



SAINT LOUIS
UNIVERSITY

Information Technology Services Logical Access Procedure

Prepared by: Jefferson Wells

Saint Louis University Logical Access Procedure

Table of Contents

I.	Introduction	3
II.	Policy	3
III.	Purpose	3
IV.	Scope	3
V.	Roles, Responsibilities and Definitions.....	4
VI.	Logical Access Flowchart – General Access.....	6
VII.	User Account Set Up.....	7
	A. Initial Account Setup.....	7
	B. Magis Identity Management System and Password Security.....	7
	C. Automatic Account Lockout.....	8
VIII.	Restricted Application Access.....	8
	A. Eligibility for Access.....	8
	B. Formal Request for Access.....	8
	C. Segregation of Duties.....	9
	D. Access Request Types.....	10
	E. Standard Access.....	10
	• Access to Multiple Academic Units' Data	11
	• ITS Access	12
	• Access Appeal Process	13
	• Performance Standard	13
	F. New Implementation.....	13
	G. Emergency Access	14
IX.	Changes to User Access.....	14
	A. Changes to Duties	14
	• User Remains in Same Department	14
	• User Transfers to Another Department	14
	B. System Class/Group Change	15
X.	Access Termination Procedures	15
	A. User Resignations/Terminations.....	16
	• ITS and Human Resource Notification	16
	• Removal of Access and Account Verification	16
	• Removing Access to Multiple Academic Units' Data	17
	• Removing IT User Access	18
	B. Emergency Terminations.....	18
	C. Lock Accounts	19
XI.	Document Retention.....	19
XII.	Monitoring.....	19
	A. Service Access and Account Inactivity Reports.....	19
	B. Position Change Reports.....	20
	C. Termination Reports.....	21
	D. Documentation of Monitoring	22
XIII.	Network Operating System Logging.....	22
	Appendices	23 - 26

Saint Louis University Logical Access Procedure

I. INTRODUCTION

The overall goal of logical access is enforce and track the level of access to computer resources, preserving both data integrity and data confidentiality. Several 'General Computer Controls' for application security are essential to achieve this goal and they are:

- the use of a unique userid for each computer user
- a strong password
- proper authorization to access computer resources
- the monitoring of userids, passwords and logical access

II. POLICY

It is the policy of Saint Louis University's Information Technology Services (ITS) department to provide all employees with system access to information resources consistent with business needs. The ITS department's function will provide a mechanism for authenticated and secure access to the University's information systems resources.

III. PURPOSE

The purpose of this documented process is to outline the procedure in which user access accounts are created, changed, terminated, and monitored within the Saint Louis University primary application architecture. The goal of the logical access process is to ensure standardization across all information technology systems and ensure the appropriate data owners are contacted, informed and approve each user access request. All user access requests must be documented using procedures outlined in this process. Implementation of this procedure minimizes unauthorized access to proprietary information and technology.

This procedure will be followed to request and approve access to University applications, create user accounts including passwords, and provide ongoing maintenance of user accounts.

IV. SCOPE

This policy applies to Banner (INB and Self Service) and its associated integrated systems (WebFOCUS, Xtender, Axiom, Workflow), Magis IDMS and underlying databases.

This policy applies to students and permanent, temporary, and part-time faculty and staff, contractors, consultants, guests, and all other authorized users of any electronic communication system, including all personnel affiliated with third parties, at Saint Louis University. This policy also applies to all equipment that is owned or leased.

In addition, this procedure will be utilized for user level and developer access accounts. A user account is defined as an account which does not have the permission to install, maintain, or alter in a material way any network, application, service or workstation resource. Developer access accounts are defined as accounts which can modify, configure and install software and/or hardware for an application. Developers can typically create new features and processes within an application and update and/or access data outside the standard application interface.

Saint Louis University Logical Access Procedure

V. ROLES, RESPONSIBILITIES AND DEFINITIONS

Role	Responsibility
User	<ul style="list-style-type: none"> • Has access to or requests access to projects, programs or application data via the Process Owner or Authorized Approver.
Business Process Owner (BPO) Also, may be referred to as Data Process Owner, Business Manager or Authorized Approver	<ul style="list-style-type: none"> • Approves access for users to specific projects, programs or application data. • Provides guidance to ITS relative to user access levels. • Identifies and provides required verifications for designated approvers and ensure these persons comprehend the significance of their role in granting access to the University's Information Systems.
Academic Security Officer (ASO) <i>(See Appendix 1)</i>	<ul style="list-style-type: none"> • Ensures the security of information which users have access and that user access is properly administered and controlled. • Responsibility to report any potential or actual risks or incidents affecting the security of information. • Monitors compliance with University information security policies and procedures, making recommendations for improved security and for monitoring the occurrence of security incidents.
Quality Assurance (QA) Administrator	<ul style="list-style-type: none"> • Monitors and reviews overall logical access management process. • Ensure continued compliance with University information security policies and procedures; ensure logical access processes remain frozen. • Reviews logical access and user account reconciliation reports. • Provides impartial 3rd party input for user access request denial appeal process.
University ITS (Product Managers) <i>(See Appendix 2)</i>	<ul style="list-style-type: none"> • Reviews user settings and establishes proper domain access based on requests from Academic Security Officers. • Creates user account and log in password.

Definitions

- ***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.
- ***Access Form*** – Abbreviated name of Access Security Request Form
- ***Business Process Owners (BPO) or Authorized Approvers*** – Certain person(s) of authority within a faculty/department/unit who have been identified to University ITS as having the power to approve both user access to University applications and specifically what processes that user is allowed access. The Process Owners or Authorized

