New Mexico State University
Information and Communication Technology (ICT)

Banner Application Security Standards & Procedures

(RPM - https://rpm.nmsu.edu/title-15/ and ARP - https://arp.nmsu.edu/chapter-15/)

Updated: 6/20/2018
Table of Contents

I. New User Account Creation .................................................................................................................. 4
   Standards ............................................................................................................................................... 4
   Banner User Account vs Banner ID Number ....................................................................................... 4
   Banner User Account Requests .......................................................................................................... 4
   Procedures ........................................................................................................................................... 4
   To request a new Banner User Account: .......................................................................................... 5

II. Usage .................................................................................................................................................. 5
   Federal Family Education Rights and Privacy Act .............................................................................. 5
   Confidentiality ..................................................................................................................................... 5
   Privacy ................................................................................................................................................. 6
   Educational Records ............................................................................................................................ 6
   User Agreement .................................................................................................................................. 6

III. Termed Users and Retirees ................................................................................................................. 7
   Standards ............................................................................................................................................ 7
   Procedures ........................................................................................................................................... 7
   Access Handling for Termed Users .................................................................................................... 7
   Access Handling for Retirees ............................................................................................................. 8

IV. User Account Modifications & Transfers ............................................................................................ 8
   Standards ............................................................................................................................................ 8
   Account Modifications to Access ....................................................................................................... 8
   Non-Access Account Modifications .................................................................................................. 8
   Transfers ........................................................................................................................................... 9
   Procedures .......................................................................................................................................... 9
   Account Modifications ....................................................................................................................... 9
   Transfers within the NMSU Community: .......................................................................................... 9

V. Account Expiring/Locking/Cleaning .................................................................................................... 10
   Standards ........................................................................................................................................... 10
   Inactive Accounts .............................................................................................................................. 10
   Locked Accounts ............................................................................................................................... 10
   Cleaning Locked Accounts ............................................................................................................... 10
   Procedures .......................................................................................................................................... 10
   Locked Accounts .............................................................................................................................. 10
VI. Passwords

- **Rationale**
- **Password Selection**
- **Confidentiality of Passwords**
- **Password Requirements**
- **Password Guidelines**

VII. Audit

- Standards

VIII. General

- Training
  - **Computer and Data Security**
  - **FERPA**
  - **Banner Student System**
  - **Banner Finance Procurement Training**
- Resources
I. New User Account Creation

**Standards**

**Banner User Account vs Banner ID Number**

A Banner User Account is not the same as an Aggie ID number/NMSU ID

- NMSU faculty, staff, and students are issued an Aggie ID upon admission or appointment. The Aggie ID is currently listed on the NMSU ID card and is used as a personal identifier for a person’s record in Banner.
- A Banner User Account is required in order to access the Banner INB system. Only authorized users are provided access.

**Banner User Account Requests**

All requests for Banner HR, Finance, University Account Receivable, or AiM/FMS Security access must be made using an updated vision of the Computer Systems Access form, available online at: [https://af.nmsu.edu/forms/](https://af.nmsu.edu/forms/). As the form is revised frequently, the form should be accessed online for each request, and blank copies of the form should not be stored for later use.

Request for Banner Student access must be made using the SIM Systems Access Request (SSAR web application), available online at: [https://ssar.nmsu.edu/](https://ssar.nmsu.edu/)

A Banner User Account is considered new if the user has never been issued an account, the account has been inactive, access was removed, or the user has transferred to a new department at NMSU.

In order for an account to be created, Security Admin must receive a completed form with all correct signatures. The user must be a currently appointed faculty or staff member. The user should have a current @nmsu.edu email account. Banner User Accounts will not be released until the user has officially begun employment and completed any required training modules.

⚠️ **Banner User Responsibility:** It is the responsibility of the user to keep their Banner User Account active and open. Users should successfully login to Banner at least every 90 days and notify Security Admin immediately if there are any login issues.

