University Health Network (UHN)

RESOURCE MATCHING AND REFERRAL (RM&R)

Policy Governing RM&R End User Account Passwords

Document Version: 1.0

Date: Last modified on April 28th, 2014

Table of Contents

1. RM&R End User Account Passwords Policy

Resource Matching and Referral (RM&R) uses passwords as a critical tool to restrict and secure access to the application, and makes all reasonable efforts to ensure that passwords are not compromised by methods such as brute-force dictionary attacks, social engineering, and keystroke capture.

Users accessing RM&R with a user account that is not their own is strictly prohibited. Users are responsible for all actions taken under their uniquely assigned user account, and will be held liable for any misuse of their account privileges. Passwords must meet the requirements specified in this policy in order to be approved for use.

All User Accounts and/or **passwords** used to access RM&R must:

- be assigned to a single individual;
- not be shared with others;
- not be re-used for another individual;
- be reported to the RM&R Service Desk if misuse is suspected;
- never be written down or stored on-line;
- be transmitted securely;
- be prevented from displaying onscreen when entered or typed by the user; and
- be prevented from displaying onscreen in the credential database.

Any account will be disabled or have its password reset upon suspicion of misuse.

When RM&R accounts are used in an environment not managed by the organization (e.g., Internet Café, hotel, conference, etc.), it is strongly recommended that users change their password as soon they have access to a trusted workstation.

If users suspect that their account or password has been compromised, they must contact the Local or RM&R Service Desks to disable their account temporarily.

Sharing accounts is prohibited due to the difficulty of auditing activity and the security risks associated with shared credentials; unless specifically exempted in writing due to exceptional circumstances.

1.1 Minimum Password Requirements

The following is a list of minimum password requirements for Participating Organizations that interface with RM&R in a non-integrated environment.

If a Participating Organization is unable to comply with these minimum password requirements, please submit an exception request to RMR_Program@uhn.ca. See “RM&R Account Management Exception Form” document. Each exception request will be sent to the RM&R Privacy and Security Team for processing.

For security reasons, the RM&R Service Desk can only provide new account passwords to the End Users directly, including for the purposes of resetting the password. Users can contact the RM&R Service Desk at 1-866-556-5005 or via email at referrals@uhn.ca to retrieve passwords, if required.

	Requirements
Length	Minimum 8 characters
Complexity	Contains at least: • One special character (e.g., 0-9, !@#$) • One uppercase letter (e.g., A-Z), and • One lowercase letter (e.g., a-z)
Expiration	After 120 days of inactivity
Account Lockout	After 3 unsuccessful consecutive attempts
Lockout Duration	Until manually unlocked by Local or RM&R Service Desks • See "Policy Governing Site-Specific Helpdesk Role Management" for further information on Local Service Desk – OR – Until automatically unlocked after 5 minutes
History	Last 13 passwords cannot be reused
Reset Duration	Must be changed every 60 days

2. Scope

All employees, contractors, consultants, temporary, volunteers, and other workers at Participating Organizations, including all personnel affiliated with third parties that use RM&R on behalf of the Participating Organization, must adhere to this policy. This policy applies to all passwords within RM&R.

3. Breach of Policy

In some instances, exceptions to the policy must be made due to extenuating circumstances. Non-compliance must be reported to the RM&R Service Desk.

Failure to adhere to this policy may result in the suspension or loss of access privileges, or other disciplinary measures, up to and including, termination of accounts.

APPENDIX A – GLOSSARY OF TERMS

End User – the person who actually uses a particular product (e.g., RM&R, ORBIT)

Integrated Environment – referring to a Participating Organization that accesses RM&R/ORBIT via that organization's Hospital Information System, by way of a Single Sign-On protocol

Local Service Desk – a support help desk operated by the Participating Organization

Non-integrated Environment – referring to a Participating Organization that accesses RM&R/ORBIT independent of any of that organization's Hospital Information Systems (also see *integrated environment*)

Participating Organization – a site that is participating in the usage of RM&R and/or ORBIT

RM&R – the Resource Matching and Referral application

RM&R Service Desk – a support help desk operated by the RM&R Program, potentially delegated to a third-party service provider

Online Referral Business Intelligence Tool – An application to provide users with the capability to view near real-time referral and wait time information for their organization and partner organizations in an intuitive, dynamic and user friendly manner

ORBIT – Online Referral Business Intelligence Tool

User Account – accounts assigned to individuals (end users or administrators) who have been authorized to access RM&R.