Clinical Research Support Office (“CRSO”)
STANDARD OPERATING PROCEDURE

SOP NUMBER CTM-SOP-2002	**TITLE** CTMS Login Access
EFFECTIVE DATE 8/15/2019	**WRITTEN BY** Jennifer Simpson
REVISED BY (DATE) Eric Bucholz and Stephanie Cason (08/23/2023)	**REVIEW HISTORY** 08/23/2023

APPROVAL

Jessica Heskel Digitally signed by Jessica Heskel Date: 2023.08.25 08:37:28 -04'00'	25-Aug-2023
SIGNATURE	**DATE**

1. POLICY STATEMENT

The Clinical Research Support Office (CRSO) has entered into an agreement with the University of Kentucky (UK) Identity Access Management (IAM) department and the UK Information Technology Services (UK ITS) to allow the CRSO Research Systems Management and Education (RSME) team to provide and manage the login access to the employees of UK and select outside-institution individuals participating in the management of clinical research studies at UK.

2. PURPOSE

To establish a standardized process for providing login access, define steps required, documents required, document retention period, and mandated role-based training to acquire login access to the CTMS.

3. SCOPE

This policy is applicable to all end-users requesting CTMS login access.

4. RESPONSIBILITY

The CRSO Research Systems Educators and CTMS Administrator will be responsible for providing and maintaining login access to the application. Refer to CTM-WI-2026 CTMS Contact Records, Login Access, and Deactivation for guidance.

The CRSO Clinical Trials Administrative Support and Billing Integrity team and select other end-users will have permission to create contact records within the CTMS for the purpose of protocol shell creation and general regulatory management. This functionality does not allow login access. It does provide access to receive notifications, will populate staff drop-down lists, and allows staff to be sent to Epic based on assigned role.

5. DEFINTIONS

Role-Based Training – Specific areas of training within the CTMS based on the major job responsibilities of the end-user. This is determined based on permissions/roles required within the CTMS that have been created by the CRSO RSME team. Role-based training may include several stackable roles within the CTMS and may not be identical in content between end-users. All role-based training surrounds the use and functionality of the CTMS. Additional training needed to perform the job functions of a research staff member is the responsibility of their department and is not included in the general CTMS role-based training. The CTMS trainer may serve as an aid in supportive training for specific job responsibilities, but is not responsible for protocol/calendar/forms – specific training, only in the functionality of these CTMS components.

6. PROCEDURE

Required Documents and Retention

1. The following documents must be filled out by all UK employees requesting login access.
   - 1.1. Request Form
     - 1.1.1. Online UK CTMS Access Request Form must be completed by/for the requester. The CRSO RSME team (CTMS.Support@uky.edu) can provide the link to this form upon request.
     - 1.1.2. For non-PI/Faculty requesters, the UK CTMS Access Request Form will be sent to the supervisor for approval.
   - 1.2. Documents
     - 1.2.1. Proof of recent Health Insurance Portability and Accountability Act (HIPAA) training. This training may be completed through the UK Web Based Training in myUK Learning or through the Collaborative Institutional Training Initiative (CITI) training provided through UK. Proof of completed HIPPA training must be current and not expired.
       - Web-based training (WBT) through the UK myUK Learning Portal must be performed annually.
       - CITI training has an expiration of 3 years from the time of completion.
       - Other external HIPAA training certificates will be reviewed on a case-by-case basis.
     - 1.2.2. A signed UK ITS Confidentiality and Non-Disclosure Agreement document. This electronic document will be available for signature prior-

to the role-based training (for digital signature or certification).

1.2.3. A hyperlink or electronic copy of the UK ITS Acceptable Use Policy will be provided to each new CTMS login requestor.

1.2.4. A signed CTMS Training Log. This form will be provided by the CTMS Trainer following completion of role-based training.

1.2.5. Proof of current HIPAA training, signed UK ITS Confidentiality/Non-Disclosure Agreement, and signed CTMS Training Log must be received by the CTMS Trainer prior to granting login access. These documents will be uploaded into the CTMS.

2. The following documents must be filled out by all non-UK individuals identified as needing access to the CTMS.

2.1. Request Form

2.1.1. All external non-UK individuals requesting access must fill out the External/Non-UK CTMS Access Request Form. This is a CRSO created form that has been verified and accepted for use by the UK IAM department.

2.1.2. This login access request has an embedded HIPAA and non-disclosure statement that must be signed. This statement has been verified by the UK Chief Privacy Officer.

2.1.3. The login access request must have the provided supervisor/sponsor signoff page filled out and signed.

2.1.4. Signed access request form and required documents should be submitted by a UK supervisor/sponsor through the UK CTMS Access Request Form online on behalf of the non-UK user. The CRSO RSME team (CTMS.Support@uky.edu) can provide the link to this form upon request.

2.2. Documents

2.2.1. Proof of recent HIPAA training.

2.2.2. An electronic copy of the UK ITS Acceptable Use Policy will be provided to each new external, non-UK CTMS requester.

2.2.3. A signed CTMS Training Log. This form will be provided by the CTMS Trainer following completion of role-based training.

2.2.4. Proof of current HIPAA training, External/Non-UK CTMS Access Form including the signed Confidentiality and Non-Disclosure statement, and signed CTMS Training Log must be received by the CTMS Trainer prior to granting login access. These documents will be uploaded into the CTMS.

Role-based Training Requirement

3. All new requests for CTMS access will be processed and access will be granted after role-based training is performed with a CTMS Trainer.