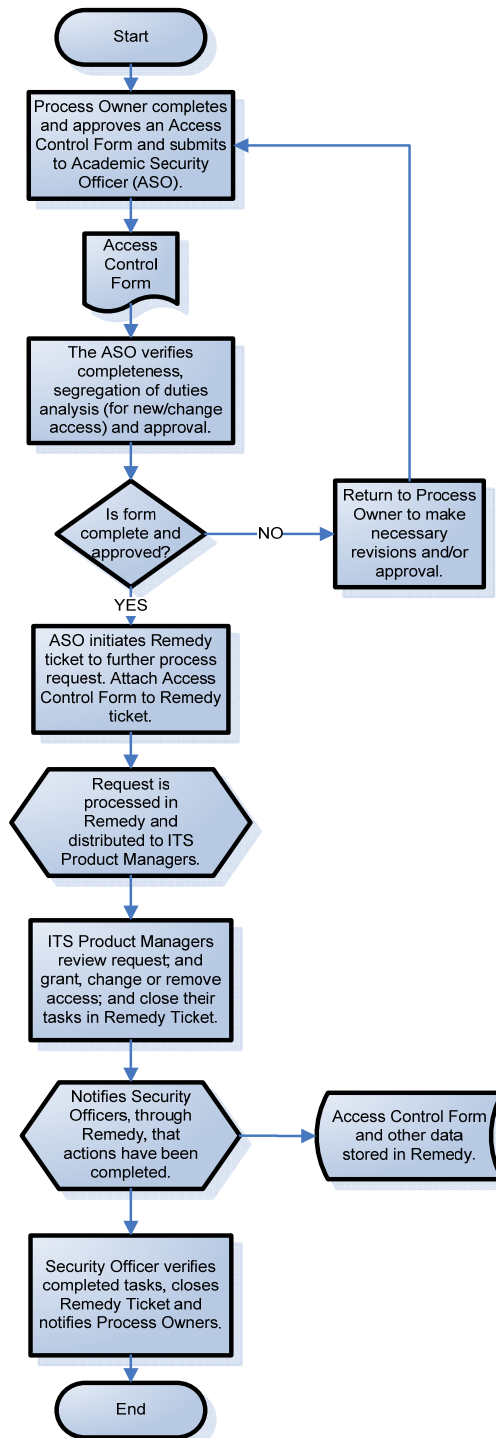
Saint Louis University Logical Access Procedure

Approvers may be Business Managers, Department Supervisors, Hiring Managers, Vice Presidents, Sponsors (in the case of guests, contractors), IT Administrators or others as designated by policy.

- **Information Security Officer** – Monitors overall compliance with University information security policies and procedures, making recommendations for improved security and for monitoring the occurrence of security incidents.
- **ITS** – Acronym for Saint Louis University, Information Technology Services.
- **ITS Management** – For purposes of this procedure, ITS Management refers to IT Administrators and other key ITS personnel 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.
- **LAN** – A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link. Typically, connected devices share the resources of a single processor or server within a small geographic area (for example, within an office building).
- **Magis Identity Management System** – A service which allows users to provide their username and password once to a trusted service and to have their identity securely, consistently and seamlessly provided to many web applications. Integrated Sign-On acronym is ISO.
- **QA** – Quality Assurance
- **Remedy** – Remedy is SLU's primary problem/request tracking system. It allows SLU ITS to track information as well as internal and external requests placed upon the organization. The information tracks various Remedy applications such as the Asset Management, Service Level Agreements, Change Request, Logical Access requests and Help Desk applications.
- **Remote Access** – An encrypted channel or method is required for private access to internal computer applications and systems.
- **SLU** – Acronym for Saint Louis University
- **University Information Systems** – Includes systems and equipment (workstations, servers, printers, telephones, switches, routers, wiring, hubs, wireless and cellular components, personal digital assistants (PDAs), and other devices and software components that access the University network) and software (applications, databases, ERS).
- **User, Username or SLUNet ID** – Refers to any person accessing the University network, including, but not limited to, students, faculty, staff, contractors, clients, consultants, invited guests, and others working at the University.
- **User Account** – The user identification, logon/login identification, or other system-specific means granted to a user permitting access to the University network.
- **Wireless Access** – Terminal access to the university network using wireless technology or technology that accesses the network without the use of hard wires or cables.

Saint Louis University Logical Access Procedure

VI. LOGICAL ACCESS FLOWCHART – GENERAL ACCESS



Saint Louis University Logical Access Procedure

VII. USER ACCOUNT SETUP

A. Initial Account Setup

In order to gain access to University computer applications and infrastructure, one must have a Banner SLU netID as established by Human Resources or in accordance with ITS Guest Account Policy and Procedures.

B. Magis Identity Management System and Password Security

The University uses Magis Identity Management System (IDMS) to provide a single source of sign-on for enterprise applications. All members of the University with SLU access will use Magis IDMS. Individual web applications using Magis IDMS for authentication may only be accessible to key personnel depending upon the nature of the application and user requirements. The Magis IDMS service provides several benefits:

- The same username and password allows access to all approved services
- The user provides their password to one trusted application
- The username and password only has to be validated once per session
- Username and passwords are treated securely

For Magis IDMS and Oracle (including those applications that validate through Magis IDMS and Oracle), the username assigned to a unique user name and password will be established in accordance to the following user password and security model structure:

- Passwords must be a minimum of 8 characters in length;
- Passwords must not be the same as the login account;
- Temporary passwords must be changed after initial log in;
- Passwords must be constructed using at least one of each of the following 3 character types:
 - uppercase alpha (A, B, C, D, E, etc.)
 - lowercase alpha (A, b, c, d, e, etc.)
 - numbers (0, 1, 2, 3, 4, 5, 6, 7, 8, 9)
 - Note: **Special characters are not allowed.**
- Passwords will expire every 180 days and users will be required to change their password upon this expiration. ITS will run a quarterly report to monitor user account inactivity.
- Passwords must not be easily guessed; must not be names, dictionary words, phone numbers, or birthdays;
- Passwords must be different from the previous 12 passwords.
- Passwords must be stored in encrypted format to prevent tampering.
- Access of privileged users who perform administrative tasks must be restricted and properly approved.

If a particular University system does not validate through Magis IDMS or Oracle, or does not support the minimum structure and complexity detailed in the aforementioned guidelines, University ITS must ensure that one of the following procedures be manually implemented:

- The password assigned must be adequately complex to insure that it is not easily guessed and the complexity of the chosen alternative must be defined and documented.
- The legacy system must be upgraded to support the requirements of this procedure as soon as administratively possible.

Saint Louis University Logical Access Procedure

- All applications should be isolated from the main university networks or relocated to a system that supports the foregoing security password structure.

