

# Specification for Staff User Record

Finalized Wednesday March 2, 2011

## St--1: Scope / Purpose

The staff user/permissions record will record information by which system administrators manage and control access to the system's staff side interface. Its purpose is two fold:

1. By creating individual user records, the system administrator establishes the credentials by which the system authenticates attempts to access the staff interface/web forms.
2. By linking user records to a user group and a repository, the system administrator sets **create**, **read**, **update**, and **delete** (CRUD) permissions for users for particular record types (such as resource, digital object, accession or subject records) or system configuration/administration functions.

The interface by which an administrator manages staff user records will include a method to browse, view, create, edit, and delete staff user records. The staff user record itself will consist of:

- a) login credentials;
- b) descriptive information about the user;
- c) a required user group/permission designation, as described in Section St--6;
- d) a required repository designation

## St--2: Record / template description

The staff user record will contain the following fields:

### 1. Data Elements

- Login (**REQUIRED**)
- Password (**REQUIRED**)
- Email Address
- Last Name

- First Name
- Phone Number
- Title
- Department
- Contact Information
- Note

## 2. Linked Records

- Repository (**REQUIRED** link to one or more repository records)
- User Group (**REQUIRED** link to one and only one user group for each listed repository)

The application will include controls allowing a system administrator or repository manager to:

- Browse all user records
- Add a new user record
- Edit an existing user record
- Delete one or more user records

### St--3: Displaying staff user records

The system must include a method for system administrators and repository managers to browse and search/filter all staff user records. The browsing interface will consist of a multi-column, sortable display, which includes the following columns:

- Column 1: Login/ID
- Column 2: Name
- Column 3: Usergroup
- Column 4: Repository (if applicable)

The list of staff users will be accompanied with a control to filter the user records to show only those linked to a particular repository. In addition, it will contain controls for creating, editing, and deleting staff user records.

## St--4: Creating, editing and deleting user records

When the application is first installed, the installer will create a “superuser” account. The person installing the software will provide a login, password, and optional information for this ‘default’ account. The application will assign this user to the “System Administrators” user group, with the permissions described in section St--6.

To create a staff user record, a system administrator or repository manager will select the ‘add new’ option from the browsing interface described in section St--3 above. The user must then provide all required information, assign the user to a user group and, if applicable, assign a repository for that user. The user group and repository linkages will determine the CRUD permissions that the user has for certain content records in the system (see section St6).

To edit an existing staff user record, a system administrator or repository manager will select the login account from the browse list. The interface to edit the record will load, allowing the system administrator to edit any of the record fields and to assign or remove the user to one or more repositories and, for each repository, to a defined user group.

To delete a staff user record, the system administrator or repository manager will enter the interface to edit an individual record and will then select the option to delete the current user record. The system administrator will be required to confirm the deletion. When confirmation is given, the selected user record will be removed from the list of user records in the browse list and system will return to the list of all users.

Finally, all users must have the ability to edit the descriptive information and password for their user accounts, but not to change the user group and repository association, nor to delete his/her user record. These personalization features may be provided via a ‘my preferences’ panel or a similar feature, separate from the interface that administrators use to manage staff user records.

## St--5: Business Rules—Staff user Record Creation and Validation

1. The staff user interface must not be browsable or listed as a menu option for members of the Read Only, Advanced, and Basic User Groups.
2. A staff user record’s password may only be edited by:
  - a. a member of the System Administrator user group; or

- b. a member of the Repository Manager Group, provided the user record is linked to the specified repository.
  - c. the individual associated with that specific user record, but a user may not modify his/her assigned permissions
3. A user must not be able to delete his or her account.
4. It must not be possible to delete all user accounts; at least one user account, assigned to the System Administrator User Group, must exist at all times.
5. Only members of the System Administrator Group have CRUD permissions on all user records, regardless of repository.
6. Members of the Repository Manager group may only browse, create, edit and delete users for the repository to which the Repository Manger is assigned.
7. A member of the Repository Manager group may not assign users to the System Administrator Group.
8. Password rules:
  - a. The password field must be stored in encrypted form in the database (MD5 or similar).
  - b. The password display must be masked in the display interface.
  - c. The system must “lock out” user accounts when there are several consecutive failed logins. The lock out should expire after a set period of time or when a system administrator unlocks the account, whichever comes first.
  - d. All passwords created by users must be very strong, under current industry best practice.
  - e. Users shall be provided a method to edit their own passwords. In addition, System Administrators and Repository managers shall be provided a method to reset existing passwords.
  - f. The password field must be set using a password and a password confirmation field. If the entered values do not match, the attempt to create the user record or reset the password will fail and the system administrator or user will be provided a message to fix the error.

