Lingnan University

Banner System Access, Data Classification and Security Policy

Document Classification: Internal	Document Owner: Information Security Officer	Publication Date: 12 October 2018

Revision History

Version	Prepared By	Approved By	Date	Revision
1.0	Jeff McDonell, ITSC		18 Nov 2008	Initial version.
1.1	ITSC		Nov 2013	
1.2	ITSC	TLISMB	12 Oct 2018	- Updated 7(b), 7(d) and 7(e) of the Section “Banner Access Guidelines” - Revised the wordings “Banner Security Administrator (ITSC, DSS Team)” and “Banner Security Administration (ITSC, DSS Team)” to “Banner Security Administrator (ITSC)”

Banner System Access, Data Classification and Security Policy

Purpose

This policy document established measures for the protection, access, and use of the Lingnan University's Banner administrative data and information. It also outlines the responsibilities of all who access and manage the Banner data.

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 the University computer systems and networks. This includes protection from unauthorised modification, destruction, or disclosure, whether intentional or accidental.

Scope

The Banner System Access and Security Policy applies to all individuals who have access to the University computer systems and networks, including but not limited to all University employees and students, who may or may not have been granted access to sensitive data during the normal course of their employment with the University. It applies not only to stored information but also to the use of the various computerised systems and 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.

Data Management Roles and Responsibilities

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.

Banner System – This includes the modules, namely Student, Human Resources, Finance, Payroll, Alumni; and any other interfaces to these systems, such as the Infosilem TPHi Timetabling and home-grown applications.

Data Owners –Data Owners are responsible for determining who should have access to data within their jurisdiction, and what those access privileges should be. Responsibilities for implementing security measures may be delegated, though accountability remains with the owner of the module/data.

Area of Responsibility

Module	Data Owner(s)

Student System	Registrar/Director of Administration and Registry Services (UGC-funded Programmes);
	Programme Directors (Taught Postgraduate Programmes);
	Director (Community College / Life)

Banner forms that begin with the letter "S" (except for SR and SA forms which are Recruit/Admissions), as well as most of the forms that begin with the letter "G". Examples are SPAIDEN, SFAREGQ, SFASLST, SGASTDN, GOAEMAL.	
Finance System	Comptroller
Banner forms that begin with the letter "F" - like FPAREQN.	
Human Resources System	HR Director
Banner forms that begin with the letters "P" or "N" - like PHATIME, or NBIJLST. Banner forms that begin with the letter "G", like GZAPINR.	
Payroll	Comptroller
Banner forms that begin with the letters "P" or "N" - like PHATIME, or NBIJLST.	
Alumni	Director of OIAAA
Banner forms that begin with the letter "A" - like APASBIO.	

Data Managers - Data Managers oversee data management functions related to the capture, maintenance and dissemination of data for a particular operational area. They are responsible for the general administration of user access to data within their area(s) of responsibility. Data Managers are appointed by the respective Data Owner.

Area of Responsibility

Module	Data Manager(s)

Student System	Team Leaders in Registry;
	Associate Director of Student Services Centre;
	Associate Programme Directors (Taught Postgraduate Programmes);
	Associate Directors (Community College/LIFE)

Finance System	Associate Comptroller
Finance System - Research Projects	Project Invigilator
Human Resources System	Associate Director
Payroll	Associate Comptroller
Alumni	OIAAA Officer

Data Administration

Under University policy, certain data is confidential and may not be released without proper authorisation. Users must adhere to the applicable Personal Data Ordinance as well as the University policies and procedures re storage, retention, use, release, and destruction of data.

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

Department/Programme/Unit heads are responsible for ensuring a secure office environment regarding all Banner data. Department/Programme/Unit heads will review the Banner data access needs of their staff as it pertains to their job functions before requesting access via the *Banner Account Request 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. The University must protect the security and confidentiality of data, the policies allowing access to data must not unduly interfere with the conduct of the University business.

Access to Banner Data

Below are the requirements and limitations for all departments/programmes/units to follow in obtaining permission for access to Banner data.

Department/Programme/Unit heads must request access authorisation for each user (staff member) under their supervision by completing and submitting a *Banner Account Request Form*. Those who request new accounts are required to submit a Confidential Pledge in addition to the *Banner Account Request Form*.

The appropriate Data Manager(s) will review the request and approve or deny. Approved requests will be forwarded to the Banner Security Administrator (ITSC) for processing. Under no circumstances will access be granted without approval of the appropriate Data Manager(s).

The *Banner Account Request Form* is to be completed for all Banner access changes, including requests for new user accounts, change to access under existing accounts, and account termination.

When a user changes departments or job positions, the account privileges associated with the old department or job position must be deleted and new account privileges associated with the new department or job requested. The account privileges deletion and new account privileges requests may be submitted on the same form, if applicable.

For new accounts and changes to existing accounts, portions of the form must be completed by each of the following: the individual (user) who is requesting access to Banner systems, the user’s supervisor and/or department head (or designated representative), the Data Owner(s) of the request module, and the Banner Security Administrator (ITSC).

For account terminations, the supervisor and/or department head should complete and forward the form to the Banner Security Administrator (ITSC).

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 department/programme/unit head and approved by the Data Manager(s).

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…

a) Access to Internet Native Banner (INB) and Self Service Banner (SSB) will only be available via the Lingnan University's web portal (Luminis).
b) Off-campus access to INB requires the use of the VPN (Virtual Private Network) client.

Data Security

All data and information systems owned by the University shall be produced and maintained to assure that:

a) accuracy and completeness of data are maintained during processing and storage;
b) system capabilities can be reestablished within an appropriate time upon loss or damage by accident, malfunction, breach of security, or natural disaster.
c) attempted or actual breaches of security can be detected promptly, reported and controlled.

