Responsible: Office of Information Technology

PURPOSE

This administrative procedure shall establish a standard for the creation, administration, use and removal of accounts that facilitate access to information and technology resources at Washoe County School District.

PROCEDURE

1. An account, at minimum, consists of a user ID and a password and may also include the classes and other types of information needed by the individual to perform their work. Accounts that access electronic computing and information resources require prudent oversight. The following security standards are a part of the District's account management environment.

2. Account Administration Standards

    a. Issuing Accounts

        i. The owners of District data, ("Data Stewards"), shall make decisions regarding access to their data. Account setup and modification require the approval of the requestor's supervisor.

        ii. The school or department responsible for an information or technology resource is responsible for requesting through Information Technology (IT) the activation of accounts as well as the application of appropriate security classes under the principle of "least required access" to perform their business function.

        iii. The school or department responsible for an information or technology resource is also responsible for requesting through Information Technology (IT) the prompt deactivation of accounts when necessary (i.e., accounts for terminated individuals shall be removed/disabled/revoked from any computing system at the end of the individual's employment or when continued access is no longer required; and, the accounts of transferred individuals may require removal/disabling to ensure changes in access privileges are appropriate to the change in job function or location.)

        iv. The identity of users shall be authenticated before providing them with account and password details. If an automated process is used, then the account holder shall be asked to provide several information items that in totality could only be known by the account holder. In addition, it is highly recommended that stricter levels of

authentication (such as face-to-face) be used for those accounts with privileged access.

v. Passwords for new accounts should NOT be emailed to remote users.

b. Managing Accounts

i. All accounts shall be reviewed at least annually by the Data Stewards to ensure that access and account privileges are required with job function, need-to-know, and employment status. IT may also conduct periodic reviews for any system connected to the District network.

ii. All guest accounts (for those who are not official members of the District community) with access to District computing resources shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

c. Disabling/Revoking/Deleting Accounts

i. All accounts may be disabled, revoked or deleted if account privileges are no longer required with an individual's function at the district or their need-to-know due to changes in their status.

ii. All accounts may be disabled, revoked or deleted if it is determined the account has been compromised or misused and may only be reinstated at the direction of the Chief Information Officer.

iii. Under normal circumstances, accounts will persist under the following schedule:

1. Student Accounts - 2 semesters after the student is no longer associated with District.

2. Employee (Faculty and Staff) Accounts - 180 days after termination, regardless of reason.

3. Consultants and other outside individuals - 180 days after termination, regardless of reason.

4. Retiree Accounts - 180 days after retirement.

5. All Other Accounts - 180 days after termination, regardless of reason.

iv. Access to account data/email can be requested during the 180 day

window by a department head. This request can be initiated through the IT Service Desk, and will be approved through the legal hold process.

3. Individual Account Standards

    a. Account Responsibilities – Users are responsible for all activity performed with their District ID. District IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their District IDs. Similarly, users are forbidden from performing any activity with District IDs belonging to other users. Any suspected unauthorized access of a user account should be reported immediately to the Chief Information Officer or designee.

    b. Passwords – Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the password. If users need to share computer resident data, they should use electronic mail, public directories on local area network servers, and other mechanisms, so long as doing so does not violate any policies, regulations or procedures of the District, or any state or federal laws or regulations, to include those governing personally identifiable information (PII) such as the Family Educational Right to Privacy Act (FERPA) or the Health Insurance Portability and Accountability Act (HIPPA). All users are responsible for both the protection of their user account password and the data stored in their user account.

4. Departmental Accounts

    a. For access to sensitive information managed by a school or department, account management should comply with the standards outlined above. In addition, naming conventions must not cause contention with centrally managed email addresses or usernames. Should the potential for contention arise, the applicable system(s) should not be connected to the District network until a mutually satisfactory arrangement is reached.

5. Shared Accounts

    a. Use of shared accounts is not allowed. However, in some situations, a provision to support the functionality of a process, system, device (such as servers, switchers or routers) or application may be made (e.g., management of file shares). Such exceptions will require documentation which justifies the need for a shared account; a copy of the documentation will be shared with IT.

    b. Each shared account must have a designated owner who is responsible for

the management of access to that account. The owner is also responsible for the above mentioned documentation, which should include a list of individuals who have access to the shared account. The documentation must be available upon request for an audit or a security assessment.

6. Administration Of Password Changes

    a. Procedures for password resets

        i. The identity of users must be authenticated before providing them with ID and password details. In addition, it is required that stricter levels of authentication (such as face-to-face) be used for those accounts with privileged access.

        ii. Whenever possible, pre-expired passwords should be used when resetting a password or activating a new account, and should comply with the above standards.

        iii. If automated password resets are available they should be utilized, provided that a recognized and approved method is used such as multiple, random challenge and response questions.

    b. Procedures for maintenance of "shared secrets"

        i. Those responsible for access to systems/applications/servers, etc. protected by high-level administrative-passwords (or the equivalent) must have proper auditable procedures in place to maintain custody of those "shared secrets" in the event of an emergency and/or should the administrative-password holder become unavailable. These documented procedures, which must be appropriately secured, should delineate how these passwords are logically or physically accessed as well as who in the "chain of command" becomes responsible for access to and/or reset of the password.

