60-6 Banner Administration, Maintenance and User Passwords

1. **Purpose.** The purpose of this policy and procedures is to define administrative and maintenance responsibilities and procedures for the Banner database at Eastern New Mexico University System (the System) and to maintain the safety, confidentiality and integrity of the System's computerized financial, personnel and student data files resident on administrative systems/servers.

2. **Policy.** The policies established in support of the purpose stated above are as follows.

   A. The System recognizes a vital and inherent need to protect the integrity and functionality of the Banner database and the data contained therein.

   B. The Information Technology Systems (ITS) personnel for the ENMU System shall be responsible for performing all routine backups, maintenance and upgrades for Banner data and program files.

   C. As part of Banner data maintenance and authority control, ITS shall have the authority to eliminate duplicate records in the production database.

   D. The access passwords for each user of Banner or its successor shall be changed at intervals of no more than ninety (90) days.

   E. The term "Banner or its successor" as used herein shall mean the ENMU System computer system on which the primary administrative application systems reside.

   F. Unauthorized use of an employee's access passwords may be considered criminal activity and treated as such. [See New Mexico Criminal Code, NMSA 1978, § 30-45-1 to-7 (1989 as amended through 2006)

The foregoing purposes and policies are implemented by the following.

Procedures

3. **Administration.** These policies and procedures are administered by ITS, with oversight by the System chief information officer (CIO).

   A. The CIO shall appoint a Banner module administrator for each computerized administrative module or subsystem.

   B. Each Banner module administrator shall be responsible for administering these policies and procedures within the administrative unit(s) for which he or she is given responsibility.

4. **Routine Maintenance, Upgrades and Backups.** The Banner server shall be closed to users periodically to allow for the backup of data and program files. Such closures shall be announced to users ahead of time. Backups shall be stored both on-site and off-site. Maintenance and minor upgrades shall be performed, if necessary, after the backup process has been completed.

5. **Major Upgrades.** ITS shall perform major upgrades to Banner as they are released after ITS personnel have reviewed the installation process and created an installation plan and schedule.

6. **Communication.** The Banner Group within ITS is responsible for communication with all campus communities concerning Banner service, maintenance and upgrades. Announcements shall be disseminated via e-mail as needed.

7. **Duplicate Banner Accounts.** As the office charged with maintaining the Banner system, ITS shall have the authority to delete any duplicate accounts in Banner.

   A. ITS shall create Banner accounts for employees after they agree to the computer use policy and complete the required account request form. If at any time more than one (1) account for the same employee exists, ITS shall determine the active account after consultation with the employee's area or department and shall disable or eliminate the duplicate(s). Under no circumstances shall an employee have duplicate Banner accounts.

   B. If a department office detects the existence of a duplicate identification number, it shall communicate the error in writing to ITS, either via memo or e-mail.

   C. If ITS identifies duplicate accounts during routine maintenance or use of the Banner database, it shall notify the employee's area or department, requesting written authorization to delete or combine the duplicates. It shall be the responsibility of a user's office to verify the accuracy of any newly combined accounts.

   D. ITS shall maintain a record of all changes regarding duplicate accounts and shall make those records available to affected users, the internal auditor, the chancellor, branch community college presidents, and/or their authorized designees.

   E. All communication concerning duplicate records shall be between the affected office and the manager of administrative computing.

8. **System Access Request by Supervisor.** The supervisor of any employee, including student employees, who requires access to the system as a condition of the employee’s job responsibilities shall request the establishment of a computer account and issuance of a password to each employee. Such request shall be made by the supervisor’s signature affixed to the Banner Administrative System Account Request form, which shall be forwarded to the ITS Help Desk

9. **Approval by Banner Module Data Custodians.** ITS will email Banner Module Data Custodians at the appropriate campus (ENMU-Roswell, ENMU-Ruidoso, etc.) for their review before access is granted to a System employee, including student employees. An annual review of Banner security access will be conducted with every Banner Module Data Custodian.

10. **Authorizations by Information Technology Services.** Upon receipt of the written request and approval outlined in sections 8 and 9 above, ITS shall:

    A. Activate a user account and establish the initial password for the employee and,

B. Upon written authorization from the Banner module administrator(s), establish components of the system to which that employee shall have access.

11. **Password Changes.** For access to Banner or its successor, ITS shall implement an online password change procedure requiring each employee to change his or her password at ninety (90)-day intervals.

12. **Other Change Requests.** Other requests for password changes must be submitted in writing (e-mail is acceptable). For purposes of verification, any such request must include the following information: login identification, employee identification number, the name of the administrative unit, module(s) to which the employee shall have access and telephone extension number. Requests shall be addressed to the ITS Helpdesk.

13. **Termination of Employee.** Supervisors of employees and work-study student employees with passwords shall notify ITS to cancel the employee's access password immediately upon an employee's termination (including resignation). The Office of Human Resources shall provide notice to ITS when employees are terminated with a termination e-mail confirmation.

14. **Transfer of Employee and Other Cancellations.** Upon transfer of an employee to another administrative unit, or upon disciplinary action or any other circumstances which warrant cancellation of an employee's authorized access to the system, the employee's supervisor shall immediately notify the appropriate Banner module administrator to cancel the employee's access password.

15. **Notice of Responsibility.** Every employee who is given an access password must assume any risk for revealing that password to another person. Supervisors shall instruct employees with access to passwords concerning the risk involved in revealing passwords to another person and strongly encourage employees to protect files by changing their passwords periodically. [See section 2. F above.]

Approved by the Board of Regents on May 12, 2006.
Amended approved by the Board of Regents, April 25, 2014.
Amendments approved by the Board of Regents on March 29, 2019