**Procedures**

**Before requesting a Banner User Account, the requested user should:**

1. Have an active appointment with NMSU & officially begun employment
2. Have an active myNMSU ID (*Network ID*)
3. Be issued an email address (*exceptions accepted, when applicable. For example, external auditors are assigned an Aggie ID and granted access but do not create a myNMSU email*)
4. Successfully complete the Computer and Data Security & FERPA Compliance Awareness training through the Center for Learning & Professional Development (CLPD).
To request a new Banner User Account:

1. Banner HR, Finance, University Accounts Receivable, or AiM/FMS Security access must be made using an updated revision of the Computer Systems Access form, available online at: https://af.nmsu.edu/forms/
2. The completed form is submitted to Security Admin.
3. The form is reviewed by Security Admin. Incorrect or incomplete forms are returned to the User or forwarded for authorization. Correct forms are processed.
4. The Banner User Account is created. Permissions are given as authorized on the form.
5. The user is notified by email (@nmsu.edu) when their account has been created. The email will include their username and a link to access requested system.
   - In the event that the user will not be issued a staff email account (@nmsu.edu), the project manager of the user will be emailed instead. The user password will be provided to the project manager.
   - More information on Passwords can be found in Part VI. Password of this manual.
6. Because NMSU uses AD (Active Directory) for authentication, password for Banner will be the same as the user’s myNMSU password.

II. Usage

Federal Family Education Rights and Privacy Act

FERPA protects student records. FERPA requires post-secondary education institutions and agencies to conform to fair information practice in their handling of student data. New Mexico State University System rules and regulations, and University rules and regulations govern the conduct of employees and School Officials with access to student records who act in the student’s educational interest within the limits of the employees or School Official’s need to know. To ensure compliance, NMSU requires that employees and School Officials be aware of federal law as well as System and University regulations that govern student records. NMSU’s IT Compliance Officer is responsible to ensure compliance.

Acknowledgement of this statement will be completed when the user completes the FERPA online tutorial thru CLPD. Additionally, Security Admin requires successful completion of the Computer and Data Security online class offered also offered thru CLPD. Security Admin requires successful completion of the above mentioned online classes before access will be granted.

Confidentiality

Security passwords should remain confidential. Users must lock the computer or log off any application they are using, including Banner, when they leave their computer work station.

New Mexico State University maintains the confidentiality and security of records in compliance with the Family Educational Rights and Privacy Act of 1974 (FERPA), the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA), in addition to other federal and state laws. These laws pertain to the security and privacy of personal academic, medical and financial information, along with identifying information such as Social Security Numbers.
Privacy

Notwithstanding users’ rights to privacy, and any rights under the Electronic Communication Privacy Act of 1986, FERPA HIPAA and GLBA, users grant specific permission to university to inspect users’ accounts and file space for investigation of violation of university policy or as needed for maintenance functions. When investigating a possible abuse of the system, Information and Communication Technologies has the authority to examine files, passwords, accounting information, printouts, tapes, or other material that may aid in the investigation. Investigations must follow university procedures. Use of university equipment or resources implies consent to this policy. Any questions should be directed to NMSU’s Chief Privacy Officer (CPO). NMSU IT Compliance Officer has been appointed to be NMSU’s CPO.

Educational Records

Users may access student records only as required to perform assigned duties. They may not update their own record or that of any person know to them or of a relative as this is considered an override of the University’s internal control system. Within the University, anyone whose designated responsibility requires access may use information from student records for appropriate research, education, or service functions.

User Agreement

Users must understand that accounts in Banner or any other auxiliary system are assigned to them at the request of their supervisor to be used only in connection with assigned duties as an employee of New Mexico State University and may be revoked without notice upon the request of the administrator or the Security Admin Team.

This Agreement is intended to define the responsibilities of those employees who have access to NMSU records that contain sensitive or confidential information about students, employees, donors or other individuals, and to record his or her recognition and acceptance of that responsibility.

FERPA protects student records. Mexico State University System rules and regulations, and University rules and regulations govern the conduct of employees and School Officials with access to student records who act in the student’s educational interest within the limits of the employees or School Official’s need to know.

HIPAA protects all medical records and other individually identifiable health information used or disclosed in any form, whether electronically, on paper or orally.

GLBA protects private, non-public information of individuals. Private, non-public information consists of information such as name, Social Security Number, date and location of birth, gender, credit card numbers and driver’s license numbers.

