ROYAL COLLEGE OF PHYSICIANS OF IRELAND

ISMS-05-Access Control Policy

Policy Title	**Access Policy**
Department:	**IT Support**
Owner:	**Michael Hughes**
Approving body	**SMT**
Effective date:	
Next review date:	
Policy number:	
Related Policy and/or Procedures	• Acceptable Use Policy • Information Security Policy • Staff disciplinary procedures

ROYAL COLLEGE OF PHYSICIANS OF IRELAND

Contents

1. Purpose **3**

2. Scope **3**

3. Responsibilities **3**

4. Access Control Policy - Guiding Principles **3**

4.1 Access Control Management Guidlines 3

4.2 Password Policy 4

5. Breach of Policy **6**

6. Review and Approval **6**

7. Reference Documents **7**

ROYAL COLLEGE OF PHYSICIANS OF IRELAND

1. Purpose

Information security has many different components those need to be take care of. Access control is the one of main parts of this elements which must be handled carefully. Access control process covers 2 basic elements which are Authentication and Authorization. Authentication is the verification of the identification of the entity (user or service) where Authorization is giving specific level of access to the authenticated user based on his/her role

The purpose of this policy is to define the process of authentication and authorization of users and the systems that they access to.

2. Scope

All operating users and information resources in RCPI IT infrastructure are in the scope of this policy.

3. Responsibilities

- IT Services is responsible for applying the rules defined in this policy to every internal or external actors and systems where possible.
- All users are required to adhere to the rules defined in this policy while accessing to any system that belong to RCPI

4. Access Control Policy - Guiding Principles

4.1 Access Control Management Guidlines

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 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

4.1.9 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

4.2 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, vendors) with access to RCPI's network

4.2.1 The following rules apply for general password use:

4.2.1.1 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

4.2.1.2 The minimum required interval for password changes is once every year

4.2.1.3 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

4.2.1.4 Passwords must not be inserted into unencrypted email messages or any other form of electronic communication

4.2.1.5 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

4.2.2 Network Account Passwords (Staff, Vendors and Contractors)

4.2.2.1 Enforce Password History 24 passwords remembered: this means that while passwords can be similar, you cannot use any of your previous 24 passwords

4.2.2.2 Max Password Age 180 days: When the 180 days are up you will be prompted to re-set your password

4.2.2.3 Min Password Length 10 characters: Passwords can be more than 10 characters in length, but they cannot be less than 10

4.2.2.4 Password must meet the complexity requirements

4.2.2.5 Account Lockout Threshold 8: If you enter your password incorrectly 8 times your account will lock.

4.2.2.6 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.

4.2.3 Password Protection Standards

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

4.2.3.1 Do not use the same password for RCPI accounts as for other non-RCPI accounts, such as personal email, banking, and other accounts.

4.2.3.2 Do not share RCPI passwords with anyone

4.2.3.3 All passwords must be treated as sensitive RCPI information

4.2.3.4 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

4.2.4 Password best practices must be followed as shown below:

4.2.4.1 Do not reveal a password over the phone to ANYONE

4.2.4.2 Do not reveal a password in an email message to ANYONE

4.2.4.3 Do not reveal a password to a supervisor

4.2.4.4 Do not write passwords down and save them

4.2.4.5 Do not talk about a password in front of others

4.2.4.6 Do not hint at the format of a password (e.g., "my family name")

4.2.4.7 Do not reveal a password on questionnaires or security forms to ANYONE

4.2.4.8 Do not share a password with family members

4.2.4.9 Do not reveal a password to co-workers (e.g., when going on vacation or leave of any kind)

4.2.4.10 Do not use the "Remember Password" feature of applications.

4.2.4.11 Do not store passwords in a file on ANY computer system (including a smartphone or similar devices) without encryption.

4.2.5 Password creation best practices:

4.2.5.1 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

4.2.5.2 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

4.2.5.3 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

4.2.5.4 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	Ilovetotravel
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

4.2.6 Changing your password

4.2.6.1 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.

4.2.6.2 Website Online Password Reset

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

5. Breach of Policy

Any breach of this policy may result in disciplinary action in accordance with RCPI procedures [for Staff] or reduction or withdrawal of services [for non-staff users].

6. Review and Approval

The College reserves the right to amend this Policy at any time and in any way the College sees fit at the absolute discretion of the College or the President of the College.

Any such revisions will be noted in the revision history of the policy, which are available to you on the website and by continuing to use the College's IT Resources following any updated you will be deemed to have accepted the revised terms of this Policy.

Version	Date	Author	Approver
1.0	27.05.2020	Omer Altundal (Evros)	Joe Brady (Evros)
2.0	15.01.2021	Alan O'Mahony	Michael Hughes

7. Reference Documents

NA