

BANNER Security Guideline (Draft) - September 16, 2005

A. Purpose:

To establish guidelines for accessing and using the University 's BANNER data.

B. Definitions:

BANNER Steering Committee: A committee comprised of BANNER Data module owners, department managers, end-users, and IT personnel (i.e Banner System Administrators) responsible for coordinating the development, implementation, maintenance, and general stewardship of the SunGard SCT BANNER information system at SCSU.

BANNER module Data owner: The individual responsible for the administrative oversight of a given BANNER system (i. e. Student, Finance, Financial Aid, etc.) and ultimately responsible for the data within said system.

Banner System Administrators: The individuals responsible for the Banner servers, Banner and Oracle Data base Administration (i.e. DBA) and Banner Operational support & Application Developers.

C. Banner Access Guidelines

1. BANNER data is the property of SCSU Access to BANNER data is restricted to authorized personnel only. Unauthorized access is prohibited.
2. BANNER data will be used for official University business only. Specific non-University business use of BANNER data may be authorized under other official University policy. Unless specifically permitted by another official University policy, the use of BANNER data for personal gain or curiosity, or another's personal gain or curiosity, is prohibited.
3. Persons, and processes, accessing BANNER data will uphold the confidentiality and privacy of individuals whose data they access and observe any laws, regulatory requirements, policies and ethical restrictions that may apply with respect to their accessing, using or disclosing such information.
4. Persons, and processes, with access to BANNER data, regardless of its form (electronic or print), will insure that all reasonable and prudent measures are taken to protect the data from theft and unauthorized or accidental viewing, copying, downloading, modification or destruction. The data must be protected while in use, in transit and in storage. The Department of Information Technology is to be notified immediately in the event the security of any BANNER or other administrative data is compromised.
5. Access to specific data is generally limited by need to know, job responsibilities, supervisor approval, and system or data owner approval. Thus, anyone in the

- service of the University , with a genuine business or educational need, may be authorized to access the BANNER data necessary to perform their duties. An individual's access to BANNER data will be removed when the individual leaves the service of the University or during an extended absence. Supervisors are to notify the Office of Information Technology and the Office of Human Resources immediately when an individual, including student employees, leaves their service or begins an extended absence.
6. BANNER Module Owners have the sole authority to authorize access to the data within the modules they administer. Module Owners are encouraged to use the principle of least privilege when authorizing access to their module data.
 7. For various security reasons,
 - a) there must be a segregation of management functions between BANNER module Data owner and Banner System Administrators
 - b) user access privileges periodically reviewed to ensure compatibility with job description
 - c) The use of generic accounts is prohibited for any use that could contain protected data
 - d) Logging will be reviewed to determine if logs are being saved an appropriate number of days (minimum 30 days).
 - e) Users accounts will need to meet the following complexity rules
 - i) Password length needs to be a minimum of 8 characters
 - ii) Passwords need to contain a minimum of three of the following classes, upper case characters, lower case characters, numbers and special characters
 - iii) Password will have a required change interval that the user must enter a new password. Normal recommendations would be 90 days..
 - iv) If an invalid password is entered more then 5 times the account will be locked out and require to be unlocked by IT.
 - v) The new password can not match a password used in the last twelve
 - vi) Privileged accounts through policies need to have stronger password security then user accounts.

D. Reporting Violations:

Any suspected violations of these policies, or unauthorized access to computing resources, or any other condition which could compromise the security of BANNER data or other University computing resources must be reported to the Office of Information Technology, CIO or Banner System Administrator (???) or Office of Human Resources.

E. Remedies for non compliance:

Failure to comply with these policies may result in one or more of the following actions:

- a) suspension of access to the network for the individual or unit violating the policy,
- b) When appropriate, disciplinary action ranging from warning to termination and (for students) expulsion from the University , depending on circumstances, in accordance with applicable policies and procedures,
- c) when appropriate, initiation of civil or criminal proceedings.