Within NMSU, employees are authorized access to University records only to the extent necessary to perform their official university duties, and are responsible for protecting such information against unauthorized access or disclosure.

The user must understand and accept the following terms and conditions:

- Passwords are the first line of security. The user agrees not to reveal their password nor allow anyone to use the account assigned to them. The user is responsible for any changes made to the database under their username.
The user must maintain the confidentiality of any and all data that they retrieve in the course of their job duties, including data they use for reporting purposes or in other software products.

Access to the records will be determined by the requirements of the user’s job, and therefore the user will only be authorized to retrieve data on a “need to know” basis.

The user will not knowingly enter false or misleading data into any record or knowingly expunge a record or data entry.

The user agrees to comply with all institutional policies on security, computer access, and confidentiality of data, data standards, and data integrity.

Any violation of these policies may lead to the immediate suspension of computer privileges. Unauthorized release of sensitive or restricted information is a breach of data security and may be cause for disciplinary action, which could include dismissal.

III. Termed Users and Retirees

Standards

NMSU Administrative Rule and Procedure (AR) 15.13 B. 6 states “Employee access to institutional data is revoked immediately upon separation”, which is compliant with data privacy regulations (FERPA, HIPAA, GLBA, FISMA, The Red Flags Rule and PCI DSS) and best information security practices. For the purposes/intent of this document, separation is defined as an employee without an active job record in Banner (NBAJOBS).

Once separation from NMSU occurs, the NMSU email account shall remain active for one year. After one year, email notifications of the impending purge shall be sent to the NMSU account. Under certain circumstances, at the direction of the Chancellor, provost, senior vice presidents, CIO, or assistant vice president for human resource services, the NMSU account shall be terminated immediately. Data associated with the purged account shall not be retained by the university.

NMSU is not responsible for data lost due to an account purge and may not be capable of recovering the data once an NMSU account has been purged.

Employee access to institutional data is revoked immediately upon separation.

Security Admin will adhere to the above mentioned policy. A report will be generated through the Cognos reporting tool, Security Admin will identify those users who have terminated or have been moved from active employee to retiree status. This report will run daily and user access will be revoked on that day. The user’s account will be locked and all access will be removed.

Procedures

Access Handling for Termed Users

1. Security Admin, on a daily basis, will run a query using the Cognos reporting tools to identify those users whose active employee status has been terminated.
2. User account identified in the Cognos report will be locked by no later than 5pm that business day.
3. Access to all NMSU systems Security Admin is tasked with maintaining will be revoked as soon as possible for those identified in the daily inactive report.
Access Handling for Retirees

It is a rule of the university that all active employees, students, and eligible NMSU retirees have an email account managed by ICT. NMSU retirees will retain their university email address with no expiration of said account. All other access will be revoked immediately.

IV. User Account Modifications & Transfers

Standards

Account Modifications to Access

Any access change to an existing Banner User Account is considered an account modification. Account modifications require the completion of a Computer Systems Access form, with all appropriate authorization for the new access being requested. Users submitting a form for modification to an existing account will be required to complete any training required of new users if they have not completed it within a year.

Non-Access Account Modifications

The university has made it possible to change your username if the following circumstances exist.

1. Your legal name has changed
2. Documented Harassment (these must be reviewed by the CIO, CPO or CISO)
3. The originally chosen username is misspelled, vulgar, suggestive, clearly objectionable, not typical in a business setting (A user can only change their username one time for this type of circumstance)

NOTE: Employees that have had access to the Banner Financial system will have financial records associated with their username and therefore will not be eligible to change their username but can request a suitable email alias be created.

New usernames must meet the following criteria:

- Be six to eight characters in length.
- Be based on your name, except for cases of harassment.

If you one of the circumstances defined above apply, you will do the following:

1. Send an email request to help@nmsu.edu from the account you want to be changed. Email must contain:
   a. Your real name
   b. Your present username
   c. Your reason for requesting the change
   d. Three suggested, unique usernames, in order of preference
2. Contact phone number
3. Call the help desk at (575) 646-1840 for instruction.