## St--6: Business Rules—Create, Read, Update and Delete Privileges for Authenticated Users

This section of the specification describes the set of features that will be available to a user, after he or she has successfully logged in to the staff side interface. When a feature is not available to a user, the menu option to access that feature must not appear in the user interface or must be disabled/grayed out to indicate that the feature is not available.

| Function<br>User Group | System Configuration               | Repository Records                 | User Records                                    | Location Records                   | Preferred Name, Variant Name, and Name Contact Records <sup>1</sup> | Subject Records  | Accessions, Resources, Resource Components, Digital Objects and their Sub – Records <sup>2</sup> | Linking <sup>3</sup> |
|------------------------|------------------------------------|------------------------------------|---|------------------------------------|---|--|--|----------------------|
| System Administrator   | Read<br>Create<br>Update<br>Delete | Read<br>Create<br>Update<br>Delete | Read<br>Create<br>Update<br>Delete              | Read<br>Create<br>Update<br>Delete | Read<br>Create<br>Update<br>Delete                                  | Read<br>Create<br>Update<br>Delete                       | Read<br>Create<br>Update<br>Delete   | Yes                  |
| Repository Manager*    | Read                               | Read<br>Create<br>Update<br>Delete | Read<br>Create<br>Update <sup>4</sup><br>Delete | Read<br>Create<br>Update<br>Delete | Read<br>Create<br>Update<br>Delete                                  | Read<br>Create<br>Update<br>Delete                       | Read<br>Create<br>Update<br>Delete   | Yes                  |
| Project Manager*       | No Access                          | Read                               | Read  | Read                               | Read,<br>Create,<br>Update,<br>Delete                               | Read,<br>Create,<br>Update,<br>Delete                    | Read,<br>Create,<br>Update,<br>Delete  | Yes                  |
| Advanced Data Entry*   | No Access                          | No Access                          | No Access                                       | Read                               | Read,<br>Create<br>Update;<br><b>No delete or merge<sup>5</sup></b> | Read,<br>Create,<br>Update,<br><b>No delete or merge</b> | Read,<br>Create,<br>Update,<br>Delete<br><b>No merge</b>   | Yes                  |

|                   |           |           |           |      |      |      |  |     |
|-------------------|-----------|-----------|-----------|------|------|------|--|-----|
| Basic Data Entry* | No Access | No Access | No Access | Read | Read | Read | Read, Create, Update<br><b>No merge, delete, or transfer<sup>6</sup></b> | Yes |
| Read Only User    | No Access | No Access | No Access | Read | Read | Read | Read   | No  |

\* Create, update and/ or delete authority applies only for records of the associated Repository. Unless otherwise specified, user has read authority for records of other repositories

1. Any user with permissions to add name variants may add a name variant sub-record to a name record; the user need not be a staff member of the repository that created the name sub-record. Users shall be able to add name variant records as a Except for System Administrator, users can view and link name contact records **only** for the named repository under which the user logged in.
2. Sub-records include any object type which exists in a one-to-one or many-to-one relationship with a parent record (extent, date, rights, de-accession, location, external document references, and collection management records).
3. Linking refers to the ability of a user to establish a relationship between objects of one type and objects of another type, in many – to-many relationships (e.g. subjects, names, name variants, and digital objects to resources.) See each specification for a description of all such many-to-many relationships.)
4. Repository Managers may not assign users to the System administrator user group.
5. Merging refers to the ability of the user to combine several existing name, subject, or resource records into one name, subject, or resource record, for the purpose of deduplicating the database or combining similar records. See the name, subject, and resource specifications for additional information.
- 6: Transferring refers to the ability of user to move child component records from one parent resource or resource component record to another parent resource or component record.

