

# 9400-P170 – User Access Management

## I. PURPOSE

The purpose of this policy is to document how access privileges to State information and information resources shall be assigned and managed.

## II. SCOPE

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to as “agencies”).

## III. POLICY

- A. Control of user access. Agencies shall control access to information and information resources for which they are the Data Steward. The Data Administrator will grant user access based on requirements issued by the IT Resource Owner or the Data Steward.
- B. Access control permissions for State systems must be set to enforce the principle of least privilege. Users will be provided access to only those systems and information assets required to perform their current duties. Access to information and information resources shall by default be denied unless specifically allowed.
- C. Each agency shall ensure that the process they use to grant, manage, and terminate access to State information and information resources adheres to the principles of this policy.
- D. UserIDs.
  - 1. A unique UserID will be created and assigned to each individual who has an account with permissions to access State information or information resources. The person to whom the UserID is issued will be individually accountable for how it is used.
  - 2. Individual UserIDs shall not be shared.
  - 3. UserIDs, with the exception of system/application-required IDs, must not give any indication of the user’s job function (like using “admin” in the User ID), especially where related to accounts with significant system privileges or access to confidential information.
  - 4. UserIDs for default system accounts that are not needed (i.e., accounts created automatically during system setup) shall be deleted, renamed or disabled if possible to prevent their unauthorized use. For those accounts that are needed, the default configurations including passwords shall be changed wherever possible (see also Section F-4 of this policy).

## 9400-P170 – User Access Management

5. As much as technically possible, standard naming convention of UserIDs shall be utilized across platforms.
- E. Group Accounts. Group Accounts, also called shared accounts, may be created only with a validated need for multiple persons to access a resource that cannot support individual user accounts. The manager of the group will be defined as the owner of, and assigned accountability for, the Group Account.
- F. Passwords.
1. Passwords shall be constructed in accordance with standards and used to validate the authenticity of the person presenting the UserID.
  2. Users may use the same password on internal systems, network devices, or applications, but should not use their internal password for external systems, such as for accounts on an external web site, in case these web sites do not protect passwords in an acceptable manner.
  3. Administrators or other super users who have two accounts on the same system shall use a password for their higher-privileged accounts that is different from the password for their regular accounts.
  4. Default passwords for system-generated accounts (accounts created automatically during system setup) shall be changed to prevent unauthorized use of the accounts.
- G. Disabling and deleting accounts.
1. Inactive accounts shall be disabled, renamed, reassigned or deleted according to governing standards.
  2. User accounts for networks and IT resources shall be disabled, renamed, reassigned or deleted according to governing standards upon the termination of employment.
  3. User Accounts assigned to consultants and contractors for network and IT resource access shall be disabled and deleted at the end of their contract. All consultant and contractor User accounts must be renewed annually or they will be automatically disabled.
  4. UserIDs shall be disabled (locked out) after a prescribed number of unsuccessful access attempts have been made as determined by standards. UserIDs so disabled shall remain disabled for a pre-set period as determined by standards. If the resource is being accessed from a dial-up connection or an external network, the connection should be immediately disconnected.

## 9400-P170 – User Access Management

### H. Account maintenance.

1. Information access authority (permissions) shall be reviewed periodically including a review at the time of transfer, promotion, or termination of employment.
2. System administrators shall follow an agency-approved process to verify the identity of users who request password resets prior to resetting the password. Systems that process sensitive information may be configured to require an administrator to unlock the account.
3. Access control requirements and access permissions for identified groups of users should be clearly documented in agency-level policies, procedures, or guidelines. Access control requirements shall consider both physical and logical access as applicable.
4. As a control against misuse, disclosure of the specific contents of the access controls and access permissions shall be strictly limited to personnel who have an authorized need-to-know. Members of large user groups with similar permissions may be informed of the general level of their access permissions.
5. Unauthenticated public accounts (i.e., guest accounts) are not allowed except where they are explicitly needed to satisfy a valid business need (i.e., public kiosk, public web site, etc.).

**CIO Approved Date: 1/5/2011**