Initial and temporary user account passwords that are systemically generated will be communicated to the BPO via a secured method per best business practices. It is the BPO's responsibility to ensure appropriate user application training and facilitating the initial password change process. The BPO should specifically instruct the user on the password change/use policy, in addition to directing them to the location of all University policies and procedures.

C. Automatic Account Lockout

ITS will enable the automatic lockout capabilities to ensure that all SLUNET IDs are temporarily suspended or locked out after three consecutive unsuccessful login attempts.

VIII. RESTRICTED APPLICATION ACCESS

In order to enforce security of sensitive and confidential data and data networks, a number of SLU business applications have restricted access. It is important to ensure that users have access only to the areas required to perform their functions at the University. The process of requesting, monitoring and modifying access to key applications, Banner financial information and Human Resources applications involves having proper eligibility for access, proper segregation of duties analysis, formal request for access, account verification and follow proper documentation retention standards.

The remaining sections describe procedures for requesting, changing and deleting user access to key applications, including Banner financial information and Human Resource applications.

A. Eligibility for Access

Individuals (faculty, staff, student, or other) may obtain access if appropriate approval(s) from the Business Process Owner (BPO) is obtained. Additionally, for access to most Financial, Human Resources and Student applications, completion of a designated training course may be required.

In order to obtain access, the individual must be an active employee and have an active Banner account record in the Human Resources database and an active email account or comply with the ITS Guest Account Policy and Procedures (see [User Account Setup](#)). The BPO for each user request must confirm appropriate eligibility before approving the request for access.

It is imperative that the BPO (or other personnel responsible for the hiring process within a department/academic unit), ensure that the necessary documentation is submitted to Human Resources so that the Banner SLUNet ID can be established in a timely manner. The BPO should verify that the Banner SLUNet ID is established before submitting a request for user access to University systems as discussed below.

B. Formal Request for Access

After an employee's eligibility is confirmed, an *Access Security Request Form* (hereafter referred to as Access Form) should be completed by the BPO. **The BPO should generally submit the Access Security Request Form at least two days prior to the users first day at work.** At a minimum, the following information should be contained and completed on the Access Security Request Form:

- User's full name; SLUNET ID (username), and Banner ID

Saint Louis University Logical Access Procedure

- User's telephone number (If Assigned)
- Job title and/or contractor name
- Employment status (e.g., Employee, Contractor)
- Employment (contractor/project) start and end dates
- Department Name and Number
- Type of Request (new user, change to existing access, delete user, developer)
- Systems to be accessed, including classes, forms, etc. (If necessary, include additional attachments to the Access Form)
- Type(s) of access requested (e.g., read, write, delete, change or execute)
- Other information as necessary to identify level/type of access requested (e.g., user, power user, administrator, developer)
- Segregation of Duties analysis
- Approval signature of the BPO (***See Appendix 3 for required approval levels***).

(Note: The "start" date on the Access Form should be included as a means to ensure access is established upon the users expected start date. The "end" date should be completed, particularly for all guests/contractors, temporary personnel and non-university users when a termination date is known or stipulated. ***The ASOs and ITS is strongly encouraged to monitor this "end" date to ensure timely removal of user access***).

The Access Form has sections for data belonging to each of the following Academic units:

- Advancement
- Business & Finance
- Human Resources
- Student
- Student Financial Services

The BPO should select the access to the data required for its users' job functions. The form is located at the following:

http://www.slu.edu/services/HR/university_security_forms.html

C. Segregation of Duties

The BPO should determine the specific functions and responsibilities for which the individual needs access, specifically access to key Financial and Human Resources applications. The BPO must perform a segregation of duties review.

Segregation of duties prevents a single person from performing two or more incompatible functions. Failure to segregate incompatible duties, or to implement compensating controls when such separation of duties is not possible, increases the risk that errors or unauthorized actions may occur and not be detected in a timely manner.

Some examples of incompatible duties include users having systems access enabling them to:

- Perform billings/invoicing, receive the corresponding payments, and record the corresponding cash receipts entries.
- Authorize disbursements, issue corresponding disbursements, and record corresponding disbursements entries.
- Set up a new employee, input pay rates/salary, and issue pay checks.

Some special aspects of segregation of duties apply to IT functions themselves. There should be segregation between systems development and operations, operations and data control, and data base administration and system development.

Saint Louis University Logical Access Procedure

Access can be restricted to specific functions within some applications. For example, a user may be given access to prepare requisitions, but not to approve requisitions. In addition, a user may be given one of the following levels of access to some applications:

- Modify (read/write) access: the ability to enter and update data and submit transactions or
- Query (read-only) access: the ability only to view information without being able to enter or change data.

The Access Form includes a statement noting that the access rights being granted are appropriate for the user's job functions and that segregation of duties has been considered. By signing/approving the Access Form, the BPO is noting that the appropriateness of the access rights and segregation of duties has been evaluated and the access is justified. As necessary, the BPO should provide any additional comments regarding the access rights and the appropriateness of the access rights to the user's job functions.

In those instances where duties cannot be fully segregated, mitigating or compensating controls must be established and documented with the Access Form, or access rights to be granted should be adjusted. Mitigating or compensating controls are additional procedures designed to reduce the risk of errors or irregularities.

D. Access Request Types

Access granted will fall into one of the following categories:

- Standard Access – A general new or change request
- Emergency – A requirement of immediate access or change that does not follow the standard access procedure, where access may need to be granted without before Access Form can be initiated.
- New Implementation – Provides for new implementation of a product, service or function that affects multiple users. Generally the same access rights are being granted to the user group.

These access scenarios are further discussed below.

E. Standard Access

The BPO will submit the approved Access Form to the appropriate Academic Security Officer (ASO). The ASO should review the Access Form to ensure all applicable details are completed. The ASO should also ensure the Form is properly approved by an authorized BPO. **(See Appendix 3 for required minimum approval levels)**

Incomplete or denied requests will be returned to the approver of the form, requesting complete details before the request will be fulfilled and/or noting why the requests is denied. Denied requests should be properly documented and retained (i.e., email communication is stored with copy of denied Access Form).

