Purpose and Scope: New Mexico State University's training management system – Training Central (aka SABA) - is deployed to maintain employee training records and provide a centralized repository for employee training. Training Central is administered by the Center for Learning & Professional Development. The Center for Learning & Professional Development's director is the data custodian for all Training Central data, including training reporting data in Cognos Analytics.

Training Central is a role-based and domain-based application. Users of the system are assigned roles based on their individual job responsibilities. Users may be assigned multiple roles. Domains define the level of access a user is granted and allows for customization of business rules and notifications for each training area. For example, a user with Catalog Admin role in the CLPD domain can only create trainings within CLPD and sub-domains and cannot edit or create offerings in other domains.

This document defines the standard roles assigned to NMSU training unit employees who maintain training data (aka training administrators). Individuals should be granted the minimum roles and privileges needed for their job responsibilities. Roles and privileges may be added and/or removed as necessary as job duties change.

System administration is shared between Information & Communication Technologies (ICT) and the Center for Learning & Professional Development (CLPD). ICT maintains the hardware and software necessary to run the system and is responsible for technical functionality including security administration (LDAP). CLPD is responsible for functional system administration and the Graphical User Interface (GUI). CLPD will appoint a primary and back-up system administrator (aka Super User) to maintain the system interface, security roles, business rules, notifications, domains, and resources.

CLPD also maintains documentation and provides training & assistance related to system administration, policies, procedures, and business rules.

Security access is granted to regular employees only. Training units requesting security access for temporary or student employees must provide justification for access and a termination date. Justification must be for genuine business need when another regular employee is not available to fill the need. All justifications must be approved by the system administrator and CLPD director.

Data Security: Training records are protected by NMSU ARP 15.50 and, in the case of student employees, FERPA laws. Additionally, NMSU must comply with NMAC Record Retention regulations. Employees with access to training records shall not access, distribute, or otherwise use such information for any purpose other than those required to perform their job duties and will not release training data without express authorization. All training record requests will be forwarded to CLPD.

- Alternate Managers & Proxies: employees requesting access to training records through the alternate manager or proxy function must provide written permission from the individual record holder or the record holder's supervisor. See additional information regarding proxies on page 5 of this document.
- Faculty: faculty members who require students to complete training as part of course requirements (i.e HIPAA training for the Dental Hygiene program) may request enrollment and training verification for their students. CLPD will verify the faculty member is responsible for the program.
- Record requests from General Counsel, Office of Institutional Equity, and HRS Employee & Labor Relations must be forwarded to the CLPD director or designee.
- Requests to have training added to an employee training record may be submitted by the employee's supervisor or their designee, the training department where training was conducted, or the employee who attended the training with appropriate confirmation of attendance. The employee's department must maintain a copy of the attendee's completion certificate or other form of confirmation of attendance in accordance with NMSU record retention policies.

All other requests for training records must be approved by the CLPD director or designee.

Security Access Procedures: All Training Central security roles are approved and administered by CLPD. A training unit needing to add or remove a member's security access must submit a Training Central Security Access Form to CLPD. Upon an employee's termination from a training unit, the training unit must submit a Training Central Security Access Form to remove Training Central security access. Members granted security access to Training Central are also added to the saba@nmsu.edu email list and Training Central SharePoint site.

Members requesting security access must complete the following requirements.

1. Approval by training unit director or training unit Domain Administrator
2. Completion of NMSU FERPA training (WBT)
3. Completion of NMSU Computer & Data Security training (WBT)
4. Completion of NMSU FSA-RMR Information Session training (WBT)
5. Completion of role-dependent training (WBT)
6. Approval by Training Central System Administrator (Super User)

Training Requirements: All persons with administrative roles are required to complete applicable training prior to access being granted. Past training will be considered if within 12 months of the security access request.

Additionally, persons being granted administrative roles will be trained by CLPD in system procedures prior to access being granted (training may be delegated to Domain Administrators). CLPD will provide assistance and procedural guidance as requested.

Domain Administrators will train training administrators in departmental procedures.

Roles & Responsibilities: The following roles may be utilized by training units.

