

Frequently Asked Questions
User Manager and Security Passwords for the Department Web Applications
Missouri Department of Elementary and Secondary Education
January, 2012

WHY THE CHANGES?

Q. Why is the Department making these changes now? Have there been attacks on the Department web site?

A. To date there have been no attacks on the Department website. We attribute this to our high security standards and implementation of procedures that limit the amount of damage that could be done in case of such an event. These changes to the Web Application security are made as a commitment to Missouri school children to keep their data safe.

Q. Do these changes to Web Applications also affect MOSIS IDs?

A. Yes and no. Yes, MOSIS users will be expected to change their password every 90 days. Their changes must follow the same guidelines as the Web Applications users. MOSIS users will also be included in the monthly email report. Although the Department would eventually like to merge the Web Applications and MOSIS user registration processes, that will likely not happen for a while. Until then, there are still two distinct registration processes, Web Applications and MOSIS.

MONTHLY EMAIL

Q. You spoke of a monthly email to User Managers, what will that email contain?

A. Many districts are very conscientious about updating their Web Applications user roles. However, some have not made updates in quite some time, while other districts may have missed some updates. User Managers will soon be receiving regular monthly emails that include a list of all individuals currently on the district's list of users. This will serve to remind the district to make the updates, as well as help to clean up the rolls and improve security for each and every district. We recommend that the User Manager(s) take time to review the list, and to make changes, if necessary.

Q. Will the monthly email list include teachers who have created their profile and account for certification purposes only?

A. At present, teachers who have a profile for certification purposes only will not be included in the monthly email list. Many of the teachers with certification only access are not necessarily connected to one or any specific district, and that information is not a part of the registration process. We will look into trying to include teachers who use Web Applications for certification only.

90-DAY PASSWORD CHANGE

Q. When will the 90-day password change rule be implemented?

A. Every password used to access any part of the Web Applications system will need to be changed every 90 days. This means teachers using the system only for certification, as well as those responsible for submitting data or working on plans, will be prompted to change their password every 90 days. Rather than have one day that all passwords must be changed (and stress the system), we will implement a rolling schedule for this change.

INFREQUENT USERS

- Q.** What is the reason for waiting 13 month before eliminating the user? If a person changes districts, retires, resigns, why would there need to be a 13 month period. In the past the Department has made multiple User IDs , one for each district.
- A.** An individual should only have one User ID. That will allow them access to their teacher certification records, as well as any programs that a district gives them access to. An individual should be able to keep that User ID throughout their career.

An individual might have a myriad of accesses throughout their career. As an individual progresses in their career, they will have a multitude of jobs and responsibilities. Some of those may require using the Web Applications system. When their employer determines the individual should have access, they can grant that access. When that access is no longer needed, the employer will remove the access, not the User ID. Maintaining the User ID will allow the individual to be granted access again, possibly in another district or another capacity.

Districts may and **SHOULD** continue to delete former employees access through their own User Manager, and are advised to make those changes **IMMEDIATELY** after the employee's status has changed.

Also, some district individuals only access web applications once a calendar year (ex. Census of Technology Screens 30 and 31, Library Media Services Screen 7) By waiting 13 months, we have given those users an appropriate length of time to log in to the system and do their work.

If an individual does not log in after 13 months, they may have left the role, district, or profession all together, or may be employed in or assigned to another role that does not require access. When they receive the email, if they wish to maintain their User ID for personal certification access, or for possible re-entry into another position, they can log back in to the system as the email details, and maintain their User ID. The email sent to the individual will contain full information on what steps to take to maintain access. If the email does not reach the individual, or the individual chooses not to log back in, the User ID will be deleted from the system. If the individual re-enters the field, or it is determined they need access after the 13-month deletion, the individual may be issued another User ID by going through the New User process.

- Q.** A thought regarding deactivating accounts for inactivity.... since this is also a guideline for certification logons as well, you may want to reconsider the deactivation or rethink it. Sometimes a teacher may not need to log in their profile for a long period of time due to their certification expiration; however, they may want to add certification at some point. If they have not been logged in for the period of time that the Department has set for deactivation, they may find themselves creating a new profile.
- A.** This is a good point...we are discussing this use, and will make sure we implement changes that do not limit the teacher's access, and best serve the teachers' needs. For now, after 13 months of inactivity, an email will be sent to the teacher, and they will be given 5 days to log in to the website to keep their certificate access active. Individuals are responsible for updating the system should the individual change their email address.

QUESTIONS ABOUT USER MANAGER

- Q.** What can the User Manager do? What are the responsibilities?
- A.** The User Manager is able to grant and delete staff access at one of the three levels, View, Data Entry, or Authorized Representative.