## St--7: Required Task Sequence-Creating and Editing Staff User Records

1. Select the option to create or edit a staff user record.
2. Enter the following information: login, password
3. Select a user group from the list of all user groups
4. Select a repository from the list of all repositories (required for all users except system administrators)
5. Save the staff user record

## St--8: Optional task sequence

1. Complete any optional data elements
2. Delete the staff user record that is open for editing

## St--9: User intentions / Application response sequence

The interface for editing, adding and deleting user records will only be available users belonging to the System Administrator (SA) and Repository Manager (RM) user groups. As specified in section St5, the Repository Manager will only be able to add, edit, or delete users associated with the named repository and will not be allowed to assign users to the System Administrator User Group.

| <b>User intention (Required fields in <i>italics</i>)</b>   | <b>Application response / action</b>                |
|---|---|
| <i>SA or RM selects option to <b>add</b> a user record</i>  |   |
|   | Machine opens the template to create a user record. |
| <i>SA or RM records the following values: login, password, password confirmation, and any optional fields</i>                     |   |
| <i>SA or RM select the user group to which the record being edited will be linked, from list of all user groups</i>               |   |
| <i>SA or RM selects the repository to which the user record being edited will be linked, from list of all repository records.</i> |   |

|   |  |
|---|--|
| <i>SA or RM selects option to save the user record.</i> |  |
|   | If a) login field is missing or duplicates an existing record, b) the passwords do not match or do not conform to the business rules for the value of the password field, or c) user record is not linked to a user group and/or repository record, the system will indicate the record cannot be saved and will alert the user to fix the error |
|   | Otherwise, the machine will save the record, display a message indicating the record was saved, delay for two seconds and return to the list of all users.   |

| <b>User intention (Required fields in <i>italics</i>)</b>  | <b>Application response / action</b>  |
|--|---|
| <i>Within the browsing interface, SA or RM selects an existing user record for editing or deletion</i>                 |   |
|  | Machine loads the selected user record, showing all values, except password, which is masked or left blank, and provides controls for saving or deleting the record.  |
| <i>SA or RM edits any of the existing credentials, descriptive information, and user group/repository associations</i> |   |
| <i>SA or RM selects option to save the user record.</i>  |   |
|  | If a) login field is missing or duplicates an existing record, b) the passwords do not match or do not conform to the business rules for the value of the password field, or c) user record is not linked to a user group and/or repository record, the system will indicate the record cannot be saved and |

|  |  |
|--|--|
|  | will alert the user to fix the error   |
|  | Otherwise, the machine will save the record, display a message indicating the record was saved, delay for two seconds and return to the list of all users.   |
| <i>User selects the option to delete the selected user records</i> |  |
|  | Machine displays a message asking “Are you sure you want to delete the user record for [Login]”  |
| User Answers “Yes”   |  |
|  | Machine deletes the user record(s), displays a message stating that the records have been deleted, pauses two seconds, then clears the message. Machine reverts list of all users, with deleted record are removed from browse list. |
| User answers “No”  |  |
|  | Machine cancels the action to delete the record, displays a message stating that the operation has been cancelled, pauses two seconds, and clears the message. Machine reverts to list of all user records.                          |

**St--10: Data elements table**

| Element                | Definition   | Type                              | Default Values   | Required |
|------------------------|--|-----------------------------------|--|----------|
| Login                  | Indicates the login id that a staff user will use to enter the staff side interface  | String                            |  | Yes      |
| Password               | Indicates the password the user will use when logging in to the staff side interface   | String encrypted                  | None, but must conform to business rules listed in section St5         | Yes      |
| Email                  | A text field containing the user's email address.  | String                            |  | No       |
| Last Name              | A Text field containing the last name that should be displayed by the machine when a user is logged in   | String                            |  | No       |
| First Name             | A Text field containing the first name that should be displayed by the machine when a user is logged in  | String                            |  | No       |
| Phone Number           | A text field listing a phone number  | String                            | None, but must allow non-US phone numbers                              | No       |
| Title                  | A text field for providing the user's job or position title  | String                            |  | No       |
| Department             | A text field for listing the department or subunit to which a user belongs   | String                            |  | No       |
| Contact Information    | A text field for listing other contact information, such as an address   | String                            |  | No       |
| Linked User Permission | A link to the User Permission Group to which the user belongs, drawn from the list of all user groups; determines level of access to read, create, edit, and | Non-config lookup; see user group | <ul style="list-style-type: none"> <li>System Administrator</li> </ul> | Yes      |

|                     |  |               |  |     |
|---------------------|--|---------------|--|-----|
| Group               | delete functions specified for that user group.                          | specification | <ul style="list-style-type: none"> <li>• Repository Manager</li> <li>• Project Manager</li> <li>• Advanced Data Entry</li> <li>• Basic Data Entry</li> <li>• Read Only User</li> </ul> |     |
| Linked Repositories | Link to one repository records, drawn from the list of all repositories. |               |  | Yes |

### Su--9: Imports

None.

### Su--10: Exports

None.

### Ex--11: Reports

None.