Visit the ICT Help Desk located in Room 105 of the Hardman & Jacobs Undergraduate Learning Center. Please have a valid form of ID (i.e. driver’s license, NMSU issued ID) with you when you come in.
Account administrators will contact you regarding the availability of the usernames you requested, or offer alternatives, and to schedule the change. Account renames are processed on weekdays between 8am and 5pm.

It is your responsibility to notify people and groups of your username change. Email to your old username will bounce once the change is complete. This is especially true if you are a member of any mailman mailing lists.

**Transfers**

Employees transferring to a new department are not considered modifications but new accounts. When a user is leaving a department, regardless of the reason, Security Admin will identify these and will notify the home organization/department the user is transferring from with a list of all access. The user’s account will be locked after their last day in the department. The user’s new department will need to submit a new Computer Systems Access form. Security Admin may lock the account of a transferred Banner User until a new Computer Systems Access Form is received and processed.

**Procedures**

**Account Modifications**

1. If the modification is to add/delete access to an employee who already has access within their home org, an email from the Business Manager within the org can be sent to security_admin@nmsu.edu requesting the change or the employee can complete a Computer Systems Access Form in full, available at: https://af.nmsu.edu/forms/
2. If the user has not already done so within a year, they must successfully complete the Computer and Data Security & FERPA Compliance Awareness training through the Center for Learning & Professional Development (CLPD).
3. Incorrect or incomplete forms are returned to the User or forwarded for authorization. Correct forms are processed.
4. The user’s account is modified as indicated on the form. Unless otherwise stated, permissions are added to existing access if the user retains the same title/department.
5. The user is notified by email (@nmsu.edu) when their account has been modified.

**Transfers within the NMSU Community:**

1. Security Admin will, on a daily basis, run a query to identify users transferring from their currently assigned organization to another. The department the employee is leaving can notify Security Admin of user’s departure by email to: security_admin@nmsu.edu.
2. Security Admin will lock the user’s account after the user’s last working day in the leaving department.
3. The user’s new department must complete a new Request for Computer Systems Access form in full and submitted to Security Admin using one of these methods:
   - Keep a copy for your files and forward original form to ICT-UCC at MSC 3AT
   - Fax the form to: (575) 646-2699
   - Scan and email to security_admin@nmsu.edu
4. If the user has not already done so within a year, they must successfully complete the Computer and Data Security & FERPA Compliance Awareness training through the Center for Learning & Professional Development (CLPD).
5. Incorrect/ incomplete forms are returned or forwarded for authorization. Correct forms are processed.
6. The existing access is replaced by the new access requested on the form.
7. The account will be unlocked and the password will be reset/expired if the account has not accessed in 30 days or more.
8. The user is notified by email (@nmsu.edu) when their account is unlocked and modified to fit their new department.

V. Account Expiring/Locking/Cleaning

Standards

Expiring, Locking, and Cleaning of accounts are necessary practices to ensure proper access is maintained. Users who only infrequently access Banner should take care to keep their account active by logging in on a regular basis (at least once every 90 days) and notifying the Security Admin Team promptly should there be any problems.

Inactive Accounts

Accounts are considered Inactive if there has not been a successful user login for 90 or more days. Inactive accounts are locked. Users must contact Security Admin if their account has been locked. To prevent an account from being inactive, the user should successfully login to Banner on a regular basis. Only successful logins to Banner INB (PBAN) are used to measure account activity.

Locked Accounts

An account may be locked after too many incorrect password attempts, at the end of a temp hire period, when considered inactive, or upon receipt of a Separation & Transfer notice. The reason for the lock will determine how the account can be unlocked. Accounts locked due to inactivity or too many incorrect password attempts require an email request to security_admin@nmsu.edu from the user’s email account. Accounts locked due to separation, transfer, or end of temp hire period require submission of a new, complete Computer Systems Access form to regain access.

Cleaning Locked Accounts

Accounts locked and/or expired for 90 days or more will be cleaned of access. Once cleaned, the user will need to submit a new, complete Computer Systems Access form to regain access.