7. Application And System Standards

    a. Applications developed by the District or purchased from a vendor should contain the following security precautions:

        i. Where technically or administratively feasible, shared ID authentication should not be permitted.

        ii. Passwords must not be stored in clear text or in any easily reversible form.

        iii. Role-based access controls should be used whenever feasible, in order to support changes in staff or assigned duties.

iv. Where technically or administratively feasible, systems should allow for lock- outs after a set number of failed attempts (ten is the recommended number). Access should then be locked for a minimum of ten minutes, unless a local system administrator intercedes. Lock-outs should be logged unless the log information includes password information.

8. Compliance

    a. All users of District Information Technology accounts are required to comply with this policy. The District reserves the right to deny, limit, restrict or extend privileges and access to its Information Technology accounts.

DEFINITIONS

1. Account – Any combination of a User ID (sometimes referred to as a username) and a password that grants an individual user access to a computer, an application, the network or any other information or technology resource.

2. Data Steward – An individual responsible for the accuracy and integrity of a set of data.

IMPLEMENTATION GUIDELINES & ASSOCIATED DOCUMENTS

1. This Administrative Procedure reflects the goals of the District's Strategic Plan.

2. This Administrative Procedure complies with Nevada Revised Statutes (NRS) and Nevada Administrative Code (NAC).

3. This Administrative Procedure complies with federal laws and regulations, to include:

    a. Family Educational Right to Privacy Act (FERPA)

    b. Health Insurance Portability and Accountability Act (HIPPA)

REVIEW AND REPORTING

1. This procedure and any accompanying documents will be reviewed bi-annually, in even numbered years.

REVISION HISTORY

Date	Revision	Modification
9/23/2015	1.0	Adopted

Appendix A - Creating a new mailbox enabled user accounts

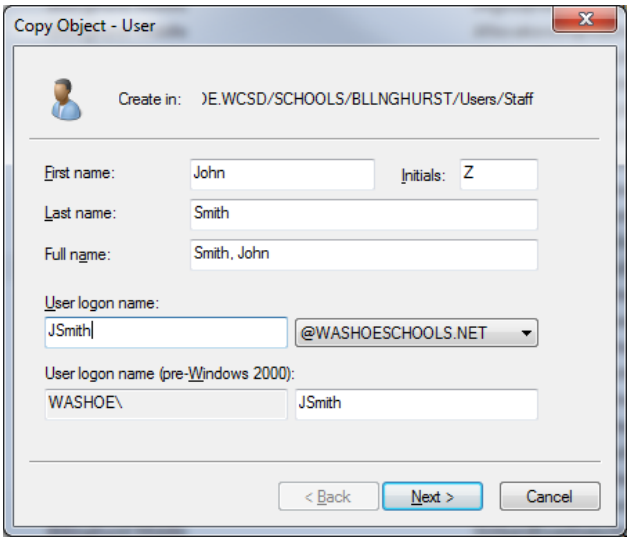
1. User Account
    a. Open Active Directory Users and Computers and change to **CORP-DC02** domain controller.

    b. Go to the OU that corresponds to the users site / department.

    c. Right click an existing account and choose copy. Use the IT Generic account if it is a school user. (staff-schoolname)

    d. Enter the new persons First name, Initial if applicable, Lastname and Username (User logon name) (John A Smith)

        i. Username is firstinitiallastname unless there is a duplicate. (JSmith)



        ii. If duplicate use firstinitialmiddleinitiallastname (JASmith)

        iii. If no middle initial use firstinitialsecondinitiallastname (JoSmith)

        iv. If the users has a hyphenated last name, use only the first of the last names for the User logon name. (John Smith-Johnson would be Jsmith)

    e. Make sure the User Logon name is **@WASHOESCHOOLS.NET**

    f. Click Next and enter the generic password.

    g. Check the box '**User must change password at next logon'**

    h. Click finish

    i. Find the user account you just made and open it by double clicking.

    j. Enter the Telephone number 775-XXX-XXXX, Fax number 775-XXX-XXXX, Description, Office and Title if applicable and check for correct group

membership (**only the –STAFF and "Domain User" Groups. Do not add them as members of any other groups.**)

2. Email Enable
    a. Open Exchange Management Console
    b. Expand Recipient Configuration
    c. Right click on Mailbox and choose New Mailbox
    d. Choose User Mailbox and click Next
    e. Choose Existing Users and click Add
    f. Click on Scope and choose Modify Recipient Picker Scope
    g. Click View all recipients in specified organizational unit and browse to the OU you created the user account in.
    h. Select the user you created above and choose ok and Next
    i. If they are an ADMIN user use database EX-DATABASE002
    j. If they are a SCHOOL user use databases 003 or 004.
    k. Check the box for Retention Policy and choose '2 Month Deleted Items'
    l. Click Next and New.
3. Notification
    a. Send email notification to the requestor listed in ticket and tell them the username and password of the user account you created. CC Michelle Hibbitt so she can update BPlus with the email address.