Bethune-Cookman University
Center for Information Technology

Data Access Policy & Procedure

Overview

Bethune-Cookman University Enterprise Resource Planning, including the student information system, is cloud-hosted by its Higher Education Technology vendor, Jenzabar, and accessed via RemoteApps. Other Electronic information, such as users' shared drives with documents, emails, etc., is stored on premises for now. This networked environment also poses a significant risk to the security of information. Protecting this University resource is a shared responsibility between the Center for Information Technology (CIT) and the individual users who have access to this information. This policy covers information maintained by administrative offices of the University related to the operation of the University and accessed by members of the University community.

Network security, including firewall technology, has been upgraded to protect servers and departmental workstations from unauthorized access through the Internet. Staff and faculty in every department or school connect to secured computers through a firewall. The IP address of each administrative computer is registered in the firewall, permitting the staff user of that computer with tailored permissions linked to position/roles/duties to access needed, including the Jenzabar One system. Again, the person still needs valid Cookman Domain credentials and specific Jenzabar module functions permission to access any Jenzabar One information. Off-campus remote access through a secure Virtual Private Network (VPN to information in the Cookman domain must have the CIT approval, and be set up, complete with encryption and an additional layer of password security.

Users must physically protect their computers, including laptops, from unauthorized access and theft. All administrative information, including word processing documents, spreadsheets, databases, schedules, etc., is backed up nightly to protect information from inadvertent deletion or computer failure.

In addition to network security, a fundamental layer of protection is the logical security plan. This plan is the key to protecting administrative information and describes the procedures by which system privileges are granted, passwords are maintained, security is monitored, and issues are communicated.

Access to information is requested by the department heads or the Deans of the colleges through Human Resources. IT Access forms are used to send requests to the CIT Help Desk by HR. Then, after review by the Administrative Computing staff, appropriate permissions are granted by the System Administrator. Inquiry Access to administrative information is authorized on a 'need to know' basis. Data maintenance permission is authorized based on job responsibilities.

Employees, including student-workers with very limited permission, granted access to institutional data may do so only to conduct University operations. In this regard, employees must:

- Respect the confidentiality and privacy of individuals whose records they access

- Observe ethical restrictions that apply to the data to which they have access
- Abide by applicable laws or policies with respect to access, use, or disclosure of information

Employees, including students, may not:

- Disclose data to others, except as required by their job responsibilities
- Use data for their own personal gain, nor for the gain or profit of others
- Access data to satisfy their personal curiosity

Employees and students who violate this policy are subject to the investigative and disciplinary procedures of the University.

Definition of Administrative Information

Administrative information is any data related to the University operations, including, but not limited to, financial, personnel, student, alumni, communication, and physical resources. It includes data maintained at the departmental and office level as well as centrally, regardless of the media on which they reside. Administrative information systems utilizing current computing technology are vital to all University administrative operations, to the reliability and integrity of University records, and to the availability of comprehensive management information for planning and decision making.

At Bethune-Cookman University, the Jenzabar One system is the institution's ERP used to hold all academic and administrative information. The university recognizes the administrative information on the Jenzabar One as a vital resource requiring proper management to permit effective planning and decision-making and to operate in a timely and effective manner. Therefore, employees with access to the system are charged with safeguarding the integrity, accuracy, and confidentiality of this information as part of the condition of employment.

Access to the administrative system is granted based on the employee's need to use specific data, as defined by job duties, and subject to appropriate approval. As such, this access cannot be shared, transferred, or delegated. Failure to protect these resources may result in disciplinary measures being taken against the employee, up to and including termination.

Requests for the release of administrative information must be referred to the office of Institutional Research and the Registrar's office, along with the Office of Administrative Computing, which is responsible for administering and maintaining the databases. The University retains ownership of all administrative information created or modified by its employees as part of their job functions. Administrative information is categorized into three levels:

Confidential information requires a high level of protection due to the risk and magnitude of loss or harm that could result from disclosure, alteration, or destruction of the data. This includes information whose improper use or disclosure could adversely affect the ability of the University to accomplish its mission, as well as records about individuals requiring protection under the

Family Educational Rights and Privacy Act of 1974 (FERPA)*, and the Gramm-Leach-Bliley Act (GLBA)*.

