Banner Systems Access & Security Policy

Bridgewater State University
131 Summer Street
Bridgewater, MA
02325

Version:	**1.4**
Date:	**September 2, 2014**

Table of Contents

Policy Revision History

It is important that this *Banner System Access and Security Policy* accurately reflect the current situation and business requirements at BSU. Updates must be provided to the BSU Information Technology team for review and inclusion in the policy.

The following table describes the history of this document.

Version	Date Issued	Reason for Update
1.0	June 21, 2012	Draft
1.1	June 29, 2012	Incorporated Admin Systems review feedback.
1.2	July 9, 2012	Incorporated Pat Cronin's review feedback.
1.3	August 15, 2012	Removed definitions section.

1. About This Security Policy

1.1. Purpose and Scope of This Policy

Administrative data captured and maintained at Bridgewater State University are a valuable university resource. While these data may reside in different database management systems and on different machines, these data in aggregate form one logical university resource. The Banner system contains data from multiple operational areas that need to be integrated in order to support institutional research, business analysis, reporting, and decision making.

The purpose of this *Banner System Access and Security Policy* is to ensure the security, confidentiality, and appropriate use of all Banner data which is processed, stored, maintained, or transmitted on Bridgewater State University or personal computer systems and networks. This includes protection from unauthorized modification, destruction, or disclosure, whether intentional or accidental.

This policy is intended to serve as a general overview on the topic and may be supplemented by other specific policies required by law such as the *Health Insurance Portability and Accountability Act* (HIPAA), the *Family Educational Rights and Privacy Act* (FERPA), *Massachusetts 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth*, and the *Gramm Leach Bliley Act*.

The *Banner System Access and Security Policy* applies to all individuals who have access to the Bridgewater State University Banner system, including but not limited to all Bridgewater State University employees and students, who may or may not have been granted access to sensitive data during the normal course of their employment with BSU.

This policy applies not only to stored Banner information but also to the use of the various computerized systems and computerized programs used to generate or access Banner data**,** the computers which run those programs including workstations/devices to which the data has been downloaded, and the monitors and printed documents that display data.

1.2. Updating This Policy

This policy must be kept up-to-date.

It is the responsibility of the BSU Information Technology team to ensure that procedures are in place to keep this policy up-to-date. If, while using this policy, you find any information which is incorrect, missing, or if you have a problem in understanding any part of this policy please inform the BSU Information Technology team so that it may be corrected.

1.3. Distribution & Communication

The BSU Information Technology team is responsible for distributing and communicating this policy. This policy is available in electronic form on the Information Technology Policies and Procedures web page and will be distributed via email to all new and existing Bridgewater State University personnel who have Banner access.

It is important that everyone familiarizes themselves with this policy and understands his or her role(s)/responsibilities and adheres to this policy.

2. Data Administration

By law and University policy, certain data is confidential and may not be released without proper authorization. Users must adhere to any applicable federal and state laws as well as Bridgewater State University policies and procedures concerning storage, retention, use, release, and destruction of data.

All Bridgewater State University Banner data, whether maintained in the central database or captured by other data systems, including personal computers, remains the property of Bridgewater State University and is covered by all Bridgewater State University data policies. Access to and use of data should be approved only for legitimate Bridgewater State University business.

Division/department heads are responsible for ensuring a secure office environment regarding all Banner data. Division/department heads will review the Banner data access needs of their staff as it pertains to their job functions before requesting access via the *Administrative Systems Access Authorization Form*.

Banner data (regardless of how collected or maintained) will only be shared among those employees who have demonstrated a job related "need to know". Although Bridgewater State University must protect the security and confidentiality of data, the policies allowing access to data must not unduly interfere with the conduct of Bridgewater State University business.

Additionally, users with access to Banner data must adhere to provisions as set forth in the following policies:

1. *Responsible Use of Information Technology Policy*
2. *Computer Database Access and Security Policy*
3. *Confidential Data Usage Policy*
4. *Data Responsibility Policy*
5. *Secure Remote Access Policy*
6. *Password Complexity Policy*
7. *Electronic Mail Policy*

3. Access to Banner Data

Below are the requirements and limitations for all Bridgewater State University divisions/departments to follow in obtaining permission for access to Banner data.

Division/department heads must request access authorization for each user under their supervision by completing and submitting a *Administrative Systems Access Authorization Form* whether the request is for a new or existing user.

The Information Technology Security Manager or his/her delegate, will review the request and approve or deny. Approved requests will be forwarded to the Banner Security Administrator for processing.

All Banner Access Authorization requests, whether approved or denied, will be presented to, and reviewed with, the Banner Steering and Review Committees as a means of allowing all interested parties fair opportunity to weigh in on access granted/denied to Banner data.

If the request is denied, the user may follow the appeals procedure described below.

Under no circumstances will access be granted without approval of the Information Technology Security Manager, or his/her delegate, or as a result of the appeals procedure.

If a user is denied access to Banner data an appeal may be made by written request to the Banner Steering Committee. The request must include:

1. A description of the specific data access requested.

2. Explanation why access was denied.

The Banner Steering Committee will review all denied access requests and supporting information and decide if access should be granted or denied. Any decision of the Banner Steering Committee is final.

4. Secured Access to Banner Data

Banner security classifications will be established based on job function. Specific capabilities will be assigned to each security classification. Each user will be assigned a security classification. Some users may be assigned several security classifications depending on specific needs identified by their division/department head and approved by Information Technology Security Manager.

The use of generic accounts is prohibited for any use that could contain protected data.

Users who are granted access to one or more Banner security classifications will establish Banner access as follows:

1. Access to Internet Native Banner (INB) and Self Service Banner (SSB) will only be available via the Bridgewater State University's web portal.

2. Access to INB or SSB from off-campus requires the use of the Cisco VPN (Virtual Private Network) client which requires separate approval via the *Secure Remote Access Policy* and associated *Remote Access Authorization Form*.

5. Banner Access Authorization Process

This section defines the process which must be followed to gain access to Banner data once a Banner user account has been created and is ready to be granted initial or additional access to Banner data.

1. Obtain and fill out *Administrative Systems Access Authorization Form*.

2. Submit completed form for review –

   Hard Copy – Send to Security Manager, Room #009, Boyden Hall.

   Electronic – Email to itsupport and refer to as Banner Access Request.

   NOTE: If you need assistance completing the form please submit a request to the Banner email address and someone will contact you and assist accordingly.

3. IT Security Manager approves or denies Banner Access request.

4. If approved, Banner Security Administrator grants access.

5. If denied, requestor appeals decision to Banner Steering Committee.

6. Reference Information

This section contains references to other documents that are relevant to the *Banner System Access and Security Policy* and with which participants to the policy should be familiar.

The reference documentation includes:

Administrative Systems Access Authorization Form

Secure Remote Access Policy

Remote Access Authorization Form