Once a properly completed Access Form is received, the ASO will initiate a Remedy Change Request Ticket to input the request for access. **(Note: Security Officers should review the Power Point Slide Presentation, "Remedy Management System for Logical Access")**. Within Remedy, tasks will be created to distribute the request to the appropriate ITS Groups and to establish other tasks necessary for granting and documenting access. The approved Access

Saint Louis University Logical Access Procedure

Form and any other applicable documents will be included in the Remedy Ticket. The submission of the Remedy Ticket will serve as documentation of the ASO's review and approval.

The ITS Product Manager(s) (within each ITS Group) will review the request, ensure completeness and verify an approved Access Form is included in the Remedy Ticket and that the Remedy Ticket was generated by an authorized ASO. If the ITS Product Manager has any concerns regarding the legitimacy of the request, the ITS Product Manager must verify the request with the appropriate ASO and/or BPO, as necessary.

Once the request has been properly verified, user access may be granted. The ASO and ITS Product Manager should pay close attention to the user "start date" noted on the Access Form. This date is intended to note the date access should be available to the user. The ASO and ITS Product Manager should ensure that the user's access is available by this date.

The ITS Product Managers will grant the appropriate access and close the appropriate tasks within the Remedy Ticket. The ASO should review the Remedy Ticket to verify that all tasks have been completed. The ASO should generate a user access profile from the WebFOCUS Dashboard (Logical Access Super Report) to verify that the access granted is in accordance with the request. The user access profile should be attached to the Remedy Ticket.

Note: The ASO may grant access to additional modules (i.e., funds/organizations) within the scope of the ASO's authority. The Banner Finance, fund security, is a unique additional access rights. There are two circumstances that require addition of a new or existing fund to a user's access. In the first scenario, a new fund is established in Business & Finance whereby there must be a Financial Manager or an existing fund is assigned to a Financial Manager. As these funds are established by the ASO of Business & Finance, submission of an Access Form is not warranted. In the second scenario, the user in Business & Finance needs access to a fund of another department. This requires the submission of an Access Form.

The ASO may also perform additional tasks as identified in the Remedy Ticket. The ASO will notify the BPO that the access request has been completed and confirm that the access rights are as requested. The ASO may choose to provide the BPO with a copy of the user access profile to confirm the access granted. Confirmation received from the BPO should be attached to the Remedy Ticket. The ASO will perform final closeout of the Remedy Ticket.

If it is determined, *after* the initial Remedy ticket to set up access has been closed, that the user should have additional access rights, the BPO should submit a separate Access Form to request these additional access rights. It will be treated as a new request and not as an extension of the original request. Therefore, it is imperative that the BPO review and properly confirm the initial access rights to the ASO.

Access to Multiple Academic Units' Data

In some instances, a user's job function may require the user have access rights to data of several Academic Units. In this instance, the BPO should complete the appropriate sections on the Access Form for each Academic Units data. A copy of the Access Controls Form should be submitted to the respective ASOs. Each ASO will process the request through Remedy in the same manner as other requests.

Example 1: A user employed in Human Resources needs access to data in Human Resources and Finance. The BPO in Human Resources will complete the appropriate sections on the Access Form for Human Resources and Business & Finance. A copy of the Form would be submitted to the Human Resource and Finance ASO.

Saint Louis University Logical Access Procedure

Example 2: A user employed in Mission & Ministry needs access to data in Human Resources, Business & Finance, and Students. The BPO in Mission & Ministry will complete the appropriate sections on the Access Form for Human Resources, Business & Finance, and Students. A copy of the Form would be submitted to the ASOs in Human Resource, Business & Finance, and Students.

ITS Access - ITS Staff

The user's direct supervisor (IT Product Manager or IT Administrator) serves as the "requestor" and is responsible for preparing and submitting an *ITS Access Security Request Form* for access requests. The Form applies to Banner and companion products, their underlying databases and servers, (including, but not limited to: WebFOCUS, Xtender, Axiom, Workflow, ODS and EDW). The direct supervisor (requestor) prepares the form and routes to the appropriate section "IT Administrator" for approvals and implementation, depending on the type of access, as follows:

- OS Level Access to a Host or Network Drive
- Direct Database Access
- Application Access

After the appropriate IT Administrator approvals, the user's IT Administrator will approve the Form and submit to the Enterprise Resource Administrator for secondary approval. After all approvals have been received, the requestor will initiate the Remedy ticket, attach the Form, and route tasks to the respective ITS Administrator or ITS Product Managers, who will complete the tasks to grant the user access and provide a reply in the Remedy ticket to the requestor. (**Note: IT Administrators and Product Managers should review the Power Point Slide Presentation, "Remedy Management System for Logical Access".**) Specific tasks should be initiated to grant access to IT staff.

The form is located at the following:

http://www.slu.edu/services/HR/university_security_forms.html

Example 1: There is a new hire (or additional access needs) for a staff position reporting to the WebFOCUS ITS Product Manager. The WebFOCUS ITS Product Manager will prepare the form (requestor) and route to the IT Administrator for each section requiring access (OS access, Direct Database and/or Application access). The form will then be routed to the ITS Administrator – Business Intelligence, for approval and to the Enterprise Resources Administrator for secondary approval. After all approvals, the WebFOCUS ITS Product Manager will initiate a Remedy ticket to grant/request the appropriate access rights.

Example 2: There is a new hire (or additional access needs) for the position Banner INB ITS Product Manager. The IT Administrator – Applied Administrative Technology (AAT), will prepare the form (requestor) and approve as the IT Administrator for Applications Access. If OS access or Direct Database access is needed, the form will be routed to those IT Administrators for approvals. The IT Administrator – AAT then approves the form and submits to the Enterprise Resources Administrator for secondary approval. After all approvals, the IT Administrator – AAT will initiate a Remedy ticket to grant/request the appropriate access rights.

Example 3: There is a new hire (or additional access) needs for the position IT Administrator (AAT, Business Intelligence, Infrastructure Services, or SSDD). The Enterprise Resources Administrator will prepare and approve the Form and submit to the

Saint Louis University Logical Access Procedure

Chief Information Officer for secondary approval. The Enterprise Resources Administrator will initiate the Remedy tickets.

