):
 - Used for Microsoft cloud services (MS365, Intune, Entra, Power BI, etc.)
 - All access via individual accounts, with MFA enforced
 - RBAC and Privileged Identity Management (PIM) for just-in-time elevation
 - GDAP relationships require approval by the customer’s Global Admin

- Emergency “Breakglass” accounts are highly restricted and used only when necessary

4.3.6 Azure Lighthouse:

- Used for Azure subscriptions, with group-based permissions and customer approval
- ARM templates used for non-reseller scenarios, mirroring RBAC and group structures

4.4 Password Policy

There must be authentication prior to access to any system. To provide this, users must use passwords to authenticate themselves to the related systems. There 2 main types of account in RCPI’s environment:

- Website Online Account: Users responsible for an account (or any form of access that supports or requires a password) on any system /service offered by the RCPI.
- Network Accounts: Users (Staff, contractors, and vendors) with access to RCPI’s network

4.4.1 The following rules apply for general password use:

- 4.4.1.1 The frequency of password change is generally based on the privilege or access level of the account. Accounts with greater privilege or access should have their passwords changed more frequently.
- 4.4.1.2 The minimum required interval for password changes is once every year with exception of system password which is scheduled to be updated and changed every 3 months.
- 4.4.1.3 If your password has been compromised or you suspect it's been compromised, contact helpdesk to alert us of this issue and change your password immediately. Change your password by visiting the password page on our website or by contacting the helpdesk at helpdesk@rcpi.ie
- 4.4.1.4 Passwords must not be inserted into unencrypted email messages or any other form of electronic or physical communication or means.
- 4.4.1.5 All user-level and system-level passwords must conform to the guidelines described in RCPI Password Guidelines. Please see addendum for additional information regarding these guidelines

4.4.2 Network Account Passwords (Staff, Vendors and Contractors)

- 4.4.2.1 Enforce Password History 24 passwords remembered: this means that while passwords can be similar, you cannot use any of your previous 24 passwords.
- 4.4.2.2 Max Password Age 180 days: When the 180 days are up you will be prompted to re-set your password.
- 4.4.2.3 Min Password Length 10 characters: Passwords can be more than 10 characters in length, but they cannot be less than 10.
- 4.4.2.4 Password must meet the complexity requirements.
- 4.4.2.5 Account Lockout Threshold 3: If you enter your password incorrectly 3 times your account will lock.

4.4.2.6 Account Lockout Duration 30 minutes: After 30 minutes a locked account will automatically unlock. Remember, entering an incorrect password 8 times will lock an account. Exception is system password which will remain locked until confirmed correct person is attempting to access the account.

4.4.3 Password Protection Standards

Password protection is a vital part of any security plan, so please observe the following standards:

- 4.4.3.1 Do not use the same password for RCPI accounts as for other non-RCPI accounts, such as personal email, banking, and other accounts.
- 4.4.3.2 Do not share RCPI passwords with anyone.
- 4.4.3.3 All passwords must be treated as sensitive RCPI information.
- 4.4.3.4 When IT works on your computer, please arrange to be available to type in your password as needed. If that is not possible, change your password immediately before and after the work is done.

4.4.4 Password best practices must be followed as shown below:

- 4.4.4.1 Do not reveal a password over the phone to ANYONE.
- 4.4.4.2 Do not reveal a password in an email message to ANYONE.
- 4.4.4.3 Do not reveal a password to a supervisor.
- 4.4.4.4 Do not write passwords down and save them.
- 4.4.4.5 Do not talk about a password in front of others.
- 4.4.4.6 Do not hint at the format of a password (e.g., "my family name")
- 4.4.4.7 Do not reveal a password on questionnaires or security forms to ANYONE.
- 4.4.4.8 Do not share a password with family members.
- 4.4.4.9 Do not reveal a password to co-workers (e.g., when going on vacation or leave of any kind)
- 4.4.4.10 Do not use the "Remember Password" feature of applications, on browsers this will be ignored by default due to current security policy in place.
- 4.4.4.11 Do not store passwords in a file on ANY computer system (including a smartphone or similar devices) without encryption.

4.4.5 Password management practices

- 4.4.5.1 Password managers help users maintain many passwords and account information. They store login information for various accounts and automatically enter them into forms. This helps prevent cyber-attacks and reduces the need to remember many passwords.
- 4.4.5.2 RCPI Staff are provided a NordPass Enterprise Account, that they are requested to use for the management of work-related passwords.

4.4.6 Password creation best practices:

- 4.4.6.1 The password complexity means the password must consist of 3 of the following:
 - Length - Make your passwords long with 10 or more characters.

- Complexity - Include letters, symbols, and numbers and a variety of upper- and lower-case characters.
- Obscurity – Good passwords are randomised combinations of characters, don't use dictionary words with personal connections to you or the service the password is for

4.4.6.2 Strong passwords are:

- At least twelve characters, (longer is better)
- A mix of upper- and lower-case letters (a-z, A-Z), numbers (0-9), and symbols (~!%^)+]>}`\$*)
- Are not a word in any language, slang, dialect, jargon, etc.
- Something hard to guess, but easy to remember.

4.4.6.3 Bad passwords are:

- Predictable patterns or significant repeating of the same character
- Personal information (name, birth date, family/friend/pet's names, address, SSN, etc.)
- A password you use for other systems.

4.4.6.4 The chart below illustrates how users may construct a strong password:

What to do	Example
First start with a memorable sentence or phrase	I love to travel
Then remove the spaces between the words in the sentence	Illovetotravel
Next capitalise the first letter of each word	ILoveToTravel
Turn words into short-hand or intentionally misspell a word	ILcTTrvl
Finally, add length, complexity and obscurity with special characters and numbers	!Lc77rv1

4.4.7 Changing your password

4.4.7.1 Network Account Password Reset (Staff, Vendors and Contractors)

- From your Office PC, press Ctrl + Alt + Delete on the keyboard.
- Select Change Password
- Follow the on-screen instructions.
- Alternatively, you can wait until the current password expires and you are prompted to reset the password.

4.4.7.2 Website Online Password Reset

- Users can reset your password at any time from here: www.rcpi.ie/myaccount
- If you have trouble changing your password or have forgotten your password, you should contact the helpdesk@rcpi.ie or 01 863 9650

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	Comments
1.0	27/05/2020	Omer Altundal (Evros)	Joe Brady (Evros)	
2.0	15/01/2021	Alan O'Mahony	Michael Hughes & SMT	
3.0	01/01/2023	Shane O Neill	Michael Hughes & SMT	
3.0	13/04/2023	Shane O Neill	Michael Hughes & SMT	
4.0	27/11/2023	Eduards Jutanovs & Michael Hughes		Updates to reflect RSM May'23 Data Protection Audit comments and as part of the annual review process
4.1	06/02/2024	Eduards Jutanovs	Michael Hughes	Updated "Access rights will be reviewed" from annually to regularly.
5.0	06/08/2025	Eduards Jutanovs	Michael Hughes	Updated doc, corrected spelling and few policies and points to ensure compliance with current and recommended security policies posture.

7. Reference Documents

- [Leaving Staff \(sharepoint.com\)](#)
- <https://rcpi.sharepoint.com/infohub/Wiki/SitePages/itservices-cybersecurity-lastpass.aspx>