Banner Data Security Policy

Administrative data are essential to Wofford College's business functions, which include, but are not limited to, financial, personnel, student, alumni, communication, and physical resources. The Data Security Policy defines the security and protection requirements for administrative data. The policy applies to data maintained both in the Banner database and at the departmental and office level, regardless of the media on which they reside. It does not include library holdings or research or instructional material unless they contain information that relates to a business function. The policy also describes the rights and responsibilities of Wofford personnel in the handling, dissemination, security, and protection of administrative data.

College procedures regarding data security shall comply with all applicable federal and state laws and regulations that govern the privacy and confidentiality of data.

Wofford College retains ownership of all administrative data created or modified by its employees as part of their job functions.

Classification of Administrative Data

For security purposes, administrative data is of three types, each requiring a different level of protection. Because of the sensitivity of the data maintained in Banner, which should be assumed to be confidential or private unless otherwise specified, the Banner system is for authorized users only.

1. Confidential Data

Confidential data requires a high level of protection. Confidential data includes information whose loss, improper use, or disclosure could adversely affect the ability of the College to accomplish its mission. It also includes records about individuals requiring protection under the Family Educational Rights and Privacy Act of 1974 (FERPA) and data not releasable under the Freedom of Information Act.

Access to confidential data is restricted and is available only to individuals who require that information to perform their College functions. It should not be discussed with others, except in the course of performing these functions. Confidential data includes, but is not limited to:

- Student data on social security number, grades, financial aid, parent’s financial status, accounts receivable transactions, biography and academic history.
- Employee data on social security number, salaries and benefits, disabilities, evaluations, appointments, and biography.
- Alumni and Friends data on social security number, gifts, pledges, financial status, and biography.

2. Private Data

Private data is data whose destruction or unauthorized disclosure would not necessarily result in any business, financial or legal loss, but which involves issues of personal privacy. Some private data may be available campus-wide, but will not be available to the public. Private data includes, but is not limited to:

- Student and Alumni data on college address and phone, email address, major field, data and place of birth, dates of attendance, degree, honors and awards received, employment, home address and phone.
- Employee data on email address, home address and phone number.

3. Public Data

Public data is available or distributed to the general public regularly or by special request. It can include names, departments, titles, degrees and majors of graduating seniors, and information in the College catalog.

Data Custodians and Data Owners

Each administrative office shall designate a Data Custodian who is responsible for the day to day oversight of administrative data in his or her functional area. The Data Custodian usually is the office head. The responsibilities of the Data Custodian include the following:

- Ensuring that his or her office's uses of administrative data are consistent with federal and state law, regulatory agency requirements, contractual obligations, and existing College policies.
- Ensuring the quality of data residing in the office's applications.

Although some of the Data Custodian's responsibilities may be delegated to others in his or her functional area, the Data Custodian will continue to have overall accountability for the use and security of the data.

An Owner of a specific set of administrative data is the Data Custodian in the office that is designated by the Banner Data Standards and Security Committee as responsible for the upgrade and maintenance of that data. The Data Owner also may be designated by the Banner Data Standards and Security Committee as being responsible for the review and approval of all requests for access to and update capability for that data.

It is the responsibility of the Data Owner to ensure that all individuals who are given access to confidential data are instructed about their confidential nature.

Banner Data Standards and Security Committee

The purpose of the Banner Data Standards and Security Committee is to oversee the on-going operation of the Wofford College Banner Information System. Members of the Data Standards and Security Committee will be the Vice President of Technology, the Banner Database Administrator, the Banner System Administrator, a staff member designated by the Data Custodian from each administrative office, and a member of the faculty.

The Banner Data Standards and Security Committee will be responsible for:

- Decisions on maintenance, upgrade, and access to specific administrative data, including the assignment of Banner classes and roles. Classes determine the forms (screens) an individual can see, which in turn determine the information to which that individual has access. Roles determine whether a person only can view the information (read-only access) or also can change the information (read-write access).
- Changes in the Wofford College Data Standards and Data Security policies.
- Coordination of testing on new procedures, modules, or versions of Banner as upgrades are made available.
- Implementing recommendations of the Banner Users Group

Routine decisions on maintenance, upgrade, and access to administrative data may be delegated to the Data Owners. In this case, the Banner Data Standards and Security Committee will be available to resolve disputes, should they arise, among offices about access to data.

