Montgomery College
Office of
Information
Technology

IT Standard
BANNER DESKTOP DATA ACCESS AND SECURITY MANAGEMENT

Standard: IT11004
Original Effective Date: 04/27/2012
Last Revised: 05/31/2015

Last Reviewed: 04/30/2020
Next Scheduled Review Date: 04/01/2021
Version No.: 2.1
Administrative Owner: Information Security and Privacy Director

PURPOSE

It is the policy of Montgomery College ("College") to protect and promote secured access to its academic and administrative data. The Ellucian Banner system is the College's primary source for enterprise resource planning (ERP) data.

The purpose of this document is to provide the minimum standard by which access to College Internet Native Banner (INB) Desktop System data is granted and managed. Access to College academic and administrative data is restricted to the minimum level of access required to perform a College approved function.

SCOPE

This Standard applies to Montgomery College personnel who are responsible for governing, creating, monitoring, limiting or managing access to the Montgomery College INB Banner Desktop System data.

DEFINITIONS

Term	Definition
Banner Data Trustee ("Data Trustee")	College administrative or academic personnel ultimately responsible for Banner data related to the academic or administrative function for which they are responsible. Banner data may or may not be directly related to a single Banner ERP module.
Banner Desktop Data Access (Banner Access)	Access to the Banner application data though the Internet Native Banner application installed on desktop workstations collegewide.
Banner Functional Leads	College business unit analyst representative of the business functions supported by Banner enterprise information. Banner Functional Leads are selected by Administrative Banner Data Trustees.
Banner Navigation Training	Online training modules provided by the College Center for Professional and Organizational Development (CPOD) office focusing on basic Banner operational use.
Banner User Account ("Banner User")	Access to the Banner system is issued in the following manner: Generic Account: A user account that does not identify a specific/unique person or process such as guest or admin. Individual Account: A user account that identifies a specific/unique person or process. Privileged Account: A user account with additional or special access to a system or application such as the ability to make configuration

	changes, perform maintenance, modify security, or perform other critical system or application tasks.
Confidential Information	Defined by College Policy 31103 as: Confidential information includes but is not limited to the following: the personnel record of any past or present employee; any record containing personally identifying information; student information which has not been identified as directory information; records or material that have been otherwise identified as confidential, subject to trademark or a copyright protection or for which there is a contractual limitation on disclosure; and information the disclosure of which outside the College violates a confidential relationship in the College's decision-making process or which disclosure is intended to prematurely influence the College's decision-making process, or which reveals confidential information or which unnecessarily invades personal privacy or impairs individual rights.
FERPA Training	The Family Educational Rights and Privacy Act (FERPA) is Federal law developed to protect the privacy of student records. College policy relative to FERPA regulations is detailed in Montgomery College Policy 41003, Student Cumulative Records. This training is required by the College Admissions and Enrollment Management Office and available through CPOD as a prerequisite to accessing College student records.

STANDARD

A. General

1. All individuals working on behalf of the College to grant and maintain access privileges to Banner system data have the responsibility to comply with existing Federal, State, and local laws and regulations, College Policies and Procedures, and IT Standards in order to protect College data and computer technology resources.
2. Banner Functional Leads shall act as the designees for Banner Data Trustees for granting access, as well as determining the level of access granted. The following Banner Data Trustee areas of responsibility are represented by Banner Functional Leads: Student (credit and non-credit), Finance, Accounts Receivable, Human Resources, Institutional Advancement, and Financial Aid.
3. The Office of Information Technology (OIT) will audit compliance to this standard.

B. Banner Application Access Privilege Management

1. Access to Banner data through Banner Desktop Data Access is restricted to active College employees or as necessary, contractors, vendors, or temporary employees serving on behalf of or assigned to a College unit. Non-employees of the College that require access to Banner data through Banner Desktop Data Access must have their access sponsored by a College Banner Data Trustee or their designee.
2. Banner access privileges shall be governed by a Banner System and Data Warehouse Account Request Process, which will consistently grant access with involvement of all the stakeholders, including OIT, the College Unit manager or supervisor responsible for the person requesting new or changed access, and the Banner Functional Lead as designee of the Data Trustee. Access privileges assigned to a Banner User must represent the minimum level of access required to perform the job function associated with the Banner User.