Confidential information includes, for example, student academic records, social security numbers, and salary information.

Sensitive information requires some level of protection because its unauthorized disclosure, alteration, or destruction might cause damage to the University. It is assumed that all administrative output from the administrative database is classified as sensitive unless otherwise indicated.

Sensitive information includes, for example, class lists, facilities data, and vendor data information.

Public Information can be made generally available both within and beyond the University. It should be understood that any information that is widely disseminated within the campus community is potentially available to the public at large.

Public information includes, for example, directory information.

Security Administration

Department heads or their designees are responsible for authorizing system access to employees under their departments. System Administrators in CIT will assign that access.
The CIT Request for Access Accounts form must be completed by the Department head to authorize, modify, or remove user privileges. Security is established in discrete "levels" within a department. For example, the Admission Office may have pre-established security classes called ADM.STUDENT.EMPLOYEE, ADM.DATAENTRY, ADM.ADMISSION.OFFICER, and ADM.MANAGER. It is acceptable and desirable to place employees into the security profile that is appropriate for the job functions they will perform. Note that requesting the same access as [person x] (where person x is another employee with the same job functions within the department) is allowable. If you do not specify a particular "level" of security or "same as person x", you must provide a detailed list of the menus and mnemonics that the employee should be granted access to. Security is explicitly granted by individual menus, screens, and processes within the iSeries system.
The CIT Request for Access Accounts form can be found in the office of human resources, which is where it will be returned after being filled out or completed. After the form has been submitted, it is automatically forwarded to the System Administrators for action. Requests for account actions are usually completed within one business day. If you have any reason to follow up with additional information after submitting the form, you may send an email message to cithelpdesk@cookman.edu or call 386-481-2070.

Procedure for creation of NEW accounts:

As stated before, access to administrative systems is granted based on the employee's need to use specific data, as defined by job duties, and subject to appropriate approval. Therefore, the user requesting access to the information needs to fill out the CIT Request for Access Accounts form in the office of Human Resources. This form needs to be signed and approved by the department head and then returned to the office of Human Resources. Once access is granted, it cannot be shared, transferred, or delegated. Failure to protect these resources may result in disciplinary measures being taken against the employee, up to and including termination

Code of Responsibility for Security and Confidentiality of Records and Files

Security and confidentiality are of concern to all University employees and to all other persons who have access to administrative records. The purpose of this code is to clarify responsibilities in these areas. Each individual who has access to confidential information must adhere to the regulations stated below:

A person who has access to administrative records may not:

- Reveal the content of any record or report to anyone, except in the conduct of his or her work assignments and in accordance with University policies and procedures.
- Release information on an individual whose records are marked confidential.
- Release any information to third parties, unless it is an official part of your job duties.
- Make or allow any unauthorized use of information.
- Knowingly include false, inaccurate, or misleading entries in any report or record.
- Knowingly expunge a data record or a data entry from any record, report, or file without authorization.
- Share or post individual passwords.
- Seek personal benefit or allow others to benefit personally from the knowledge of any confidential information they have acquired through work assignments.
- Remove any official record or report, or copy of any official report, from the office where it is maintained, except in the performance of official duties.
- Update data that has been downloaded from the central databases. (unless it is an official part of your job duties)
- Make downloaded data available to those that not have authorized access.

Individuals who are given access to records and systems must agree to abide by the guidelines outlined in this document and by Bethune-Cookman University's Policy. Any knowledge of a violation of this code must be reported **immediately** to supervisors or human resources. Violations may lead to disciplinary action, including dismissal. Violations can also lead to action under the State of Florida statutes about theft, alteration of public records, or other applicable sections.

Access to the university's system is granted only to authorized individuals who agree to abide by the above Code of Responsibility for Security and Confidentiality of Records and Files.