COLLEGE OF MEDICINE TUCSON
Information Technology
Services

1501 N. Campbell Ave.
P.O. Box 245017
Tucson, AZ 85724

Ofc: 520-626-8931
medicineit.arizona.edu

Information Technology Services

Subject: eRegulatory External User Access Management and Account Provisioning Procedures

Date Created: 8/24/2023

Responsible Team: Business Intelligence and Data Services

1. Introduction. This Access Management and Account Provisioning document outlines the procedures for managing user access to the eRegulatory (eReg) system for external users. Effective access management and account provisioning and deprovisioning are crucial to maintaining data security, confidentiality, integrity, and availability.

2. Purpose. The purpose of these procedures is to establish a standardized approach to granting, modifying, and revoking user access privileges to ensure proper authentication, authorization, and accountability while minimizing security risks. The eReg system does not currently offer two factor authentication (2FA) for locally provisioned accounts. While the College of Medicine and University of Arizona Health Sciences recognize the benefit of implementing 2FA for access to view university restricted data, the strict implementation and execution of these procedures as an administrative compensating control is sufficient to reduce the risk to an acceptable level.

3. Scope. The scope of these procedures is for limited time use external monitor/auditor access to the eReg system to conduct regulatory compliance audits only.

4. Related Policies, Standards, and Procedures.

a. University of Arizona Identity and Access Management Policy

5. Definitions.

a. Locally provisioned account – A locally provisioned account refers to a user account that is created and managed directly on a specific computer, device, or system rather than being managed through a centralized authentication system like a network domain controller or cloud-based identity provider.

6. Service/Procedure/Guideline.

a. Account Provisioning:
   1) External monitor/auditor access to the eReg system shall be granted based on the principle of least privilege, ensuring that users have the minimum necessary access to perform their job responsibilities.
   2) User access shall be requested by the University of Arizona Health Sciences Research Administration office via TicketCat. The request must include the following:
      i. A Non-Disclosure and Acceptable Use Agreement signed by the monitor/auditor and Research Administration
      ii. A copy of their Advarra eReg training certificate

iii. A copy of their Information Security Awareness training certificate (must have been completed within the past 365 days)

iv. A completed account provisioning request form

3) Once all documentation has been received, the College of Medicine (COM) Information Technology Services (ITS) shall provision the requested account.

i. The username shall be firstname.lastname. A number may be added at the end if required.

ii. The username and default password shall be emailed separately to the user.

iii. The user shall be prompted to change their password at first login.

iv. Password requirements shall be set to 16 characters with at least one upper case, one lower case, one number, and one special character.

b. Access Review and Recertification:

1) Regular access reviews shall be conducted to ensure that user access privileges remain appropriate and aligned with their roles and responsibilities and dates of access as identified in the account provisioning request form.

2) Access reviews shall be performed at least monthly.

3) Managers and supervisors within COM ITS and Research Administration shall be responsible for reviewing and recertifying access privileges.

c. User Roles and Responsibilities:

1) View only access rights shall be assigned for all monitors/auditors and only for the data required to perform their job.

2) Requests for any privileges other than view only shall be reviewed by the Director, Business Intelligence and Data Services for necessity.

3) Users are responsible for safeguarding their access credentials (e.g. usernames and passwords) and shall not share them with any other individual or entity.

d. Account deprovisioning:

1) User access shall be promptly revoked upon job completion, end of service date, termination, or if abuse is discovered.

2) Deprovisioned user accounts shall be disabled and retained for a period of one year, after which they may be purged from the system.

e. Enforcement:

1) Violation of these procedures or the NDA and Acceptable Use Agreement may result in immediate revocation of access or legal action.

7. Service/Procedure/Guideline Review. These procedures shall be reviewed and updated at least annually.

Table of Annual Review

Author:	Trevino, Lorenso - (lorensotrevino)
Created on:	8/24/2023
Last reviewed/updated by:	Trevino, Lorenso - (lorensotrevino)
Last reviewed/updated:	8/24/2023