

**Office of the Chief Information Officer
Enterprise Policy**

Policy Number: CIO-072

Effective Date: 06/01/2002

Revision Date: 05/29/2007

Subject: UserID and Password Policy

Policy: This policy supports the Enterprise Architecture for end-user security and represents a set of standards to be followed by all employees for UserID and password usage. Often UserIDs and passwords are the first and only line of defense protecting Commonwealth resources. Effective UserIDs and passwords will improve the likelihood that the identification of the user is correct and that a user's access is controlled effectively. Both are important deterrents to intrusion.

All users must have their identity verified with a UserID and password (or by other means which provide equal or greater security) prior to being permitted to use hardware/software connected to the Kentucky Information Highway (KIH).

Responsibility for Compliance: Each agency is responsible for assuring that employees within their organizational authority have been made aware of the provisions of this policy, that compliance by the employee is expected, and that intentional, inappropriate use may result in disciplinary action pursuant to KRS 18A up to and including dismissal.

It is also each Executive Cabinet's responsibility to enforce and manage this policy. Failure to comply may result in additional shared service charges to the agency for COT's efforts to remedy intrusion activities resulting from inappropriate UserID/password usage.

Policy/Procedure Maintenance: This Enterprise Policy has been approved by the Enterprise Architecture and Standards Committee and constitutes an element of the Security Domain in the Enterprise Architecture. The Commonwealth Office of Technology, Office of Infrastructure Services has the responsibility for the maintenance of this policy. This policy is to be adhered to by all agencies and employees within the Executive Branch of state government. However, agencies may choose to add to this policy, in order to enforce more restrictive standards as appropriate.

Therefore, employees are to refer to their agency's internal policy, which may have additional information or clarification of this enterprise policy.

Procedure:

UserID Usage:

Individual Ownership

UserIDs must be individually owned in order to maintain accountability. Each UserID must be used by only a single individual who is responsible for every action initiated by that account. There must not be any re-use of the UserID. Where supported, the system must display the last use of the individual's account so that unauthorized use may be detected.

Logging of Administrator Activity

All UserID creation, deletion, and change activity performed by system administrators and others with privileged UserIDs must be securely logged and reviewed.

Concurrent Connections

For those systems that enforce a number of concurrent connections for an individual UserID, the number of concurrent connections must be set to one. This prevents multiple people from sharing a UserID.

Outside UserIDs

UserIDs established for a non-employee/non-contractor must have a specified expiration date unless approved by the agency security office or approving agency authority. If an expiration date is not provided, a default of 30 days must be used.

The agency shall maintain documentation of any exceptions granted.

Password Usage:

Passwords must be:

- Kept confidential;
- Changed at least every 31 days unless otherwise approved (non-expiring passwords must be approved on an exception basis);
- Changed whenever there is a chance that the password or the system could be compromised;
- Encrypted when held in storage or when transmitted across the network when the path is connected to an external network.

Passwords must not be:

- Reused;
- Shared with other users;
- Kept on paper unless it is securely stored;
- Included in a macro or function key to automate the log-in;
- Stored in any file, program, command list, procedure, macro, or script where it is susceptible to disclosure or use by anyone other than the owner;
- Vendor default passwords (default passwords must be changed immediately upon use);
- Visible on a screen, hardcopy, or any other output device;
- Hard coded into software developed (unless permission is obtained by the agency security office);
- Stored in dial up communications programs or internet browsers at any time;
- Recorded in system logs unless the password is encrypted in the log.

Passwords must not contain:

- Repeated letters or numbers or sequences of letters or numbers;
- A word contained in any English or foreign language dictionaries;
- A common phrase;
- Names of persons, places, or things;
- The UserID;
- Repeating letters with numbers that are indicative of the month; i.e., vmPtm\$01 in January, vmPtm\$02 in February.

Passwords must:

- Be eight (8) or more characters;
- Contain uppercase letter(s);
- Contain lowercase letter(s);
- Contain a number;

- Contain a special character.

Accounts with privileged access must:

- Be eleven (11) or more characters where permissible or the maximum allowed length;
- Contain uppercase letter(s);
- Contain lowercase letter(s);
- Contain a number;
- Contain a special character.

Exceptions must be documented for auditing purposes.

Password History

Individuals must not reuse previously used passwords. To prevent this, a password history of 12 or more previous passwords must be kept.

Password Change

Passwords must be changed by the user at least every 31 days. If inadvertent disclosure is known or suspected, the passwords must be changed immediately. NOTE: In the event misuse is suspected, do NOT change the password; IMMEDIATELY notify the System/Network Administrator and/or the agency's security office. A security incident must be documented. Subsequent password change shall be made by the System/Network Administrator's and/or agency's security office direction only.

Non-Expiring Passwords

All requests for non-expiring passwords for COT managed servers must be submitted to COT, Security Administration Branch.

All requests for other non-expiring passwords must be submitted to the agency security officer.

The request must include the platform on which the UserID and password are used; sensitivity of the data accessed by the UserID; the function the UserID is performing that justifies having a non-expiring password; and additional security safeguards used to secure the use of the UserID and password (i.e., encryption, UserID not used for log-in). Included in the request should be a migration plan for moving toward compliance.

Exceptions will be approved by the Security Administration Branch on a case-by-case basis. Examples of exceptions considered for approval are:

- System Process UserIDs
- Application UserIDs used to connect to the database

The makeup of a non-expiring password is very important, as the strength of the password will determine how easily it can be broken. Every effort must be taken to ensure that the non-expiring password complies with the strictest interpretation of the COT password composition rules. For passwords used in cases of compiled programs, the length should be equal to or greater than 16.

Assignment of Passwords

The initial passwords issued by an administrator must be valid only for the user's first on-line session. At that time, the user must be forced to choose another password before any other work can be done. The initial password must comply with password composition rules.

Minimum Password Age

Where supported, the minimum password age must be set to one day. This will help prevent users from “cycling” through passwords, thus bypassing the password history list. However, if inadvertent disclosure is known or suspected, the password must be changed immediately. In such instances, notify the systems administrator immediately.

Storage of Administrative Passwords

Administrative passwords with special access must be stored off-site at the agency-approved disaster recovery location. A procedure must be established to ensure that the passwords are kept current.

Protection of Password Generation Algorithms

If passwords or PINS are generated by a computer system, all software and files containing formulas, algorithms, and other specifics of the process must be controlled with the most stringent security measures supported by the involved computer system.

Personal Identification Numbers (PINs)

All PIN's must be created with a similar construction as passwords in that they must not be numbers that are easily identifiable with the user. Password composition rules may not apply to PINs; however, other applicable password rules apply. Since a PIN may be used for individual authentication and have legal standing as an electronic signature under current state law, agencies should consult KRS 369 or contact COT for assistance.

Cookies for Automatic Log-in

Users must refuse all offers by software to place a cookie on their computers so that they can automatically log-in the next time that they visit a particular Internet site.

Password and UserID Lockout

To prevent individuals from attempting to log-in with UserIDs by guessing passwords, accounts will be locked after three (3) consecutive invalid log-in attempts. Password resets must follow the policy stated herein for password length/composition.

END