3.1. A description of the end-user's scope and/or job responsibilities should be outlined within the login access request form. Based on the defined scope, the CTMS Trainer will determine what role-based training(s) must be completed to obtain access.

3.1.1. CTMS Trainer may assign pre-requisite eLearning modules that must be completed before providing instructor-led role-based training.

3.1.2. Depending upon the scope of the end-user, multiple role-based training modules may be required.

3.2. Role-based training may be provided remotely in a 1:1 setting or virtual classroom using a video conferencing tool of choice.

3.3. Role-based recommendations must be performed minimally to obtain access. However, CTMS users are encouraged to request any of the training modules that interest them and are not restricted to only those that pertain to their role.

3.4. Pre-existing users within the CTMS who have a change in their job functions or role will be required to perform the role-based training that pertains to their new role prior to having their permissions changed within the database.

3.5. Following completion of role-based training, the CTMS Trainer will send the requester a CTMS Training Log that describes the scope of the training provided. The requester must sign and return this log to the CTMS Trainer before receiving login access.

Account Activation

4. After the CTMS access form is completed, all required documents are signed/received, role-based training has been performed, and a signed CTMS Training Log has been returned, the end-user will receive login access to the CTMS.

4.1. All end-user accounts will be set-up to use SAML authentication.

4.2. The process of creating a new user account within the CTMS requires an email verification step by the application.

4.3. UK employees and non-UK/external employees will use their assigned Linkblue User ID and password to log into the CTMS.

4.4. End-users who are transferring positions and changing research departments will have to submit a new login request form outlining change in scope.

4.5. If a user transfers to a different Organizational Unit, the CTMS Trainer for that unit will review previous role assignment(s) against the new login access request to determine the need for any additional training.

4.5.1. If there is no change of scope and the end-user was active within the CTMS during the previous 180 days, no refresher training is necessary unless requested.

4.5.2. If there is a change of scope or if the end-user has not been active within the CTMS during the previous 180 days, refresher or full role-based training will be provided prior to receiving login access.

Account Deactivation

5. The CTMS Trainers will manually perform monthly quality control and deactivate any active user accounts without a login for ≥ 180 days.
   5.1. The user account should remain as an active contact record within the CTMS.
6. End-users who are leaving a current research position for a new research position between departments will have their account deactivated by the CTMS Trainer for the current Organizational Unit.
   6.1. Stop dates will be added to all protocols with active staff assignments.
7. The CTMS Trainers will manually perform monthly quality control to identify user accounts with expired HIPAA training documentation in the CTMS.
   7.1. If an end-user does not provide proof of current HIPAA training within 2 weeks of initial communication, the user account should be deactivated.
   7.2. The user account should remain as an active contact record within the CTMS.
   7.3. When proof of current HIPAA training is provided, the account will be re-activated without need for additional training unless the user's CTMS inactivity period exceeds 180 days.

Deprovisioning of Linkblue Accounts

8. Every month a deprovisioning report will be generated to compare end-user accounts within the CTMS and University of Kentucky/UKHC Linkblue accounts.
   8.1. Individuals with a deactivated Linkblue will be evaluated to determine whether it warrants a full deactivation within the CTMS.
      8.1.1. When a deprovisioned Linkblue is verified, the end-user's account and contact record will be deactivated, and stop dates will be added to all protocols with active staff assignments.
   8.2. Deprovisioned Linkblue accounts may be temporary and require reactivation with UK ITS.
   8.3. External end-users apply for temporary Linkblue IDs that deprovision regularly based on their inability to receive password update emails.
      8.3.1. These end-users will need to contact UK ITS to have their Linkblue reactivated.
      8.3.2. The CTMS Trainers can then reactivate the CTMS accounts based on the procedures outlined in this SOP.

Reactivation of Account

9. Any end-users who have a deactivated user account can contact the CRSO RSME team (CTMS.Support@uky.edu) to have their account reactivated.
   9.1. If deactivation occurred due to lack of login activity for ≥ 180 days and a request for reactivation is received:
      9.1.1. Less than 12 months after deactivation, refresher training will be required.
      9.1.2. Greater than 12 months after deactivation, full role-based training will be required.

9.2. If the end-user's account and contact record has previously been deprovisioned, or if the end-user has changed department and/or job responsibilities, the end-user will be required to follow the Account Activation process outlined above.

9.3. The extent of required re-training will be at the discretion of the CTMS Trainer.

7. ATTACHMENTS

1. UK CTMS Access Request
2. CTMS Training Log
3. External/Non-UK CTMS Access Request Form

8. REFERENCES

1. University of Kentucky/ UK HealthCare Enterprise Policies: https://ukhealthcare.mc.uky.edu/policies/enterprise/default.aspx
2. University of Kentucky / UK HealthCare Enterprise Policy and Procedure. Policy #A13-100 Acceptable Use Policy. Retrieved from: https://ukhealthcare.mc.uky.edu/policies/enterprise/_layouts/15/WopiFrame.aspx?sourcedoc=/policies/enterprise/Enterprise/A13-100%20Acceptable%20Use%20Policy.docx&action=default
3. University of Kentucky/UK HealthCare User Confidentiality and Non-Disclosure Agreement. Retrieved from: https://spwww.ukhc.org/itsecurity/Forms/User%20Confidentiality%20and%20Non-Disclosure%20Agreement.pdf?Web=1
4. CTM-WI-2026 CTMS Contact Records, Login Access, and Deactivation