Email
It is also the responsibility of the data users to take adequate steps to protect and dispose of properly all personal data that they include in, or attach to, any email to be sent on a network. Employees are requested to note that more than a copy of the data may be established after the first transmission of the email containing such data; (e.g. a copy of the email may reside in the transmitting email server computer and another copy may remain in the receiving server). Also emails encrypted using certain methods (e.g. S/MIME) are only protected during transmission but may be read by any person having access to the sender's or the recipient's computer. All UPD users should implement practices with respect to the proper destruction of emails and attachments to emails that contain personal data. Examples of good practices include:

(i) always use the Lingnan University Campus Email to avoid sending sensitive data over public Internet email that may result in a copy being stored or archived by a third-party server
(ii)password protect the data file using tools such as Word, Excel, Acrobat, etc. when it is necessary to send sensitive data using email. The password should be sent via a separate email message or different mean.

Data Storage on Computer Devices
Sensitive data should be stored on a secure network drive instead of a mobile device to prevent data leakage in case of losing the device. Sensitive data should be encrypted before transferred into removable media or via email. UPD users can consult ITSC on the most updated encryption software. Encrypted USB storage device may be used for additional level of protection. Proper

security should be enabled to prevent the loss or theft of a computer, mobile device or USB storage device. Virus scanning is important to prevent data leakage. Files downloaded from the Internet, email attachments or external storage devices should be scanned for virus before opened or saved on a computer.

Data Protection

Module/Data Owners and Data Managers shall ensure secure office environments with respect to data and any automated systems used to process data. Data Owners and Data Managers shall validate the access requirements of their respective staff, according to job functions, before access is provided. Data Owners and Data Managers shall terminate access immediately the departure of staff or suspected breach of trust.

Data Accuracy

All users of data have the right to expect that this data is accurate. Staff entering data are therefore responsible for providing accurate information to the best of their ability. Each user of the administrative information is assigned appropriate combinations of inquiry only and rights of access to update specific parts of the administrative information system.

Banner Access Guidelines

1) BANNER data is the property of Lingnan University. Access to BANNER data is restricted to authorised personnel only. Unauthorised access is prohibited.

2) BANNER data will be used for official University business only. Specific non-University business use of BANNER data may be authorised under other official University policy. Unless specifically permitted by another official University policy, the use of BANNER data for personal gain or curiosity, or another's personal gain or curiosity, is prohibited.

3) Persons, and processes, accessing BANNER data will uphold the confidentiality and privacy of individuals whose data they access and observe any laws, regulatory requirements, policies and ethical restrictions that may apply with respect to their accessing, using or disclosing such information. The university considers any breach of data security to be a serious offence and any such breach is subject to the Hong Kong Personal Data (Privacy) Ordinance.

4) Persons, and processes, with access to BANNER data, regardless of its form (electronic or print), will insure that all reasonable and prudent measures are taken to protect the data from theft and unauthorised or accidental viewing, copying, downloading, modification or destruction. The data must be protected while in use, in transit and in storage. Information Technology Services Centre (ITSC) should be notified immediately in the event the security of any BANNER or other administrative data is compromised.

5) Anyone in the service of the University, with a genuine business or educational need, may be authorised to access the BANNER data necessary to perform their duties. An individual's access to BANNER data will be removed when the individual leaves the service of the University or during an extended absence.

6) BANNER Data Owners have the sole authority to authorise access to the data within the modules they administer.

7) For various security reasons…
   a) there must be a segregation of management functions between BANNER module Data owner and Banner System Administrators;
   b) user access privileges should be reviewed annually to ensure compatibility with the job description;
   c) the use of generic accounts is prohibited for any use that could contain protected data;
   d) audit logs recording user activities, exceptions, and information security events should be produced and kept for a period that aligns with the Information Security Policy of the University to assist in future investigations and access control monitoring;
   e) users accounts will need to meet the complexity of password rules specified in the Information Security Policy of the University.

Reporting Violations:

Any suspected violations of these policies, or unauthorised access to computing resources, or any other condition which could compromise the security of BANNER data or other University computing resources must be reported to the ITSC, the Registry or Human Resources Office.

Banner Account Request Form

Please read through the procedure in the overleaf before hand in the request form

To: ITSC-DSS Team Manager (MB203)
Via Internal Mail

Implementation Date
(Filled by ITSC DSS Team): ____________________

Cc: Department Head

Our reference
(Filled by ITSC DSS Team): ____________________

Part A : Request Details (To be completed by the requestor)

* Name of the Requestor :

* Department :

* Title :

* Requested Date :

Banner Account Name (if any): ____________________

* Signature : ____________________

* Signature : ____________________

*^ Endorsed by Data Manager : ____________________

*Name of the Department Head: ____________________

*^ Name of the Data Manager : ____________________

Action:

□ New Account

□ Terminate Account (please provide the Banner Account Name:________________)

□ Modify Current Account/Access (please provide the Banner Account Name:________________)

* Brief description on the Banner Account request :

Part B : Banner Account Request Details (To be completed by the requestor)

Module (Please select as applicable)

□ Alumni (add / delete) **

□ Admission (add / delete) **

□ Examination (add / delete) **

□ Faculty (add / delete) **

□ Finance (add / delete) **

□ HR (add / delete) **

□ Payroll (add / delete) **

□ Student Records (add / delete) **

□ Web for Advisors (add / delete) **

□ Others (Please specify) ________________

* Effective Date: ______________(dd/mm/yyyy)

Part C: To be completed by ITSC, DSS Team Manager

□ The above request is approved.

□ The above request is not approved due to ________________________________

* Mandatory fields

** Delete where appropriate

^ Data Manager – The person(s) who oversee data management functions related to the capture, maintenance and dissemination of data for particular operational area.