FAYETTEVILLE STATE UNIVERSITY

ADMINISTRATIVE SYSTEM SECURITY ADMINISTRATION

Authority:	Information Technology and Telecommunication Services
Category:	University-wide
Applies to:	Faculty, Staff, and Students
History:	Approved on….Jul 1st, 2005 First Issued on Feb 2nd, 2005 Revised August 31, 2011
Related Policies:	Copyright Ownership and Use Policy - [1.20] Information Security Policy Acceptable Use Policy of Computer Resources Data Ownership Network Use Policy
Contact for Info:	Chief Information Officer – (910-672-1477)

I. Purpose

The purpose of this policy is establish/provide Standard Operating Procedures (SOP) for Banner Security Administration and relevant third party applications. To establish a standard for creation of a Banner User account, creation of strong passwords, the protection of those passwords, and the frequency of change. This Policy applies to:

A. All individual users (FSU students, faculty, staff, and others affiliated with FSU, including but not limited to those in program or contract relationship with FSU), who use the Native Banner System and other relevant third party applications.

B. All Banner related resources owned or managed by (FSU).

C. Steps to follow when creating, modifying, and deleting a Banner User Account to include modifications throughout the life of an account.

II. Definitions

Terms used in this policy. Knowledge of these definitions is important to an understanding of this policy.

A. Password - A string of characters that serves as authentication of an individual’s identity, which are to grant or deny access to private shared data.

B. Password History File - An encrypted file that contains previous passwords used by the userid.

C. Password Lifetime - The length of time a password may be used before it must be changed.

D. Strong Password - Strong passwords are constructed of a sequence of upper and lowercase letters, numbers and special characters depending on the capabilities of the operating system or application. Typically, the longer the password the stronger it is. Passwords must be unique and not easily tied back to the end user such as userid, given name, social security number, telephone, employee number, phone or office numbers, address, nicknames, family or pet names, birth date, license plate number, etc.

E. User Account - A user account is a collection of information that tells Banner what files and folders you can access. The user account is made up of the end userid and password.

F. User - The individual requesting a user account in order to perform work in support of a FSU program or a project, by accessing the FSU computer network.

G. Userid - Also referred to as a username. A construction of letters and numbers that, in conjunction with a password, uniquely identifies a person.

III. Responsibilities

A. User - is responsible for the day-to-day hands on security of Banner and relevant third party system assets.

B. Chief Information Officer - has overall responsibility for Administrative Security Administration.

C. Applications Manager - is responsible for identifying and training those responsible for Banner Security Administration. Also responsible for providing all required equipment and tools necessary to perform their duties.

D. Network Administrator - is responsible for providing connectivity to the FSU network.

E. Banner Security Administrator or Relevant Third Party Application Administrator - responsible for following the procedures established in this document.

F. Departmental Banner and Third Party Application Security Managers - are the gatekeepers of access to University Data contained within Banner and relevant third party application databases. Their duties are as follows:

1. Determine appropriate Security Class or profile associations for new and existing departmental users.
2. Act as a central point of contact for Banner access related departmental issues.
3. Act as primary departmental contact with Banner Administration for access and profile related problem resolution.
4. Review, update, or delete security access or profiles on a quarterly basis.

IV. Violations of Policy

FSU considers any violation of this Policy to be a serious offense and reserves the right to copy and examine any files or information resident on FSU ITTS resources to ensure compliance. Violations of this policy should be reported to the appropriate FSU authority.

V. Disciplinary Actions

Violators of this Policy may be subject to disciplinary action up to and including dismissal or expulsion pursuant to applicable Board policies and collective bargaining agreements.

VI. Banner Password Criteria

When composing a password, it must adhere to the following standards:

A. Passwords must be a minimum of eight (8) characters. Passwords must be complex and difficult to guess. Passwords shall be composed of a variety of letters, numbers and symbols[4] with no spaces in between. (Strong passwords must be used).

