UNIVERSITY OF Southampton

Report

Title: Banner Internet Native Banner (INB) Access Statement

From: Anne-Marie Drummond
Academic Registrar, Student and Academic Administration

Date: 30 April 2014

1. Introduction

1.1 Purpose and Scope

Administrative data captured and maintained at the University of Southampton 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 Student Record 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 Internet Native Banner (INB) System Access Statement* is to ensure the security, confidentiality and appropriate use of all Banner data which is processed, stored, maintained, or transmitted on University of Southampton computer systems and networks. This includes protection from unauthorised modification, destruction, or disclosure, whether intentional or accidental. This statement is intended to serve as a general overview on the topic and may be supplemented by other specific policies of the University and those as required by law such as the *Data Protection Act and Freedom of Information Act*.

The Banner (INB) System Access Statement applies to all individuals who have access to University of Southampton computer systems and networks in order to have access to Banner INB for administrative purposes. This includes, but is not limited to, all University of Southampton employees and students, who may or may not have been granted access to sensitive data during the normal course of their employment with University of Southampton including trained employees of Southampton, and recognised members of the permanent staff of the University Students Union (SUSU). It applies not only to stored information but also to the use of the various computerised systems and computerised programs used to generate or access data, the computers which run those programs including workstations to which the data has been downloaded, and the monitors and printed documents that display data. Access to Self Service Banner through Student Self Service or Faculty Self Service is excluded.

1.2 Definitions

Banner Data – Any data that resides on, is transmitted to, or extracted from any Banner system, including databases or database tables/views, file systems and directories, and forms.

Student Systems Board (SSB) – A University Board with membership representative of Banner system areas. This Board provides oversight for the entire Banner system and other student related systems including, Syllabus Plus, E-Assignment, Oracle CRM, POAS, POMBS and other local system developments for which there is agreed University support

Banner System – Student, Banner Document Management System (BDMS formerly known as Xtender (BXS)), and any other interfaces to these systems relating to the student workstream.

2. Data Administration

By law and University policy, certain data is confidential and may not be released without proper authorisation. Users must adhere to any policies and procedures of the University of Southampton concerning storage, retention, use, release, and destruction of data.

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

The Director of SAA is responsible for ensuring a secure office environment regarding all Banner data.

3. Access to Banner Data

Below are the requirements and limitations for all University of Southampton staff to follow in obtaining permission for access to Banner data for administrative purposes within the SAA Workstream.

The Director of SAA or delegated Authorising Officer responsibility as indicated in Table One

Table One: Banner INB Authorising Officers

Section or Service	Authorising Officer	Alternate Authorising Officer
SAA	Head of Student Systems and Operations	Faculty Academic Registrar (FAR)/ Hub Manager
Student Services	Service Delivery Managers	Service Delivery Managers
iSolutions	ICT Operations Manager (Steve Head)	Head of Student Systems and Operations
Finance	Assistant Director of Finance (Mary White)	Head of Student Systems and Operations
Students Union (SUSU)	Head of Student Systems and Operations	SAA Student Records Manager (Liv Stobseth-Brown)
International Office	Head of Student Systems and Operations	SAA Student Records Manager (Liv Stobseth-Brown)
Library	Head of Student Systems and Operations	SAA Student Records Manager (Liv Stobseth-Brown)
Other Professional Service	Head of Student Systems and Operations	SAA Student Records Manager (Liv Stobseth-Brown)

All authorising officers as indicated above will review the Banner data access needs of their staff as it pertains to their job functions before requesting access. Any staff outside the workstream will be given access at the discretion of the Director of SAA or their nominee.

All authorising officers must request access authorisation for each user under their supervision by completing and submitting a *Banner Training Form:*
http://www.soton.ac.uk/isolutions/computing/training/tutorled/banner/index.php

Access to the Banner (INB) Student Records System will be granted for hub/faculty/professional service access through the iSolutions IT Training & Development team only. Following the training session, the appropriate access in connection with the training will be granted by iSolutions ServiceLine. **By authorising the training, authorising officers are authorising access to the Banner (INB) Student Records System.** Additional access for members of the SAA Hub will be granted through training and operational requirements and authorised through the Director or Assistant Director of SAA.

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 University of Southampton must protect the security and confidentiality of data, the policies allowing access to data must not unduly interfere with the conduct of University of Southampton business.

Students should never normally be allowed to attend training or have any sort of access to Banner even if they have a dual role as a member of staff. Exceptions may be granted for short term activities where students are employed for specific purposes and managed in a single location (e.g. Visa check in, clearing/enrolment hotline). Students granted access to Banner must be made fully aware of the implications of the Data Protection Act in relation to accessing other students' information and students should never be given access to update assessment or award records.

In the event that a member of staff who is also a student should apply for training, the FAR or member of Professional Service should raise the issue with the Assistant Director of SAA (Head of Student Systems and Operations) in the first instance and the appropriate SAA Hub Team Manager(s). Each case will be reviewed in the light of the individual circumstances.

4. Withdrawal of Banner Access

When staff either leave the workstream or the University, Banner access will be withdrawn. It is the responsibility of the line manager of the staff or the appropriate Authorising Officer to ensure that the form SEC 05 Removal of Access Form is completed as part of the leaving process.

This form should be signed by the Director SAA, or delegated to an Authorising Officer (Table 1), and sent to ServiceLine for the access to be withdrawn.

5. Secured Access to 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 line 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 classification will establish Banner access as follows:

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

2. Access to INB from off-campus requires the use of VPN (Virtual Private Network) client or Terminal Services.

Anne-Marie Drummond

Direct tel: +44 (0)23 80593799