IT Password Protocol

This password policy is being implemented at the request of the EKU Auditor as well as other external auditing agencies. Information resources are vital assets that require protection in order to ensure the integrity of computing facilities for all constituencies of Eastern Kentucky University. These requirements are intended to afford an adequate level of security with as little inconvenience as possible for all involved.

Data, whether stored in central computers accessible through remote systems, processed locally on microcomputers, delivered via email, or generated by word processing systems, are vulnerable to a variety of threats. Unauthorized access to the University's information or systems has been identified as a major information security risk that must be proactively managed. Access to our IT resources by unauthorized people or computer processes can result in:

- The University's sensitive information (personal, both staff and students; research; financial) being compromised.
- Non-compliance to legal and regulatory requirements; e.g. Privacy Act, and prosecution through non-adherence to legislation
- Adverse impact on the University's image and reputation
- Theft of University resources and the potential for other unlawful acts.

With the increase in attempted break-ins to computer systems across the world it is critical that everyone at EKU do their part to protect our computing resources and assets. If someone else determines your password, they can effectively assume your electronic identity. This means that individual then has full access to your files, your e-mail, personal information, and more. This intruder could modify or destroy your files, send threats via e-mail in your name, or subscribe to unwanted services for which you would have to pay. In short, an insecure password can easily wreak havoc in your life. It is your responsibility to guard your password in the same way you would guard a personal bank account pin.

It may be argued that less strict policies than those defined in this document are appropriate for systems that do not store "sensitive" information. However, it must always be remembered that if such systems are connected to the University network, they can potentially provide a means of unauthorized access to sensitive information residing in other locations. Whenever possible, therefore, the comprehensive access control regime defined here should be adopted to mitigate the risks in this area.

Central computer and network systems will have accounts created and/or activated as new hires are entered in the Human Resources system. When employees leave the university, accounts will be removed after Human Resources has completed their termination procedures. Similar procedures are in place for student accounts in conjunction with admission to the University and continued enrollment. Support staff such as help desk personnel will work with users to create and change secure passwords/pins that will provide adequate protection. Procedures are in place to ensure the authenticity of callers requesting password/pin assistance. In some instances,

changes will only be made when the account holder is present and has presented sufficient identification.

1. User IDs shall be unique and assigned to an individual EKU computer and/or network system user. Shared computer and/or network system user accounts shall only be used in the extraordinary case when it is not operationally feasible to do otherwise, and the risk of using shared accounts is at an acceptable level. The assigned individual for the shared account is still fully responsible for all activity in that account.
2. It is the responsibility of everyone to keep his or her passwords and/or pins secret. Passwords/pins are considered confidential information and shall not be shared or transferred to others.
3. Passwords/pins must not be written down, or otherwise posted, where they could be seen or interpreted easily by others.
4. Where technically and operationally feasible, passwords/pins shall not be electronically stored, cached, or transmitted in clear text via e-mail or any other technical means.
5. Passwords/pins must be changeable by the user except in the extraordinary case of shared user IDs and passwords/pins. In the case of shared user IDs and passwords/pins, procedures must be in place to securely manage the shared user ID and password/pin (e.g., password/pin change and distribution). An audit log of password/pin changes will be kept where supported by the system.
6. Minimum password requirements for EKU computer and network systems are as follows (as available in the system):

    - Passwords/pins shall be a minimum of 10 characters in length.
    - Passwords must meet complexity requirements. Passwords must have 3 of 5 characteristics below to be complex:
        - Uppercase letters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
        - Lowercase letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
        - Base 10 digits (0 through 9)
        - Non-alphanumeric characters (special characters) (for example, !, $, #, %)
        - Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
    - When choosing passwords, users should avoid using their name, pet's name, relative's name or other common names, user ID, dictionary words (including words from foreign language dictionaries), drowssap (password spelled backwards), not be a set of adjacent keyboard keys (e.g., POIUY), birth date, phone number, address, or any other type of personal information or that which is easily derived from such information.
    - Passwords/pins shall be changed every 90 days.
    - Password history is enforced. The previous 4 passwords will not be allowed to be used.

- After 6 consecutive unsuccessful logon attempts, computer and network system user accounts will be locked out for a period of at least 30 minutes. Systems will be monitored for login failures.

7. Authentication information stored on any University computer or network system shall be protected so the authentication information cannot be accessed by an unauthorized user or process.
8. Workstation screens shall be locked after 15 minutes of in inactivity. Windows workstation users and administrative system users must re-authenticate after the timeout period.
9. System Administrators shall periodically review and remove or modify EKU computer and network system user accounts as appropriate or whenever the status of the user changes. This process will be automated wherever possible.
10. Eastern Kentucky University reserves the right to review and/or require change of any identification and/or authentication process for compliance with this policy.