De-Provisioning/Deactivation of SOM Clinical Solutions Access
IS&T Procedures
Last Reviewed: 06/28/2013

1. Scope

This document outlines the requirements for the de-provisioning/deactivation of Clinical Application accounts for SOM employees upon separation from, or transfer within the University.

2. References

A. Cancelation of Access to University Assets 00-01-10-160:00
B. Access to University Administered Software Systems 00-01-95-10:00
C. Rights and Responsibilities for the Use of University-Accessed electronic Information Systems 00-01-95-10:05
D. Separation from Employment 30-01-20-75:00

3. Definitions and Acronyms

3.1. Definitions

A. Employee – An individual paid through Rowan payroll
B. Electronic Resources – Material (data and/or programs) encoded for manipulation by a computerized device. This material may require the use of a peripheral directly connected to a computerized device (e.g., CD-ROM drive) or a connection to a computer network (e.g., the Internet). Examples include, but are not limited to, computers, books, tools, keys, cell phones, and pagers.
C. De-Provisioning/Deactivation – The removal of any computing, networking, telephony, physical or access to information resources owned by, procured through, operated, maintained or contracted by the University.
D. Asset provider – A department or group within a University organization responsible for managing and maintaining any electronic and/or physical resources for the Rowan community.
3.2. Acronyms
   A. SOM – School of Osteopathic Medicine
   B. FPP – Faculty Practice Plan
   C. IS&T – Information Systems and Technology

4. Introduction

IS&T offices for the School of Osteopathic Medicine (SOM) are required to de-provision/deactivate Clinical Solution application access for any users that are either leaving the University or transferring within the University.

5. Applicability

This procedure applies to all SOM IS&T management and staff members responsible for de-provisioning/deactivating Clinical Solution accounts.

6. Standard

The University requires the timely de-provisioning/cancellation of access to University-provided assets, both electronic and physical, upon employee separation from or transfer within the University. The Cancellation of Access to University Assets Policy, 00-01-10-160:00, defines required de-provisioning timelines.

In instances where access is provided to Clinical Solution applications, the management of the application will be responsible for deactivating accounts that are inactive or no longer needed due to separation of employment from Rowan or transfer within Rowan to a non-Faculty Practice Plan department or position not requiring access to Clinical Solution applications.

7. Procedures

A. Steps for Separation from the University:

   Upon notification of employee separation (department notification, notification from SOM-IT End User Services management or Rowan Separation Report), SOM Clinical Solution application access will be deactivated. If the access being terminated is for a user in C-EMR, the security officer will put in an expiration date and email the Administrator and Chair of the department to determine where all unsigned documents should sent. Once all documents have been routed the user can be marked obsolete.
Deactivation of account is noted in termination log, stored in a departmental folder on University network drive. Clinical Solution application user accounts which have been deactivated are noted within the Security feature, along with the user login initials of the analyst responsible for the account deactivation.

B. Steps for Transfer within the University

Upon notification of employee transfer within the University, Clinical Solution application access shall be deactivated as follows:

i. The Rowan Separation Report is reviewed by the application systems administrator.
ii. Verification is made of transfers requiring a change to a user’s account.
iii. Accounts for users that have been transferred to a position requiring that access privileges be maintained are verified via employee’s new department. Employees are required to complete a new Security Access form indicating the new department for which they will need access.
iv. Accounts for users that have been transferred to a non-FPP department or to a position that does not require access, will be deactivated.

C. Periodic Compliance review

Bi-annual review of current accounts will be performed in June and December, to ensure compliance. Reports of users and access level will be generated by Department and will require review with notes for changes or deactivation by the Department Administrator. The report must have a physical signature of approval.

8. Standard Ownership and Responsibilities

It is the responsibility of the management of the IS&T department to communicate and enforce this procedure as it relates to the Clinical Solution applications.

By Direction of the SOM Clinical Solutions Assistant Director:

[Signature]

Lori Smith