

LOGICAL ACCESS QUICK REFERENCE GUIDE

(For Process Owners, Academic Security Officers and ITS Product Managers)

The following reference guide is a summary description of the Logical Access procedures. Please review the Logical Access Policies and Procedures for complete details. Logical Access Forms and Guides can be located at http://www.slu.edu/services/HR/university_security_forms.html.

<u>Procedure and Timing</u>	<u>Key Controls</u>	<u>Forms/Reports/Tools</u>	<u>Responsible Party (Note 1)</u>
Granting and Changing User Access (As Needed):			
1. Complete an Access Security Request Form.	LA 1 through LA 4	Access Security Request Form Security Request Form How-To Instructions	Business Process Owner or Authorized Approver
2. Perform an evaluation of the segregation of duties (appropriateness of access rights in relation to other access rights in place or to be provided). By approving the Form, the requestor attests that access rights and segregation of duties is appropriate.	LA 5, LA 6	Access Security Request Form Service Level Review Guide	Business Process Owner or Authorized Approver
3. Approve Access Security Request Form and submit to appropriate Security Officer.	LA 3	Access Security Request Form Listing of Authorized Approvers	Business Process Owner or Authorized Approver
4. Review Access Security Request Form for completeness and proper approval. Establish Remedy ticket for the access request and attach Access Security Request Form to the Remedy ticket. Access request is distributed to applicable ITS Product Managers through Remedy.	LA 1 through LA 6	Access Security Request Form Guide For Security Officers for Remedy Requests	Security Officer.
5. Review Remedy tasks for completeness of request. Set up or change access rights. Close appropriate tasks in Remedy ticket. Notify Security Officer that access has been granted or changed.	LA 1 through LA 6	Remedy Ticket	ITS Product Manager
6. Security Officer notifies Business Process Owner that access rights have been granted. Business Process Owner confirms that access rights are in accordance with request and notifies User.	LA 4	Email	Security Officer Business Process Owner
Terminating User Access (As Needed):			
1. Complete and approve Access Security Request Form and submit to Security Officer.	LA 10	Access Security Request Form	Business Process Owner or Authorized Approver
2. Review Access Security Request Form for completeness and proper approval. Establish Remedy ticket for the access removal and attach Access Security	LA 10	Access Security Request Form	Security Officer

LOGICAL ACCESS QUICK REFERENCE GUIDE

(For Process Owners, Academic Security Officers and ITS Product Managers)

Request Form to the Remedy ticket. Access removal request is distributed to applicable ITS Product Managers through Remedy.		Guide For Security Officers for Remedy Requests	
3. Review Remedy tasks for completeness of request. Disable access rights. Close appropriate tasks in Remedy ticket. Notify Security Officer that access has been removed.	LA 10	Remedy Ticket	ITS Product Manager
7. Security Officer notifies Business Process Owner that access rights have been removed.	LA 10	Email	Security Officer
Service Access Report and Account Inactivity Review (Bi-Annual):			
1. Obtain Service Access Report and Account Inactivity Report. Review appropriateness of user access rights.	LA 11	>Service Access Report >Account Inactivity Report >Service Level Review Guide	Security Officer Business Process Owner ITS Management
2. Document review of the Reports. Forward confirmation of review (Monitoring Review Form) to the QA Administrator.	LA 11	Monitoring Review Form	Security Officer Business Process Owner ITS Management
3. If changes or termination of access is needed, follow procedures as noted above in Granting and Changing User Access or Terminating User Access.			
Termination and Position Change Report Review (Weekly):			
1. Obtain Termination and Position Change Report. Review appropriateness of user access rights with assistance from Business Process Owners where need.	LA 10, LA 11	>Termination Report >Position Change Report >Service Level Review Guide	Security Officer Business Process Owners ITS Management
2. Document review of the Termination and Position Change Reports. Forward confirmation of review (Monitoring Review Form) to the QA Administrator.	LA 10, LA 11	Monitoring Review Form	Security Officer Business Process Owner ITS Management
3. If changes or termination of access is needed, follow procedures as noted above in Granting and Changing User Access or Terminating User Access.			

Business Process Owners (BPO) or Authorized Approvers –The Authorized Approvers or Process Owners may be Department Supervisors, Business Managers, Hiring Managers, Vice Presidents, Sponsors (in the case of guests, contractors), IT Management (for IT personnel) or others as designated by policy.

Academic Security Officer (ASO) – Individual within an academic unit assigned the role of ensuring the security of information which users have access and that user access is properly administered and controlled.

ITS Management – For purposes of this procedure, ITS Management refers to IT Administrators and other key ITS personnel that are in management/supervisory roles of ITS units (i.e., IT Administrators for TLRC, Enterprise Resources, Academic Technologies, Business Intelligence, etc).

ITS Product Managers – ITS personnel responsible for physically granting access to the various applications or databases, such as Banner INB, Banner Self Service, WebFOCUS, Xtender, Axiom, Workflow, Oracle.