⚠️ Banner User Responsibility: It is the responsibility of the user to keep their Banner User Account active and open. Users should successfully login to Banner at least every 90 days and notify Security Admin immediately if there are any login issues.

Procedures

Locked Accounts

1. Accounts can become locked after too many incorrect password attempts (3), when the account is considered inactive, at the end of a temp hire period, or after the last day of employment within the department as defined by a Separation & Transfer (PAF) notice.
2. Once locked, the user will need to notify Security Admin to regain access. This could require a password reset, an email from the department, or a new Computer Systems Access Form, depending on the reason for the lock.

3. Accounts locked for any reason for 90 or more days are cleaned of all access.

4. Once an account is cleaned, the user must submit a new complete Computer System Access Form if he or she wishes to regain access.

VI. Passwords

Rationale

Password maintenance is the most important activity a user can make in securing institutional data. Since the password is the final token used to access sensitive data, it should be guarded from inappropriate use.

Password Selection

A password should be selected in such a way that the password cannot be guessed or reverse engineered. Passwords should be selected using accepted industry standard techniques. At a minimum the password should have at least 17 characters and should not be guessable. A password should be changed every two years (730 days).

Confidentiality of Passwords

User passwords should never be shared with any other person including a supervisor (this excludes system passwords which are used by technical staff to maintain a server). Request for employees to share their password with other should be reported to the ICT Security Officer. Sharing of user passwords is prohibited.

Password Requirements

Password reset using myNMSU is programmed to synchronize passwords on all systems (temporary disabled until Banner 9)

A user password must:

- Be 17 to 64 characters in length
- Not be reused
- Contain NO spaces
- Expire every two year (730 days)
- BANNER/ORACLE users passwords cannot start with a numeral or special character
- Certain special characters may be used. However, in some applications these characters have special meaning and may cause problems. If problems are encountered, changing your password to a combination of letters and number should solve the problem. Examples of special characters are ! @ $ _,
Password Guidelines

Current password policy requires:

- The Banner User Account will be locked after 10 unsuccessful password attempts. The user will need to contact Security Admin for assistance.
- Password reset requests must be made in writing from the user’s official email address (@nmsu.edu.)
- Passwords are not sent by email. Instead, users are contacted by telephone and given the password.

VII. Audit

Standards

Regular audits are necessary to maintain appropriate access. Security Admin or NMSU IT Compliance Officer conducts many different types of audits/reviews including:

- To evaluate access controls over data
- To review audit trails related to users access controls activity
- To review for suspicion of hacking accounts activity
- To review legitimate access need and inactivate accounts with no activity in 1 year, etc.

If a user whose access has been removed or modified as a result of an audit requests to be returned to their previous level of access, they will be directed to have their supervisor send an email to security_admin@nmsu.edu including the user’s name and Aggie ID, the access the user needs, and a quick statement explaining why this access is needed. This email will then be forwarded to the Custodian who requested the user’s access be removed. It will be up to the Custodian and Security Admin to determine if access will be returned.

If a user’s account has been locked as result of an audit due to inactivity, the user will need to email security_admin@nmsu.edu to request their account be unlocked. If the account has already been cleaned of access, a new Computer Systems Access Form will be necessary.

If the user’s account has been locked as a result of an audit finding an expired employment appointment, Security Admin will verify that the employee has current active job (NBAJOBS) before unlocking the account.

Banner User Responsibility: It is the responsibility of the user to keep their Banner User Account active and open. Users should successfully login to Banner at least every 90 days and notify Security Admin immediately if there are any login issues.
VIII. General

Training

Training, both classroom-based and online, is available to assist Banner Users and University staff with understanding and using Banner. Questions concerning course content can be directed to the posted contact(s) for the course(s). Questions concerning difficulties using or logging in to the Center for Learning and Professional Development web site can contact them directly at:

New Mexico State University
Center for Learning & Professional Development
http://training.nmsu.edu/
(575) 646-7444
training@nmsu.edu

Computer and Data Security

Computer and Data Security is a Web Based training module available to all NMSU staff through the Center for Learning & Professional Development (CLPD) and participation is required before Banner Student access is granted. Registration is available at: https://training.nmsu.edu/web-based-training/ or call (575) 646-7444.