Access Appeals Process

The requester's Department Head (or designee) and the Data Owner (or designee) should discuss the request to determine if they can agree to a resolution (i.e., both agree to grant or deny access). If a mutual agreement is not reached, the access request details should be submitted to the QA Administrator for review. The QA Administrator, acting as an impartial 3rd party, will consult with both the requester's Department Head and the Data Owner. A final resolution and decision will be determined by these three. This resolution should be documented and retained with the original access request.

Performance Standard

For those complete access requests received by the ASO on or after the day the user has began work, access should be granted within 48 hours of receipt of the complete request by the ASO. This includes a 24 hour turnaround for the ASO and a 24 hour turnaround for ITS. **Note:** New hire access requests (or change requests for transferring employees) that are submitted in a timely manner (at least 2 days prior to the users' first day of work in the department) should be processed by the users' first day at work.

F. New Implementation

There may be instances where systems access will be required for a large group of people needing the same access rights. (Example: Self-service EPAF rollout to all business units or the implementation of a new Xtender application in a particular business unit). In these situations, preparing a user access form for each user request may be counter productive.

The BPO or ASO should complete an Access Form to document the access to be provided and include the proper approval. User information may not be filled out directly on the form due to multiple users included in the request. However, the BPO will need to clearly note on the form that this is a mass access request and include/attach the following documentation:

- Brief explanation of the nature of the access request
- Any additional documentation regarding the access rights to be granted
- A report or listing of all users, containing the user information that would generally be noted on the Access Form (i.e., name, SLU NETID, Department, etc) or a listing of the organizational units to be affected (discuss with ITS the best manner to communicate affected users).

It is imperative that the BPO or ASO considers segregation of duties for each user in the group request. The ASO should ensure a thorough review of the request and must clearly note in Remedy that this includes a report of users. This process is general and may not address specific aspects of all new implementations. However, BPO and ASO should ensure documentation of the following key items:

- Appropriate approval
- Clear description of the affected users

In some situations, a department may hire a large group of people who are starting on the same day (Example: Student workers at the beginning of a semester). If these users will need the same access rights, the use of "new implementation" may be warranted. Submitting group access requests should only be done in rare or extreme situations.

Saint Louis University Logical Access Procedure

G. Emergency Access

Situations may arise where immediate access rights are required. In these instances, a member of University management may find it necessary to temporarily by-pass preparation of the Access Form and verbally communicate (or email) the need for access to the ASO or ITS Product Manager (i.e., an employee or consultant is asked to start immediately and needs access rights to begin project).

To ensure the emergency is properly documented, reviewed and eventually approved, the ASO or ITS Product Manager would initiate the Remedy ticket and select "Emergency". The preparer of the ticket would include an appropriate task to ensure an approved Access Form is obtained and included in Remedy.

Note: The absence of the primary ASO does not automatically warrant the use of the Emergency Access process. The BPO should refer to the designated ASO Backup (**See Appendix 1**).

IX. CHANGES TO USER ACCESS

Periodically, changes to user access become necessary. Changes to user access may be determined by the BPO or ITS Management during the normal course of business (i.e., determine that a user needs additional access rights to perform his/her job functions) or as part of periodic security access reviews. (See [Monitoring](#) Section below).

Changes to user access will fall into one of the following categories:

- Change of duties – Normal access changes resulting from a change in a user's duties. User changes position within department or transfers to another department requiring change in access rights.
- System Class/Group Change – Changes to a class or group – not individual.

These Change scenarios are further discussed below.

A. Change of Duties

User Remains in the Same Academic Unit/Department (Example: A user in Business & Finance changes position from Accounting Clerk to Accounting Manager):

Overall, the changes to user access will follow the same process as that for the initial granting of user access, including the completion and submission of an Access Form. The BPO should determine the specific functions and responsibilities for which the individual needs access and whether the specific functions and responsibilities that the user will have access to after the change will be appropriate. The BPO must perform a segregation of duties review. The BPO should identify on the Access Form the access rights to be granted and/or removed. The Access Form will be submitted, processed in Remedy and documentation retained in the same manner as that for Restricted Application Access.

User Transfers to another Academic Unit/Department (Example: A user in Business & Finance changes position and moves to Human Resources):

The BPO of the former department should submit an Access Form to its ASO in advance of the transfer. This will allow the ASO of the former department to coordinate efforts with the ASO and/or BPO of the new department. Since the user is not leaving the University, the ASO should

Saint Louis University Logical Access Procedure

ensure that the request is NOT submitted as a “termination or resignation” as this would indicate the removal of all access to the University systems. The goal is to remove access rights related to the former department and establish access rights for the new department, in a seamless manner to prevent gaps in access capabilities and reduce loss of productivity. The ASOs of the former and new department should discuss the following:

- Position change dates (last day in former department and first day in new department)
- Ensure that the BPO of the new department initiates the access request process in a timely manner for any new access rights required.
- Identify common access rights between the former and new position, whereby the access rights do not have to be removed. (Utilize the access profile on the WebFOCUS Dashboard – Logical Access Super Report, to evaluate current access rights).

B. System Class/Group Change

A System Class/Group Change is similar to a New Implementation as discussed in the [Restricted Application Access – New Implementation](#) section above, in that it affects a large group of people needing the same access rights. In this situation, new “forms” are added to already existing “classes”. Unlike other access requests that are initiated by the BPO, this process is initiated by the ASO.

The ASO should complete an Access Form to document the access class/group change to be performed and include the proper approval. The general user information section will not apply. The ASO will need to clearly note on the form that this is a system/group access request and include or attach the following documentation:

- Brief explanation of the nature of the class/group change
- Any additional documentation regarding the access rights to be granted
- A report or listing of all users, containing the user information that would generally be noted on the Access Form (i.e., name, SLU NETID, Department, etc) or a listing of the organizational units to affected (discuss with ITS the best manner to communicate affected users).

X. ACCESS TERMINATION PROCEDURES

When a relationship is discontinued between a person and the University, the ITS department must revoke that user’s access to services and it may be necessary to reallocate ITS resources used by that person. Exactly how that deletion and reallocation occur, however, depends on the circumstances under which the person is leaving.

