Name and Password Conventions

This document explains the name and password conventions that will be used in the Idaho Consolidated Services (ICS) System, and what State of Idaho employees should do before and after migration.

These conventions are necessary to provide the flexibility and capacity to uniquely identify and yet securely accommodate many thousands of users. Employees will be able to log in at any facility that is connected to the state network. Information will be accessible across organizational and geographic boundaries, permitting access when employees are travelling, working at home, or on cross-agency collaboration efforts.

E-mail Addresses

E-mail addresses must be unique for all State employees. The ITRMC standard of *firstname.lastname@anyagency.idaho.gov* has been adopted and will be implemented as agencies are migrated to the Idaho Consolidated System. "*Anyagency*" will be a distinct designator chosen by each agency. If two or more employees in the same agency have the same first and last names, any of the following can be used to create unique names:

- *first name.middle initial.last name@anyagency.idaho.gov*
- *first initial.middle name.last name@anyagency.idaho.gov*
- *first name.middle name.last name@anyagency.idaho.gov*
- *first initial.sequential number.last name@anyagency.idaho.gov*

Most agencies currently use this convention, and all existing e-mail addresses that use "Idaho.Gov" after the "@" may continue unchanged. For those that do not, the CMS migration team will setup new e-mail addresses before the agency is migrated. E-mail sent after migration will contain the new addresses. Incoming e-mail directed to another domain (state.id.us) will be forwarded to the users' inboxes for 60 days after migration, and the recipients will be notified to ask the senders to update their addresses.

As you receive e-mails from someone whose address has changed on the ICS, you may want to update their addresses in your Contacts list (Outlook 2007) or Address Book (Outlook 2003).

User Names

Employees must have a user ID to access the State network and may have an optional second one for existing applications or applications requiring a log-on with a different format. This document describes only the attributes for the network log-on user name.

All user IDs must be unique within the State, contain not more than 20 characters and be constructed in one of the following formats:

1. *<first initial><last name>*
2. *<first initial><middle initial><last name>*
3. *<first name><last name>*
4. *<first name><middle initial><last name>*
5. *<first initial><middle name><last name>*
6. *<first name><middle name><last name>*
7. *<first initial><sequential number><last name>*

No change is required if an agency currently uses one of the above formats and the names are unique within the State. If a name is a duplicate, a unique name should be constructed using the sequence of formats above. If an agency does not currently use one of the above formats, new names should be assigned starting at the top of the list.

Passwords

A password is the first line of defense in protecting an individual's computer and through it, access to all the State's network resources. Since hackers or insiders will always look for the weakest security link, any weak password is a benefit to them and a significant detriment to securing the entire network.

If your existing password does not meet the following requirements, you will need to establish a new one prior to migration:

1. Must not have been used recently (in your last 12 passwords).
2. Must be at least 8 characters in length (longer is strongly encouraged).
3. Cannot contain your USERID.
4. Three out of the following 4 are required:
    a. Must have upper case letters (A-Z).
    b. Must have lower case letters (a-z).
    c. Must have at least one number (0-9).
    d. Must have at least one special character (! @ # $ % ^ & * ( ) [ ] { }, etc.).

Passwords will have to be changed at least every 90 days and you can change your password at any time by simultaneously depressing the "Alt", "Ctrl" and "Delete" key combination, clicking on "Change Password" and filling in the dialog box.

Try to make your passwords creative and unique, yet simple to remember so you do not have to write them down. Avoid names or personal information such as birthdays and anniversaries.

A recommended approach is to use the first letters of words in a phrase or favorite song. Choose something relevant to you with spaces, punctuation marks and replace an occasional letter with a number or special character. Examples of phrases are: “I L0ve my wife!”, “I am a g0lf3r?” or “My d0g is not sp0t!”. Or from the song “I’d like to teach the world to sing”, a password could be “iL2TtWtS_!”, which would be very difficult to crack.

Lock-out Policies

Incorrect attempts at logging in may indicate an attempt to break into a network using an employee’s user account. In order to prevent this, the account will be locked after five consecutive incorrect attempts to log in. Accounts can be unlocked by administrators, or users may wait fifteen minutes for the account to be open again.

All desktop computers shall be configured to have a password-enabled screen saver set to no greater than 20 minutes; a shorter time delay is encouraged. This security-lockout feature shall automatically initiate after the desktop computer remains idle from user interaction. The user must then reenter their password to gain access to the computer. All users are encouraged to screen-lock their computers (Windows-L) when they leave their desks for more than a couple minutes.

Having a computer system remember security information, such as a USERID or password is an inherent security risk. Therefore, whenever a user logs off his computer, the USERID will not be “remembered” by the computer, requiring users to re-enter both their USERID and password each time they log in. This does not mean the USERID must be re-entered to unlock the computer after it has been screen-locked. Screen-locked computers will only require the password be re-entered.