Access Control and Account Auditing for {Enter System Name}

Last Update: {Enter date procedure was approved}

**Procedure Owner:** {Enter procedure owner, typically business owner}

# Purpose

The University’s {Enter system name and link to home page of vendor} contains confidential data. {Enter system name} contains data with {short description}. To protect this data, Western must ensure accounts are issued and revoked as users are onboarded and offboarded, or their roles change. Western must also ensure every user account is unique.

This procedure shall also describe periodic auditing for users.

*Add below if relevant.*

# Directory Integration

*Customize the paragraph below.*

The {Enter system name} uses {local and/or Active Directory integrated accounts}. {Enter system name} {is integrated with Active Directory using LDAP, Kerberos, SAML2 authentication} {Enter system name} {supports/does not support multifactor authentication}.

# {Replace with System Name} System Roles

Western’s {Enter system name and link to home page of vendor} instance has {X number} of user, and {X number} of service/automation accounts. Service/automation accounts are granted the least privileged permissions necessary to do their tasks and are only changed if a notice is received from the vendor or a cybersecurity threat is detected. Users and test accounts can have {X number} of roles:

*Below is an example*

* Administrator – A full control, highly privileged role.
* Dashboard Administrator – A user role that can manage all aspects of {Replace with system name} dashboards.
* Mobile Device Administrator – A user role that can modify all settings related to {Replace with system name} mobile devices.
* Remote Cashier Admin – A user role that can perform all aspects of collecting payments.

# Managing Users

User management consists of creating, modifying, and deleting user accounts.

## Procedure to Add or Edit a User

{Enter system name} has various types of user accounts including {e.g., local, Active Directory integrated}. To create a new user, see Figure 1 below and do the following:

*Below is an example*

1. This procedure must be performed by someone with a XX Administrator role.
2. Select the **Insert/Edit User** Menu.
3. Enter the user’s *username* in the **User** box. The user’s *username* should match their Western Universal ID.
4. The user **Type** and **User Auth Method** is always **XX**.
5. Select one or more of the **Roles** checkboxes. **Roles** should be configured for the least privileged access necessary. When **Roles** are selected, the **Privileges** boxes below should auto-fill.
6. Enter a *password* in the **Password** and **Confirm Password** boxes.
7. Enter the user’s *first name* in the **Nickname** box.
8. In the **Description** field, enter a short *description* of the user type.
9. Check the **Is Active** checkbox.
10. Select the **Password Change Required at Next Login** box.
11. Deselect the **Account Locked** out box.
12. Create the account by clicking **Save**.
13. Inform the user the account is created and provide them with the initial password. They will have to change it at their first login.

Figure 1 - Adding a User



## Procedure to Modify a User

If a user needs their roles, name, or job description changed, or they forgot their password, you must make these changes from the Insert/Edit user menu. See Figure 1 above.

*Below is an example*

1. This procedure must be performed by someone with a XX role.
2. Enter the **Insert/Edit User** menu.
3. Deselect and select the appropriate **Roles** for the user.
4. Update the **Nickname** and **Description** boxes if needed.
5. For a password change, enter a new password in the **Password** and **Confirm Password** boxes, then select the **Password Change Required at Next Login** box.
6. Update the account by clicking **Save**.
7. Inform the user their account has been modified. If their password was changed, provide them with the initial password and let them know they will have to change their password at their next login.

## Procedure to Disable a User

If a user no longer needs access, but there is a need to not yet delete the account, the user must be disabled. See **Figure 2** below.

*Below is an example*

1. This procedure must be performed by someone with a XX role.
2. Enter the **Insert/Edit User** menu.
3. Enter a new password in the **Password** and **Confirm Password**.
4. Deselect the **Is Active** box.

Figure 2 – Deactivating a User



## Procedure to Delete a User

*Below is an example*

1. This procedure must be performed by someone with a XX role.
2. Enter the **User** menu and view all accounts.
3. Select the account to view and delete it. See **Figure 3** below.

Figure 3 – Deleting a User



# Auditing

To ensure that only authorized users have access to {Replace with system name} and their roles are configured with least privilege, user accounts and their privileges must be periodically audited.

## Auditing Frequency

Auditing occurs at the following times:

*Below is an example*

1. Any time a user account is created or deleted.
2. At the beginning of each academic quarter during the first departmental standing meeting.

## Auditing Procedure

*Below is an example*

1. This procedure must be performed by someone with a {Replace with system name} Administrator role.
	1. View the {Replace with system name} user list. You may also see additional information about users using the {Replace with system name} Flex query UID 2866.
2. Delete any accounts that no longer need access.
3. View the privileges on existing accounts and make sure they have least privileged roles. Remove any extra roles they do not need.

*Figure 4 - User List*



*Note that the best way to do auditing is to use an automated system. Western can use Microsoft Entra ID Governance (*[*Access Reviews*](https://learn.microsoft.com/en-us/graph/tutorial-accessreviews-m365group?toc=%2Fazure%2Factive-directory%2Fgovernance%2Ftoc.json&bc=%2Fazure%2Factive-directory%2Fgovernance%2Fbreadcrumb%2Ftoc.json&tabs=http)*)*