When deleting user accounts, both the BPO, ASOs and ITS should remember that user terminations:

- Should not be categorized as a standard change.
- Requires determination of why someone is leaving. That answer will help determine both the category and priority of the change.
- Requires a risk assessment to identify any threat to the organization. (This may be formal or informal).
- Requires an evaluation of the user’s role and responsibilities, and a plan for transitioning those to other users identified, if such a transfer is required.
- Should not be done until all dependencies on the account have been removed. Accounts should be disabled when the user leaves, and deleted later.

Saint Louis University Logical Access Procedure

- Requires that access to all accounts a departing user might have—such as Active Directory, line of business applications, and other directory services—must be disabled and eventually deleted.

Changes to user access will fall into one of the following categories:

- Resignation/Termination – Defined as follows:
 - Resignation - A voluntary separation by the user, such as a retirement, or taking another job outside the University. The BPO will probably want to maintain user access and privileges until the person's departure. To be processed under normal circumstances.
 - Termination – A non-voluntary separation by a user, such as a firing, forced resignation, layoff, or work project ends. While time is of the essence for access removal, the circumstances warrant that the BPO still submit an Access Form through the standard process.
- Emergency Termination – Similar to a Termination, but with a requirement of immediate access removal. The primary difference being the circumstances surrounding the termination or the nature of the user access rights, warrant the need to immediately communicate (verbally or email) the access removal directly to ITS, rather than initiating an Access Form.
- Lock Account – An emergency suspension of access rights, until appropriate authorization of access rights is confirmed

These Access Removal scenarios are further discussed below.

A. User Resignations/Termination

ITS and Human Resources Notification

Unless circumstances prevent advance notice or justify deferred notice, the BPO should initiate the access removal process at least two days prior to the user last day. This includes contractor, temporary personnel and non-university employee access termination. Initiation begins with the submittal of the Access Form.

The BPO should also give advance notification to Human Resources that the user is leaving the University. This will ensure that users, whose access rights have not been removed, are recorded to the Termination Report , as discussed below in Monitoring – Termination Reports.

The BPO will prepare an Access Form and send to the ASO requesting removal. The BPO should clearly note the reason for the access removal (i.e., termination, resignation). The BPO should clearly note the date that access is to be removed (i.e., specific date or immediately). The ASO should ensure that this date is input into the tasks within the Remedy ticket. Also, if necessary, the BPO should indicate any temporary restrictions to be placed on the user's access rights until final removal.

Removal Of Access and Account Verification

The ASO will initiate a Remedy Change Request Ticket to input the request. Within Remedy, tasks will be created to distribute the request to the appropriate ITS Groups and to establish other tasks necessary for granting and documenting access. The approved Access Form and any other

Saint Louis University Logical Access Procedure

applicable documents will be included in the Remedy Ticket. The submission of the Remedy Ticket will serve as documentation of the ASO's review.

The ITS Product Manager(s) (within each ITS Group) will review the request and ensure completeness. The ITS Product Managers will disable the user account immediately upon receipt of the request and place into a "null" account status. The ITS Product Manager should close the appropriate tasks within the Remedy Ticket. The user account should be fully deleted within 30 days.

By placing the account in "null" status, ITS Product Managers, ASOs and BPOs have the opportunity to complete an evaluation of the user's roles and responsibilities, determine whether account responsibilities need to be reassigned to another user, and evaluate the disposition of the user's files.

The ASO should review the Remedy Ticket to verify that all tasks have been completed. The ASO should generate a user access profile from the WebFOCUS Dashboard to verify that the access has been disabled in accordance with the request. The user access profile should be attached to the Remedy Ticket.

The ASO will notify the BPO that the access removal request has been completed. The ASO may choose to provide the BPO with a copy of the user access profile to confirm the access removal. Confirmation received from the BPO should be attached to the Remedy Ticket. The ASO will perform final closeout of the Remedy Ticket.

The BPO, ASO and ITS Product Manager should discuss the disposition of any residual data such as network files and data stored on the users local PC, zip disks, etc. The data, as necessary, should be archived either to tape or to an alternative location as directed by the BPO or as recommended by ITS. Any archived data should be retained for a length of time in accordance with University policy. (Disposition of data files involving ITS may require a "task" be established in the Remedy Change Request Ticket).

Note: The ASO and key ITS Management should also perform a weekly review of Termination Reports to ensure that all users whose access should be terminated are identified. See [Monitoring – Termination Reports](#), below.

Removing Access to Multiple Academic Units' Data

The BPO should complete the appropriate sections on the Access Form for each Academic Units data to be removed. A copy of the Access Controls Form should be submitted to the respective ASOs. Each ASO will process the request through Remedy in the same manner as other access removal requests.

Example 1: A user employed in Human Resources needs to have access removed from Human Resources and Business & Finance. The BPO in Human Resources will complete the appropriate sections on the Access Form for Human Resources and Business & Finance. A copy of the Form would be submitted to the ASOs for Human Resource and Business & Finance.

Example 2: A user employed in Mission & Ministry needs access removed from Human Resources, Business & Finance and Students. The BPO in Mission & Ministry will complete the appropriate sections on the Access Form for Human Resources, Business & Finance and Students. A copy of the Form would be submitted to the ASOs in Human Resource, Business & Finance, and Students.

Saint Louis University Logical Access Procedure

Removing ITS Access

The user's direct supervisor (IT Product Manager or IT Administrator) serves as the "requestor" and is responsible for preparing and submitting an *ITS Access Security Request Form* for access removal. The direct supervisor (requestor) routes the Form to the appropriate section "IT Administrator" for review and approvals.

After the appropriate IT Administrator approvals, the user's IT Administrator will approve the Form and initiate the Remedy ticket, attach the Form, and route tasks to the respective ITS Administrator or ITS Product Managers, who will complete the tasks to remove the user access and provide a reply in the Remedy ticket to the requestor.

B. Emergency Terminations

Emergency Terminations are situations that require immediate removal of user access rights, in the judgment of the BPO or other high ranking University official. In these instances, circumstances surrounding the termination and/or the nature of the user access rights makes it necessary to temporarily by-pass preparation of the Access Form and/or the ASO, and verbally communicate (or email) the need for access removal to the ITS Product Manager.