B. Passwords must not be reused until six additional passwords have been created. (Verified against a password history file that is set to the maximum size that the system supports)

C. Privileged account passwords (system accounts, administrative accounts, etc.) must be changed at least every thirty (30) days. User account passwords must be changed at least every ninety (90) days. (maximum lifetime)

VII. Password Protection

All passwords are treated as sensitive, confidential FSU information and therefore must be protected as such:

A. A password administrator must not reset passwords without the user first providing definitive evidence substantiating his or her identity.

B. Passwords issued by a password administrator must be unique and must be sent via a communications channel other than the channel used to login to the system.

C. Passwords must never be shared or revealed to anyone other than the authorized person. Passwords must not be written down on any medium.

D. Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, devices without access control, dial-up communications programs, Internet browsers, cookie files or in other locations where unauthorized individuals might discover or use them.

E. Passwords must immediately be changed if the user suspects their user ID or password has been disclosed to an unauthorized person or if the system has been compromised.

VIII. Requesting a new Banner Account

Before you can access specific screens in the Banner system, you will need to be granted access. The departments that assume ownership of specific modules in the system approve requests for access. For this reason, access requests typically require multiple approvals from across campus before ITTS can complete the process.

A. A Banner account will only be created after completion by an authorized person and submission of the Banner Account Request form located at the below link. https://forms.uncfsu.edu/departments/ITTS/BannerSecurity/index.cfm

B. If any part of the logon process (User ID, Password, etc.) is incorrect, the user must not be given specific feedback indicating the source of the problem. Instead, the user must simply be informed that the entire logon process was incorrect.

C. Passwords issued by a password administrator must be pre-expired, forcing the user to choose another password before the logon process is completed

IX. Banner User Accounts

The following standards are enforced when using a user account:

A. User accounts must be locked out for a period after a maximum of three (3) unsuccessful attempts to gain access to a user account

B. Accounts shall be created utilizing the steps as outlined in the Banner Security Administration guide.

C. Fayetteville State University Affiliate Accounts

User Accounts established for an affiliate of the University must have a specified expiration date unless the provision of a user ID without a specified expiration date is approved in writing by the Security Administrator. If an expiration date is not provided, a default of thirty (30) days must be used. A University affiliate is any non-employee, contractor, vendor, third party consultant or temporary employee who has an approved, legitimate business relationship with the University that requires them to gain access to University resources. Affiliates must adhere to the same university and UNC system policies and procedures as traditional University employees.

D. Access Control

If existing access controls pose a risk that confidentiality may be breached, access control may be modified in response to the confidentiality of information contained on the system.

X. Concurrent Banner Connections

A maximum number of concurrent connections for an individual user ID must be set to two (2).

XI. Workstations

Workstations shall be safeguarded from unauthorized access especially when left unattended. All workstations shall be configured to require a password-protected screen saver after a maximum of thirty (30) minutes of inactivity. Users shall not disable the established password-protected configuration specifications.

XII. Banner Account Termination

When a faculty or staff member leaves the University for any reason, it is the responsibility of the Office of Human Resources to notify the Banner Security Administrator, ITTS of the change in the individual's employment status. The Human Resources designee must submit the Delete Account Request Form to begin the termination process. Under normal circumstances access to BANNER may be promptly terminated:

A. When the user's employment is terminated.

B. When the user's job functions change and access is no longer required.

C. When the user account is inactive for thirty (30) days, the account must be disabled, except as specifically exempted by the Security Administrator.

D. Immediately, if it is determined that the user has violated any Fayetteville State University confidentiality, Information Security, Administrative System Security or Use of Computer Resources policy.

XIII. Disclaimer

FSU disclaims any responsibility for and does not guarantee information and materials residing on non-FSU systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions, or values of FSU, its faculty, staff, or students

XIV. Notice

As laws, technology and standards change from time to time, this Policy may be revised as necessary to reflect such changes. It is the responsibility of users to ensure that they have reference to the most current version of FSU Policies.