

**Education and Workforce Development Cabinet
POLICY/PROCEDURE**

Policy Number: EDU-02

Effective Date: December 21, 2004

Revision Date: December 20, 2012

Subject: UserID and Password Policy

Policy: This policy supports the Education and Workforce Development Cabinet (EDU) 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).

Scope: This policy applies to all EDU employees and contractors, including all persons providing contractor services, who use, process, or store computerized data relevant to agency business on an EDU maintained server or workstation.

Policy/Procedure Maintenance Responsibility: The EDU Agency Security Contacts (ASC) is responsible for the maintenance of this policy. The Chief Information Officer (CIO) is responsible for the revision of the EDU Policy and Procedures Manual (PPM). The EDU CIO is responsible for authorizing all changes to the PPM.

Applicability: All EDU employees and contractors shall adhere to the following policy.

Responsibility for Compliance

Each Department/Office 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, intentional misuse and/or inappropriate use may result in disciplinary action pursuant to KRS 18A up to and including dismissal. It is also each Department's responsibility to enforce and manage this policy.

Overview

Passwords are the first line of defense against unauthorized users. The Computer Emergency Response Team (CERT) reports password cracking as the most popular computer attack. Users have a tendency to create passwords from what is familiar such as pet names, anniversary dates, and other easy to remember words. However, there are no good passwords that use words found in the dictionary. For example words that contain alpha, numeric and special characters would be considered a strong password.

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. UserID must not be shared nor used to login the computer in for someone else to use.

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. If an expiration date is not provided, a default of 31 days must be used.

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; and
- Mixed-case alphabetic (A,a), numeric(1,2) and special characters (@,#), or ASCII characters (required).

Passwords must not be or contain:

- Reused;
- Shared with other users;
- Repeated sequences of letters or numbers;
- A word contained in English or foreign language dictionaries;
- A common phrase;
- Kept on paper;
- 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;
- Names of person, places, or things that are easily identified with the user;
- The same as the UserID;
- Repeating letters with number that are indicative of the month; i.e., vmPtm\$01 in January, vmPtm\$02 in February etc..
- 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's 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;
- Emailed

Password Composition

Password length must be eight (8) or more characters. Passwords must use a combination of letters (UPPER/lower case), numbers and the use of at least one special character or ASCII extended character is required. For those UserIDs that have administrative access, minimum password length must be 11 characters or more where permissible. In those instances where a password length of 11 is not permissible, the maximum length allowed must be used. Since password change is required on a monthly basis, the number used in the password creation should not be the numeric value of the month (e.g. December = 12).

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

The user must change passwords 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 EDU's Security Audit Group. A security incident report must be completed (EDU-F01). Subsequent password change shall be made by the System/Network Administrator's and/or EDU's Security Audit Group direction only.

Non-Expiring Passwords

All requests for non-expiring passwords for the EDU UserIDs must be submitted to Chief Information Officer. The Security Exemption Request form (**EDU-F03**) must be used to request an exemption.

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.

The CIO on a case-by-case basis will approve exceptions. 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 EDU 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 two (2) days. 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 in an encrypted file that can be accessed by the CIO or authorized personnel at the agency-approved off-site 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.

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.

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 Administration

Password Security

Software must be installed in such a manner as to prevent general system users with the capability to view password or access control tables, bypass security mechanisms, or use restricted security software functions.

Security Privileges

The least amount of security privileges required for a person to perform their job must be assigned. Furthermore, privileges must be layered to reflect job functions and separation of duties. For example, different security privileges for System Administrators, Backup Operators, Managers, and end-users must be defined. People may be assigned multiple UserIDs in order for them to perform their work. For instance, one UserID may be used while performing server administration functions while another UserID is used for checking e-mail, searching the Internet, or entering time into a time tracking application.

User Verification

When an individual requests that their password be reset, or they are authorized a UserID, the System/Network Administrators must verify the identity of the requestor and ensure they have access to the UserID. This can be accomplished through call back, caller id, supplying some key identification number such as last four digits of their social security number, or visually inspecting their employee or contract badge.

Individual Access Termination

For situations involving employment termination, the CIO must be notified immediately so UserIDs assigned to the individual may be disabled, minimizing the security exposures a potentially disgruntled individual may cause.

Password Utilization

Telecommunications Security

Where dial-up capability is present, access controls must be implemented only through approved combinations of hardware and software security tools that meet the following requirements:

- Unique identification or access code (UserID) for each user
- Verification of UserID by the use of a secret password, separate from the operating system UserID/password assigned to the user. Security tokens or software challenge /response methods that generate dynamic passwords are the preferred methods for authenticating dial-up access users for systems connected to the EDU network. Systems using fixed password dial-up authentication must provide password management functions to enforce periodic change intervals and password syntax standards. The CIO must approve exceptions to this policy. The Security Exemption Request Form must be used to request an exemption.
- Employees and contractors must be cognizant of not storing sensitive information (including system passwords) on their home computers when dialing-up remotely.

Workstation Security

Workstations must be configured with screen savers to blank the screen and require a password to resume operation whenever the workstations are unattended for a period of 10 minutes. Workstations performing administrative duties must be configured with screen savers to blank the screen and require a

password to resume operation whenever the workstations are unattended for a period of 5 minutes. EDU employees and contractors must not leave their workstation unattended without first shutting down the workstation, locking the workstation, logging out, or invoking a password-protected screen saver. The owner of the workstation has ultimate responsibility for the security of the information on their workstation. Workstations will not be logged onto by a user and shared by multiple users (exception to this are the workstations used by the resource rooms).

For workstations that employ operating systems software that have the capability to enact password restrictions, such as Microsoft Windows NT, those capabilities must be configured and enabled.

Procedural Issues

Audit Trails

To provide a logical audit trail, both successful and unsuccessful log-in attempts must be recorded with the following information:

- Terminal addresses (TCP/IP, MAC, etc.)
- UserID
- Date and time of occurrence
- In the event of a breach or an audit, the EDU Security Audit Group will review event logs

Specific Procedure for Hacker/Cracker Incidents

Hacker incidents can be divided in to three types: Attempts to gain access to a system; an active session on the system; or events which have been discovered after the fact. When facing one of the three types of hacker incidents, contact the EDU Security Audit Group, notify your manager of the breach and leave the computer on but lock the workstation. Hacker/Cracker incidents shall be reported using Security_Incident Reporting Form (**EDU-F01**).

Review Cycle:

Annually

Timeline:

Review Date: November 29, 2012

Reviewed By: EDU Agency Security Contacts

Enterprise Security and Policies

Cross Reference:

<http://technology.ky.gov/governance/Pages/policies.aspx>

CIO-072 -- UserID and Password Policy

CIO-081 -- Securing Unattended Workstations Policy

OTS Standards

Cross Reference:

EDU-F01 -- Security Incident Report Form

EDU-F03 -- Security Request Change Form