The BPO/ASO should consider the circumstances surrounding the termination or the nature of the user access rights, when making this decision.

Example 1: A temporary project is ending, a pending layoff, or semester ends for a student work, where the last day of work is several days or more into the future. The user has access to systems and access rights (i.e., read-only) that do not pose a high risk to the University, do not warrant immediate removal of access rights and the BPO expects the user to continue with normal work responsibilities until their last day of work. This should be processed in the same manner as a Resignation/Termination, as noted in the previous section.

Example 2: A user is being terminated under negative circumstances and/or the user has access rights that may allow them to compromise University data or inappropriately distribute data. The BPO may determine it is necessary to request immediate removal of access, which would be processed as an Emergency Termination.

The ITS Product Manager will "lock" the account and prepare a Remedy ticket, with tasks to ensure subsequent confirmation of the access removal request.

As a follow up to ensure confirmation of the access removal request and satisfy documentation of removal, tasks should be directed to the appropriate ASO to obtain an Access Form from the BPO. The Access Form should note that the removal of the user's access was requested under immediate circumstances and provide a brief description as to those circumstances. The Access Form should be submitted to the ASO. The ASO should ensure/confirm that all applicable access rights have been removed and include the Access Form and any other follow up correspondence within the Remedy Ticket.

Note: The absence of the primary ASO does not automatically warrant the use of the Emergency Termination process. The BPO should refer to the designated ASO Backup (**See Appendix 1**).

Saint Louis University Logical Access Procedure

C. Lock Accounts

There may be instances where a BPO, ASO or ITS Product Manager determines that a user access rights needs to be temporarily “locked” until authorization of user access rights can be confirmed. This will typically occur as a result of the review of Service Access Reports, Termination Reports or Position Change reports (discussed in the [Monitoring Section](#) below). This could also occur when a user is separating from the University and the BPO must determine the appropriate disposition of the users account.

XI. DOCUMENT RETENTION

Approved Access Forms and other documents used to support authorization (or denial) to access University Information Systems or to support removal of user access, should be retained or embedded within the corresponding Remedy ticket. If circumstances warrant (i.e., Remedy is unavailable), the supporting documentation may be stored in electronic email folders or in secured file cabinets (in the case of hardcopy). If documents are retained in email or hardcopy, the documents should be organized by user name or by other means which would allow easy location of the supporting documentation for any particular user. Documents should be retained for a length of time in accordance with the University’s Data Retention policy.

XII. MONITORING

The BPO, ASO and ITS must monitor users for the following types of events within the organizations for which they are responsible and determine if individual user access needs to be modified or removed:

- Termination of employment
- Change in employee duties due to:
 - reorganization of work within department
 - personnel changes within department
- Change in organization hierarchy and/or creation of new organization
- Establishment of new projects.
- Account Inactivity

The following sections provide detailed procedures for the Monitoring Reviews (***See Appendix 7 for a Summary of Monitoring Reviews***):

A. Service Access and Account Inactivity Reports Review

On at least a bi-annual basis, University ITS will initiate a review of user accounts and corresponding access rights. Reports will be provided or made available to ASOs, BPOs (as identified), ITS Product Managers and/or ITS Business Manager (collectively to be referred to as “Reviewers”). The following reports will be utilized:

- Service Access Report – Comprehensive listing of users’ access rights by organization units. (***See Appendix 4 for sample report***) The reports should list all students, employees (faculty/staff), guests, and contractors who have access, including power users, developers and administrative users, to Banner (INB and Self Service) and its associated integrated systems (WebFOCUS, Xtender, Axiom, Workflow), and underlying databases.
- Account Inactivity Report – Lists accounts with no log-in activity for at least the last 90 days.

Saint Louis University Logical Access Procedure

The review process will be performed as follows:

1. The reports are produced and made available to each Organizational Unit (OU) via WebFOCUS Report Caster. An email message will be issued to each OU BPO of record informing them that the reports are ready for review, providing instructions on how to access the reports, and a summary of the review process.
 - a. For ITS, the ITS Business Manager and/or designated ITS Administrators and Product Managers, fulfill the role of the BPO. There should be separate reports and reviews for ITS staff user access rights and DBA users.
2. The BPO reviews the report for their respective OU and takes action as necessary. (Note: The ASOs and ITS Business Manager may access the Service Access Report at any time, on the WebFOCUS Dashboard, to review access rights.)
 - a. The identified BPO for distribution of the report may be at an Executive Level. The Executive may delegate the review and disseminate the report to its management staff as deemed necessary.
3. If it is determined that a user has access rights that should be changed/removed (i.e., inappropriate rights, segregation of duties issue, terminated employee), the BPO or ITS Management should submit the request for changes on an Access Form in accordance to the [Changes to User Access](#) or [Access Termination Procedures](#), as discussed within this desk procedure. The Access Forms should be retained in accordance with Document Retention procedures, as discussed within this desk procedure.
4. The BPO sends an email reply to the QA Administrator with a *Monitoring Review Form* attached to note that the review has been performed. In the Monitoring Review Form, the BPO will note a brief description of action taken. Example message from the BPO of General Counsel (E15):
 - a. "Completed review of report dated 4/30/08 for OUs S52, S53, S54, S56, S57. Action taken for user John Doe, SLU NETID #222222 – removed access."
5. The QA Administrator will maintain a log noting each review completed and ensure all reviews are completed. The QA Administrator will follow up with the BPO that have not submitted a *Monitoring Review Form*.
6. The QA Administrator stores the log along with the email confirmations in a secured electronic folder. Corresponding reports should also be maintained.
7. If an ASO wants to verify that their areas have been reviewed, they can contact the QA Administrator or request that BPOs copy them on the emails.

The Service Access Reports and Account Inactivity Reports review (including submission of *Access Forms* and *Monitoring Review Forms*) should be completed and by the end of the following month. (Example: For the period ending April 30th, the review should be completed by the last working day in May).

B. Position Change Reports

On at least a weekly basis, ITS will make available or provide a Position Change Report to all ASOs and the ITS Business Manager. **(See Appendix 6 for sample report)**. The Position Change Report lists employees (faculty/staff) who have changed positions within the University (over the last 28 days). The ASOs and ITS Business Manager should review the reports to determine whether any changes are necessary to user access rights. The ASOs and ITS Business Manager should identify BPOs in a position to assist in the review process and coordinate the dissemination of the reports to those BPOs for review, as necessary, or inquire with the BPO regarding needed changes.