3. Banner Access is granted only after the completion of online Banner Navigation Training and if applicable online FERPA Training.
4. Banner Access is granted only after the Banner User agrees in writing to the requirements stated in the Notice to Information Systems and Data Users during the Banner System and Data Warehouse Account Request Process.
5. College unit managers and supervisors are responsible for monitoring the access privileges of their direct report employees and contractors. The managers and supervisors are responsible for ensuring that the above referenced minimum level of access is maintained during the course of the employee's job assignment and that if the Banner User's access needs change, a new request for access will be commenced.
6. OIT consulting with Banner Functional Leads serving as designees of their respective Data Trustees will review positions changes identified each month by the Office of Human Resources, Development and Engagement (OHRDE) and adjust Banner access accordingly.
7. Banner Functional Leads, serving as designees of their respective Data Trustees, will periodically review a list of all Banner Users with access to their area of responsibility. The review will correct any access inconsistencies, including but not limited to unneeded access, overbroad access, locked, and terminated access. The Banner Functional Lead review will be supported by the Office of Information Technology (OIT) as necessary.
8. Upon request of a Data Trustee, any or all Banner Users with current access privileges may be asked to undergo a review of the current privileges with the possibility of reapplication.
9. Access privileges to Confidential Information should be assigned when possible to the data element level.
10. Banner User access to College sensitive or Confidential Information during testing and training tasks will be subject to the same protection as production data including but not limited to least privilege.
11. Temporary Banner User access is only allowed for a reasonably defined period of time, specifically defined purpose, and upon full documentation and approval by the appropriate Banner Functional Lead.

C. Banner Application Access Termination

1. Banner User Accounts must be locked when they are no longer required or have met their expiration date. This includes but is not limited to the following employment changes: employee placed on administrative leave, employee termination, or employee job responsibility change (current level of required access is no longer required). New Banner User Accounts privileges should be initiated where applicable.

D. Banner Application and System Controls

1. Banner User Accounts must lock after at a maximum of five invalid authentication attempts. The Banner User Account should remain locked for a period of 15 minutes or until unlocked by the responsible system administrator.
2. Banner User Account sessions must timeout after a period of inactivity equal to at most 65 minutes.

E. Banner Data Warehouse

1. Access to Banner data resident in the Banner Data Warehouse is subject to the same standards and processes that apply to Banner Desktop Data Access.

EXCEPTIONS

This standard is applicable as of its Effective Date. Exceptions to this standard will be considered on a case-by-case basis in accordance with the IT Standard Exception Request Form or as approved in writing by the IT Privacy and Cybersecurity Compliance Director.

COMPLIANCE AND RECOURSE FOR NON-COMPLIANCE

Montgomery College has established College Policies/Procedures and the OIT has established IT Standards and Processes and associated guiding documents to provide appropriate protection of technology resources, to assure protection of personally identifiable and sensitive information and to promote privacy. Any faculty, staff, contractor, or vendor found to have violated any part of College Policies, Procedures or IT Standards or Processes may be subject to disciplinary action and/or legal action.

RELATED DOCUMENTS

- Montgomery College Policy 66001, Acceptable Use of Technology
- Montgomery College Policy 31103, Confidentiality: Employee Use, Release and Disclosure of Information
- Montgomery College Policy 41003, Student Cumulative Records
- Montgomery College Policy 66002, Confidential Data Management and Security
- IT08001 Information Technology Resource Authentication
- IT11001 IT Access Management Standard
- IT11002 Remote Access Standard
- IT Standard Exception Request Form
- Banner System and Data Warehouse Account Request Process
- Notice to Information Systems and Data Users

WEB SITE ADDRESS FOR THIS STANDARD

APPROVALS / REVISION HISTORY

DATE	VERSION / REVISION / NOTES	APPROVER
April 27, 2012	Original roll-out of this Banner Access document.	Patrick Feehan, Information Security and Privacy Director/ITPA
May 31, 2015	Revised. (Version 2.0)	Patrick Feehan, Information Security and Privacy Director/ITPA
September 30, 2020	Decided upon and added review cycle dates. (Version 2.1)	Nell Feldman / Keith Wilson