Requesting Authorization for Forms Access to Banner Data

Requests for access to data using Banner forms should be submitted electronically to the Data Owner, who will arrange the access with the Banner DBA. We will use the principle of least privilege in granting access to data: users are not to be given access to more data, or given more access privileges, then is necessary to perform their duties. No Banner user will be permitted to query all Banner data.

We recommend a conservative approach when assigning Banner access privileges, which should be commensurate with an employee's training, knowledge, skills, degree of supervision, and assigned duties.

Third Party Access to the Banner Database

Users are granted query-only access to Banner tables via an ODBC login to the database using third-party reporting tools such as MS Access, MS Excel, and Crystal Reports. Data Owners are responsible for determining which database role a user, needing third-party access to the data within the Data Owner's Banner domain, will be given.

Users accessing Banner using third-party tools are responsible for complying with all College policies regarding privacy, security, and the appropriate use of Banner data. Supervisors are responsible for ensuring that their staff members comply with said policies and procedures.

In general, data are entered and manipulated in the Banner database only through the Banner forms. In exceptional circumstances, such as the verification of large data loads, limited Insert/Update/Delete access using third party tools will be granted on a temporary basis.

Direct Modification of Banner Data

Only the Banner DBA will be allowed to directly modify Banner data in order to correct errors. Such modifications must be requested in writing or electronically by the Data Custodian responsible for the data. After the correction has been made, the Banner DBA will retain a record of the authorization and of the actual updates made.

Requesting Authorization for Data Extraction

Extraction of administrative data for processing on other systems should only be done for purposes that cannot be accomplished using Banner. If data extraction is necessary, the confidentiality, integrity, and accuracy of the downloaded data must be ensured. Data extraction is to be done only by individuals who have been granted permission by the Banner Database Administrator and the Data Owner to do so. Requests for permission to extract data are handled in the same way as requests for authorization for access to that data.

Employee Responsibility

Individuals are responsible for the security of administrative data. Employees must:

- Not access and use information in unauthorized ways. Employees must not peruse through administrative data not specifically provided to them for their work. They must not enter areas where administrative information is stored unless they are authorized to do so.
- Secure their passwords to protect data from unauthorized access.
    - *Never share passwords*, even with a supervisor or an IT staff member.

    - Select passwords that are not obvious choices. Passwords other than family member names, nicknames, and words found in the dictionary are preferable. Including characters other than letters in passwords also is worthwhile.
    - Never tape passwords to a wall, under a keyboard, or in other easily discoverable areas.
    - Change passwords every 90 days or so even if a system does not force it.
- Log off desktop computers to a point that requires a new log-on whenever they leave their work area, except for specially designated areas. All access IDs must be logged off whenever an employee leaves for the day.
- Orient screens to prevent unauthorized people from reading confidential or private information. The location of the screen must face away from any traffic areas.

Unauthorized or inappropriate use of data or lack of adherence to security policies and procedures will not be tolerated and may result in disciplinary action, which may include termination of employment.

Supervisor Responsibility

It is the responsibility of supervisors to maintain a high level of security in the work place. Supervisors must

- Ensure that employees comply with security policies and procedures. Supervisors must counsel staff who violate security procedures and are responsible for managing improvements in staff behavior. If violations continue, the problem must be resolved.
- Remove access when staff members separate from the office.
    - Supervisors must notify the Human Resources Office and Banner DBA when an employee voluntarily separates from an office, so that the employee's access can be closed at the end of the last day of employment.
    - When an employee is terminated, the supervisor must report the dismissal to the Human Resources Office and Banner DBA prior to the termination meeting in order that computer access can be cancelled during the meeting.
- Supervisors periodically should review their staff members' access privileges to ensure that their access still is appropriate for their assigned duties

---

Data Custodian Responsibility

At least twice a year, the Banner DBA will send Data Custodians a printed report of all users who currently have access to some portion of their data. The Data Custodian is required to review this information, sign off, and return it to the Banner DBA.