The purpose of this training is to introduce participants to the most critical threats to our computing environment and the actions individuals must take to safeguard against those threats. This interactive module also covers what is considered “responsible use” of New Mexico State computing resources, including careful protection of confidential college data. Participants will learn the following: New Mexico State University General Acceptable Use Policies, Institutional Data Security Policy, Password Maintenance Policy, and the Do and Don’ts of most common security mistakes.

FERPA

FERPA is an online training module available to all NMSU staff through the Center for Learning & Professional Development (CLPD) and required before a Banner Student access can be granted. The module can be accessed at any time, from any computer with Internet Explorer, Mozilla Firefox, and Safari access, completion takes approximately 15 minutes. Users must have an active myNMSU ID (network account) in order to login to training central.

This tutorial is designed to give you a base level of knowledge of the rules governing release of student information and to ensure that you understand your obligation for proper use and protection of student records. The completion of this tutorial is an important step in safeguarding student data and strengthening the trust of our students.

The tutorial concludes with a multiple choice assessment. In order to receive credit for completing the tutorial you must answer all assessment questions correctly.

Banner Student System

Banner 8 Student System training is recommended for Staff/Faculty who access student information, the class is Instructor-Led and available through the Center for Learning and Professional Development. You
can be register to attend at any time at: [http://training.nmsu.edu/CLPD/training-calendar.php](http://training.nmsu.edu/CLPD/training-calendar.php) from any computer with internet access, the course has a duration of 3.5 hours to complete. Users must have an active myNMSU ID (network account) in order to login to the training material. The Training will teach attendees how to use Banner Student System to look up and update student data. This course will familiarize participants with student forms that can be used to view course information on Admissions and process information such as Student Registration as well as identify common NMSU policies and procedures when working with student data.

**Banner Finance Procurement Training**

Banner Finance Procurement is a classroom-based training course available to all NMSU staff that will need access to Banner Finance. Staff must register for the course through Center for Learning & Professional Development: [http://training.nmsu.edu/CLPD/training-calendar.php](http://training.nmsu.edu/CLPD/training-calendar.php). Users must have an active myNMSU ID (network account) in order to login to Banner. Banner Finance Procurement will familiarize participants with the Banner Finance module used to create purchase requisitions and electronically receive ordered product. The training will also familiarize participants with additional Banner forms that may be used to copy, cancel, delete, and query a requisition. The course is taught in two 4 hour classes that run on consecutive days to allow for optimal retention of knowledge and skills.

This training is demonstration with hands-on practice and exercises to help develop key skills. Participants will create purchase requisitions and electronically receive an order in a training environment. If Banner is not used in the performance of their daily duties, participants should review the Banner Navigation Tutorial or Banner Navigation User Manual prior to training to receive the full benefit of the training.

**Other Training** The following training is also offered through the Center for Learning & Professional Development:

- Student Data Reporting in Cognos
- Student Data Reporting II
- Procurement Card Policies 7 Procedures
- Electronic Labor Redistribution
- Navigating PeopleAdmin 7
- Introduction to Business Reporting Using IBM Cognos
- Hiring Student Employees using the EPAF System

**Oversight, Compliance and Maintenance**

Failure to meet or exceed this standard can put university information assets at risk and may have disciplinary consequences for employees, up to and including termination of employment. Contractors and vendors who fail to adhere to this standard may face termination of their business relationships with the University. Violation of this standard may also carry the risk of civil or criminal penalties. NMSU IT Compliance Officer is responsible to oversee and to ensure compliance with this standard. This manual will be updated annually by IT Compliance Officer and Banner Security Administrator.
Resources

- NMSU Acceptable Use Rule: https://arp.nmsu.edu/15-11/
- General NMSU Information and Communication Technologies Policies and Administrative Rules:
  - ARP - https://arp.nmsu.edu/chapter-15/
  - RPM - https://rpm.nmsu.edu/title-15/
- NMSU Non-Disclosure Agreement: https://www.nmsu.edu/legal/nondisc.html
- NMSU Account Password Requirements https://arp.nmsu.edu/15-51/