|  |  |
| --- | --- |
| *Communications and Information Technologies(CIT)*  Banner : Operating System Shell Account Password  Management Policy | |
| Purpose | The purpose of this policy is to establish standard practice for  operating system password management for shell access to the  Banner operating system (OS) shell account environment. |
|  | |
| Scope | This policy applies to all Faculty, Staff, Students, and/or Vendors of the  University that use the Banner system via operating system shell  account access. Operating system levels access is currently only  available via secure shell encrypted access mode. Shell account  passwords must be managed in accordance with password policy  described herein. This policy establishes the requirements for creating  strong passwords, the protection and management of passwords, the  frequency passwords are to be changed, and password privacy. |
|  | |
| Policy | Operating system (OS) shell account passwords in the Banner system  must be managed to ensure 90 day password expiration and forced  password change and complexity. Passwords must comply with the  minimum strong password requirements described herein. All other  passwords for other systems must comply with the latest general  password policy last posted to URL:  http://www.tnstate.edu/cit/documents/policies/PasswordPolicy.doc |
|  | |
| Procedures | **Creation of Strong Passwords:** The use of strong passwords  is necessary to thwart would be computer hackers attempting to  “guess” your password using what are known as “password  crack” programs.  **Strong password construction criteria:**   * Must be at least eight (8) characters in length * Must contain at least 1 uppercase letter (A–Z)   Must contain at least 1 lowercase letter (a-z)  o Must contain at least 1 or more numbers (0-9) or special  characters.  **Additionally, the construction of passwords should not:**   * Include a word in any language, slang, dialect, jargon, etc. * Be based on personal information, names of family, * birthdates, etc.   **Password Management and Protection**   * Passwords must not be inserted into email messages or * other forms of electronic communication. * Do not use the same password for TSU accounts as for * other non-TSU access (e.g., personal ISP account, option * trading, benefits, etc.). |
| Procedures | Do not share TSU passwords with anyone, including  administrative assistants or secretaries. All passwords are  to be treated as sensitive, Confidential TSU information   * Passwords should never be written down or stored on-line * Do not reveal a password over the phone to ANYONE * Do not reveal a password in an email message * Do not reveal a password to your boss * Do not talk about a password in front of others * Do not hint at the format of a password (e.g., "my family * name") * Do not reveal a password on questionnaires or security forms * Do not share TSU passwords with anyone, including * administrative assistants or secretaries. All passwords are * to be treated as sensitive, Confidential TSU information * Passwords should never be written down or stored on-line * Do not reveal a password over the phone to ANYONE * Do not reveal a password in an email message * Do not reveal a password to your boss * Do not talk about a password in front of others * Do not hint at the format of a password (e.g., "my family * name") * Do not reveal a password on questionnaires or security * formsname") * Do not reveal a password on questionnaires or security forms * Do not share a password with family members * Do not reveal a password to co-workers while on vacation * Do not use the "Remember Password" feature of * applications (e.g. Outlook) that remembers your password * when the username is entered. * Do not write passwords down and store passwords * anywhere in your office * Do not store passwords in a file on ANY computer system * including mobile devices without encryption * Change passwords every 90 days or password will expire.   **Monitoring, Enforcement, and Reporting:** Operating system  password management controls for shell accounts are  implemented in this policy. Passwords which expire after 90  days will require renewal actions by the affected user(s).  Password complexity is implemented within the limits of the  operating system capability. Quarterly reports on the password  renewal status may be created upon request by CIT  management.  **Password Reset Frequency:** Banner operating system user  shell accounts on Banner SQL server, INB, SSB, and MyTSU OS  nodes will be forced to reset passwords every 90 days.  Otherwise, passwords will be set to expire.  **Password privacy :** If a password compromise is suspected,  report the incident to CIT and change all passwords. No one  should every demand your password including CIT staff. If your  account has issues that require CIT to login, the password will be  reset with your knowledge and once the work is completed, you  will be requested to reset the password to one of your choosing.  **General Password Construction Guidelines:**  **Weak passwords** have the following characteristics:   * Contains less than eight characters * Forms a word found in a dictionary (English or foreign) or * is a common usage word such as: * Names of family, pets, friends, co-workers, fantasy * characters, etc. * Computer terms and names, commands, sites, * companies, hardware, software. * The words "TSU" or any derivation * Birthdays and other personal information such as * addresses and phone numbers. * Word or number patterns like aaabbb, qwerty, * zyxwvuts, 123321 * Uses any of the words referenced above spelled * backwards * Uses any of the above preceded or followed by a single * numeric digit (e.g., secret1, 1secret)   **Strong passwords** have the following characteristics:   * Contain both upper and lower case characters (e.g., a-z, * A-Z) * Have digits and punctuation characters as well as letters * e.g., 0-9, !@#$%^&\*()\_+|~- =\`{}[]:";'<>?,./) * Are at least eight alphanumeric characters long. * Not a word in any language, slang, dialect, jargon, etc. * Not based on personal information, names of family, etc.   **Terms and Conditions**  Only CIT staff have access to banner system accounts named  “oracle” and “banner”.  CIT staff must execute “su” in order to use the oracle and  banner account roles  CIT MIS department will be responsible for sharing the “oracle”  and “banner” account passwords with CIT MIS employees.  All shell accounts will include standard shell logging and system  logging.  A notice of university computing no expectation of privacy  notice may be included on the system login page.  A notice of university acceptable use may be included on the OS  system login page.  All users should exerciser appropriate caution to avoid any data  corruption or loss, since system backups are only intended for  disaster recovery mitigation.  All data on the system are subject to the university  confidentiality agreements as well as relevant state and federal  rules and regulations. |

Revised 02/26/2013