The User Manager function allows the District User Manager (UM) to:

Manage User IDs by these four actions

- Add User to District
- Modify District Users Account
- Remove User from District
- View all District Users

Access these two Reports

- User
- System

Make changes to a District Users Account by granting access to one of these three levels

- Level One - View Only – view data
- Level Two - Data Entry – view/enter/edit data
- Level Three - Authorized Representative – view/enter/edit data/submit data

Some individuals are designated User Manager for your district, and also has the responsibility of developing or submitting data through the web applications. A User Manager still has to be given access to the various programs and levels in order to use Web Applications to input data or submit. If a User Manager needs access to program(s) or level(s), another User Manager should give them that access using the district's standard method of granting such things.

- Q.** How do we designate a User Manager for our district? What if our User Manager moves from our district to another - how do we ensure that individual no longer has access to our records?
- A.** Only the Department staff can activate the User Manager access. At present, we consider every superintendent to be the user manager for their district. However, an application must be submitted to the Department before the superintendent's designation becomes active. Every district has the opportunity to designate additional User Managers along with the superintendent. The district must submit a User Manger request form, found at https://k12apps.the Department.mo.gov/webapps/securityforms/MO-2356_USER_MANAGER_FORM.pdf to designate an individual as a User Manager.

Districts should use the same form to remove an individual from the User Manager role. This should be filed as soon as the individual has left the district. Note that removing an individual from the User Manager role does not delete them from the system completely; the individual will still have access to their personal teacher certification files. If the individual moves on to a new district, and the new district wants that individual to have access to the new district's files, the new district should be able to use the person's name and identifying information to pull up their User ID and attach that User ID to the desired new district files.

- Q.** Who should be a User Manager?
- A.** Each district should have at least one User Manager, the superintendent. Other staff members to consider as user managers may be the secretary of the board, the assistant superintendent, principal, technology coordinator, or other administrative staffer.

USER LIST AND ACRONYM LIST

- Q.** Is there someplace where districts can view all users for their districts?
- A.** User Managers can view this list by clicking on the *User Manager* link found at the bottom of the list of *User Applications* that comes up when they log on to the Web Applications site. Clicking on the *Report Menu* link will give them access to two reports, User Report and System Report.
- Q.** Will there be some document to explain the various accesses available and define acronyms on the request list? Is there a definitions page for the user permissions so we can know exactly what someone will have access to in each area?
- A.** This is one of the improvements we have planned for web applications.
- Q.** Is the User Manager able to see when the last time was that a user from their district signed in?
- A.** At present, that is not possible. However, that is a good suggestion; we will look into this capacity and investigate how we might incorporate it.
- Q.** Can a person have access to schools in multiple districts? If so, how do we go about that?
- A.** Access to multiple districts is not a problem. An individual should have a User ID, if not, one of the districts should add the individual to the system. To grant multiple district access, the User Manager at each district should pull up the individual using the *User Search* screen in *Add User to District* feature under *User Access*. The

User Manager will either type in the User ID in the *Edit User Access* box or type in the first and last name of the individual in the *Search for User ID* box. Either one of these searches will bring up the User ID in the new district(s) and allow the User Manager to add in access to their district.

USER IDS

Q. Please explain the three ways a User ID can be created.

- User IDs can be created by the district User Manager with the intent of assigning the individual access to specific applications in order to provide a service to the district.

When a User Manager creates a User ID for an individual, the individual is notified by email of their User ID. The password for the new account is set to the supplied mother's maiden name. The new user must log in within 24 hours in order to change their user password, or else the User ID is voided.

- If the User Manager is not able to make these arrangements (either because of time or other problems), then the application may be sent to the Department's Office of Data System Management, and the Department staff will create and assign the roles as authorized by the paper application.

When a User Manager creates a User ID for an individual, the individual is notified by email of their User ID. The password for the new account is set to the supplied mother's maiden name. The new user must log in within 24 hours in order to change their user password, or else the User ID is voided.

- An individual may create their own User ID to gain access to their own teacher certification records in order to update or verify certain information. An individual who creates their own User ID will not be able to access any district data until a specific district gives that user access to specific programs. An individual who sets themselves up as a new user cannot give themselves any access to district files.

When an individual creates their own User ID, the individual is NOT notified by email of their User ID; the individual will set their own User ID. The password for the new account is set to the supplied mother's maiden name. The new user must log in within 24 hours in order to change their user password, or else the User ID is voided.

Q. Are we able to change the User ID, if so how do we change it.

A. No, the User ID is developed when the user is created, and cannot be changed.

GRANTING ACCESS

Q. Since my administrators are the ones to submit certain plans and data, they should then be listed as the authorized representative instead of using the superintendent password to do so. Correct? Does giving Level 3 access need to be done in paper work or can I do that under the User Manager area?

A. Administrators and others using the Web Applications **should not** share passwords. The User Manager can grant any level of access appropriate for that user.

Q. In the past, our users that needed access to the Department's Web Applications site had to fill out a sheet of information and be approved by the superintendent before getting access. Do our users still have to fill out that information or is the User Manager responsible for deciding who can have access?

A. The User Manager function allows districts to manage staff access to the Department Web Applications at the district level. Although the Department cannot tell districts how to handle this decision-making process, we recommend each district establish a protocol for approval and inform staff of the procedure to request or grant access.