

OCR FM PASSWORD POLICY

AIM

The aim of this policy is to set out and communicate rules concerning the use and security of passwords that must be observed whilst using OCR FM computer and email systems. While OCR FM provides and encourages presenters to use an OCR FM email address, it is the responsibility of that presenter to keep information safe.

The requirements defined within this policy will assist to mitigate the risk of unauthorised access to Information and Communications Technology systems and applications, thereby safeguarding the confidentiality, integrity and availability of information essential to the needs of OCR FM members and presenters.

DEFINITIONS

The following definitions apply:

Term	Definition
Administrator account	A userID with elevated access control privileges to an ICT application or system; not used for routine business purposes such as accessing OCR FM email and login to the OCR FM network.
OCR FM	3OCR community radio station
ICT systems and applications	Includes but not limited to all OCR FM networks, systems and software including DEECD Local Area Networks (LANs), Wide Area Networks (WANs), Wireless Local Area Networks (WLANs), Intranet, Extranet, DEECD email systems, computer systems, software and servers.
ICT	Information Communications & Technology
Initial password	A temporary password assigned to the userID on creation; user to change password at first login.
Reset/Temporary password	A Password reset is an operation that allows an administrator or helpdesk operator to set another user's passwords to a desired new value.
Presenter account	A userID and password allocated to a Presenter/User primarily for the purpose of email communications with external parties including music organisations, band managers and news outlets.
Service account	A userID and password allocated to an ICT system or application; not to a person. For example, an application is allocated a service account to access a backend database.
User	A person that this policy applies to.
User account	A userID and password allocated to a person.

POLICY

This policy governs the creation, management and protection of passwords used to access OCR FM ICT systems and applications and is derived from the OCR FM ICT Security Policy.

OCR FM Executive, Presenters and other authorised users must take reasonable steps to protect the secrecy of their passwords, including but not limited to the following:



- Users must not share their userID and password with a third party.
- Users must not write down their password and leave in a place where it could be easily found.
- Users must take care when typing their pass words if they are being observed.
- Users must change their password if they suspect that someone else knows it.

OCR FM ICT systems and applications that authenticate users via a userID and password must comply with the following:

- The password controls prescribed by this policy.
- System administrators must change default vendor and manufacturer passwords during product installation.
- Users must change their initial password at first logon.
- The clear text password is not visible on the screen when entered by the user, except on mobile devices that briefly display each password character as it is entered.
- Users must enter new passwords twice for confirmation of accuracy.
- System generated initial passwords and reset (temporary) passwords must be pseudo-random and comply with password construction rules prescribed in this policy.
- All incoming Executive members of OCR FM must change their password when commencing their role.
- Users are accountable for the actions performed when their userID and password are used to access OCR FM ICT systems and applications.
- System administrators who are responsible for setting password controls must ensure that the controls comply with this policy.
- Personnel involved in application development or acquisition must ensure that the required password controls exist and can be configured to comply with this policy.

A 7 day changeover period will be provided for outgoing Executive accounts to be 'cleaned' in preparation for the incoming recipient.

PASSWORD CREATION

It is recommended, but not essential, that OCR FM ICT user's use and create a complex password structure and contain at least one character from at least three of the four sets below.

Lowercase characters (a - z); Upper case characters (A- Z); Numeric characters (0 - 9); Special characters and punctuation (e.g. !@#\$\$%^&).
--

The 'System Admin' and 'Station Admin' accounts must have a password change every 12 months. The 'DJ' account will remain without a password to enable all Presenters access to on air content and creation.

OCR FM will keep a register of names of members and presenters and the accounts that they have passwords for.



Community Radio
Shop 6 Bowling Arcade, Colac
Post: P.O. Box 31, Colac 3250
Ph: 0352 321 991
Email: admin@ocrfm.org.au
Web: www.ocrfm.org.au
ABN 35 575 865 292

This policy was adopted as policy in principle by the OCR FM Committee of Management

Signed *Tyson Graham*

Date 15th September 2021

This Policy is due for review within 24 months of the date shown above.