NMSU Domain Administrators: Domain Administrators are assigned to training organizations with multiple training administrators and/or a high volume of trainings. Domain Administrators have the highest security of all roles with the exception of Super Users and the staff of the Center for Learning & Professional Development, and as such, have a higher degree of responsibility and expectations than other security roles in Training Central.

The Domain Administrators are responsible for, but not limited to, the following tasks:

- Approve the assignment of training administrators in their area and submit security access requests for additions and removals of security access in their domain
- Oversee department-level procedural training, ensure the accuracy of training administrators' inputs, and act as the liaison between training administrators and the Center for Learning & Professional Development (CLPD)

  Note: Department-level procedures may add to, but may not take away from, system procedures established by CLPD
- Provide input regarding system configuration, policies, and procedures
  - Identify potential changes to the course catalog, delivery types, audience types, facilities, and rooms; communicate those needs to CLPD for approval and implementation
  - **Note**: Final decision-making authority lies with the system administrator (Super User)
- Maintain notifications for their domain

  Note: Notification administration is not domain-based; it is crucial that administrators only change notifications for their domain. Changes made to other domains may result in the Domain Administrator role being withdrawn
- Maintain equipment inventory for their domain, as appropriate
- Identify and create domain-specific training reports using built-in Analytics or request reports in Cognos Analytics through ICT Enterprise Reporting Services
- Create end-of-course certificate templates for their domain using approved templates
- Create multi-day session templates for their domain following established procedures
- Administer API scripting (aka web services) for departmental websites connecting to Training Central

NMSU Catalog Administrator: Catalog Administrators are responsible for performing the functions associated with building and managing a catalog of offerings. This role is typically assigned to the unit's instructional designer or equivalent and includes, but is not limited to:

- Manage and schedule resources used in the delivery of training (rooms, facilities, instructors, etc.)
- Set up and maintain courses and offerings
- Print rosters for any class
- Close classes after delivery
- Set up and maintain curricula
- Set up and maintain certifications
- Run training reports through Training Central Analytics

Catalog Administrators who need access to view employee training records must also request NMSU Monitor access.

NMSU Content Administrators: Content Administrators are responsible for importing learning content in a variety of formats, including SCORM, video, and e-signature documents into the content repository. The repository consists of two components: the production repository and the knowledge base. The production repository is where online course content resides. The knowledge base contains untracked job aids and documents not used in a course. Additionally, Content Administrators maintain the training unit's evaluations, tests, and surveys in accordance with established policies and procedures.

A maximum of two (2) Content Administrators are assigned to each domain. The Domain Administrator may will this role.

NMSU Monitor: Monitors have limited view-only access to Training Central for the purpose of verifying training records and running reports. This role is granted at the NMSU domain allowing access to ALL employee training records. This role requires justification as to why the user needs this role. Monitors perform the following functions:

- Print rosters for any class
- Run training reports through Training Central Analytics
- View training records for individuals

NMSU Human Capital Admin (aka People Administrator): People Administrators perform the following functions. This role will be assigned to select members of CLPD only. Requests for this role outside of CLPD require a written justification as to why the individual needs this role. People Administrators perform the following tasks:

- Create distribution lists for use by the training unit
- Administer requests by users or management for training records in accordance with established policy
- Create new accounts for learners not loaded by Banner load

- Create and maintain prescriptive rules for assigning training to learners based on roles or employee type

Proxy Access: Although the Training Central system allows all users to assign a proxy, employees with training administrator roles in Training Central **may not delegate** these roles or any associated tasks to a proxy. For example, if you have access as a Catalog Admin and Manager's Desk and want to give proxy access to your administrative assistant to monitor your team's training, you may grant proxy access to Home and Manager's Desk only and may not grant proxy access for your Catalog Admin role.

Sanctions: Use of information or unauthorized access to Training Central or related records in violation of university policy and the Training Central Security Guidelines may result in sanctions, which include, but are not limited to, the sanctions listed below:

1. Written warning to offender and notification to department director.
2. Mandatory training refresher including, but not limited to, the training requirements outlined in this policy.
3. Temporary or permanent withdrawal of privileges.

For additional information regarding roles, refer to the SABA System Administrator Guide.