If a change to one or more user's access is required as a result of the review, the BPO and ITS Business Manager should submit the request for changes on an Access Form in accordance to

Saint Louis University Logical Access Procedure

the [Changes to User Access](#) procedures, as discussed within this desk procedure. The Access Forms should be retained in accordance with Document Retention procedures, as discussed within this desk procedure.

The ASO and ITS Business Manager must document that the Position Change Report has been reviewed as required. (See examples of the documentation of review in the section [Documentation of Monitoring](#) below). The ASO and ITS Business Manager should forward a Monitoring Review Form of the review to the QA Administrator for maintaining. In the verification form, the BPO will note a brief description of action taken. The Position Change Reports should be retained for a length of time in accordance with University policies.

The review (including submission of Security Request Forms and Monitoring Review Forms) should be completed by the end of the week. (Example: If the Report is available on Monday morning, the review should be completed by Friday of that week).

C. Termination Reports

On at least a weekly basis, ITS will make available or provide Termination Reports to all ASOs and ITS Business Manager. (**See Appendix 5 for sample report**). The reports should be formatted or segregated in a manner that allows the ASOs and ITS Business Manager to review terminations for their respective academic units or areas of responsibility.

The Termination Reports lists all students, employees (faculty/staff), guests, and contractors who have separated from the University, but whose application and/or database access has NOT been removed to date. The Termination Reports should not serve as the first identifier of separated employees. As discussed in the [Access Termination Procedures](#) section above, if the BPO submits a request for access removal at the time of the user's separation, then the user should not appear on the Termination Reports. The Termination Reports should only serve as a secondary identifier of those users who were not properly identified for processing through the Access Termination Process or who have future dates for termination.

As the Termination Reports represents separated users, the ASO and ITS Business Manager may utilize the reports as the basis to remove the user's access. The ASO and ITS Business Manager should perform the following:

- Send a Remedy task to the Banner INB Product Manager to request that the account be temporarily locked.
- Confirm the employment status of the user with the BPO and determine if access rights should be removed. The reply should be documented via email.
 - If no reply is received within 24 hours, submit Remedy ticket to remove access.
- Based on reply, if access is to be removed, submit Remedy ticket to remove access. If access is to remain, inform Banner INB Product Manager to remove the temporary lock.
- For access removal, the Termination Reports and email replies should be attached to the Remedy ticket. The Remedy ticket should also include a task to notify the BPO of the access removal. (Note: Only remove access for those users whose terminated dates have passed; not those with future termination dates)

The ASO and ITS Business Manager must document that the Termination Reports have been reviewed as required. (See examples of the documentation of review in the section [Documentation of Monitoring](#) below). The ASO and ITS Business Manager should forward a Monitoring Review Form of the review to the QA Administrator for maintaining. In the verification form, the BPO will note a brief description of action taken. The Termination Reports should be retained for a length of time in accordance with University policies.

Saint Louis University Logical Access Procedure

The review (including submission of Security Request Forms and Monitoring Review Forms) should be completed by the end of the week. (Example: If the Report is available on Monday morning, the review should be completed by Friday of that week).

E. Documentation of Monitoring

The Reviewers must document that the Service Access Report, Audit Inactivity Report, Position Change Report, and Termination Report have been reviewed as required. The Reviewers are required to submit a Monitoring Review Form indicating that the reports have been reviewed and include a description of the action taken regarding user access rights. The reviewers should maintain documentation for their records. Some examples of documentation of review may include, but are not limited to, one or a combination of the following:

- The Monitoring Review Form (Note: This form should be retained for all reviews)
- Hardcopy report with Reviewers initials/signature and date directly on a hardcopy, as evidence of review. Tickmarks and other notations, as necessary, may be included on the report noting individual items reviewed and action taken.
- A log (electronic or hardcopy) that lists the reports and report date, with an indication that the report has been reviewed by the BPO, ASO, and/or ITS Management. (You may consider embedding or linking a copy of the reviewed report in your electronic log).
- Emails indicating that the reports have been reviewed and a notation of those users that required some change/removal of access rights.

Regardless of the manner of review, the QA Administrator should ensure for audit validation that the documentation of review and action taken as a result of the review is clearly noted. The QA Administrator should ensure the reports reviewed are retained (whether electronically or hardcopy) for a length of time in accordance with University policies. The QA Administrator will provide a periodic logical access compliance report to upper management.

XIII. NETWORK OPERATING SYSTEM LOGGING

Banner and other key network Operating Systems can be utilized to provide built-in auditing capability and to monitor a variety of events. The following audit categories must be enabled:

- Logon and Logoff – Success and Failure
- Use of user rights – Failure
- User and Group Management – Success and Failure
- Security Policy Changes – Success and Failure
- Restart, Shutdown, and System –Failure

ITS will maintain Audit Activity Logs capturing these events. ITS will review the Audit Activity Logs on a weekly basis for potential security problems or suspicious activity. ITS will use its judgment in determining the appropriate level of investigation and action to be taken, if any. The action should be taken in a timely manner to resolve the issues. **(Note: ITS will designate a person(s)/position for the review of the audit logs. Also, ITS should consider a policy requiring specified action based upon the type of event, including events to be escalated to the University's Information Security Officer or Chief Information Officer).**

ITS Product Managers must document that the Audit Activity Log has been reviewed as required. The Audit Activity Logs and all documentation related to the investigation of events should be retained for a length of time in accordance with University policies.

The QA Office will be responsible for ensuring that required audit activity is maintained and documented in accordance with these procedures.

Saint Louis University Logical Access Procedure

APPENDICES

Appendix 1: ACADEMIC SECURITY OFFICERS

Note: Security Officers and Organizational Unit heads should ensure that the backups are aware of their roles and are properly trained.

<u>Department/Unit</u>	<u>Security Officer</u>	<u>Back Up</u>
Advancement	Will Curran	Valerie Mangnall
Business & Finance	Lisa Zoia	Jenny Kukic
Human Resources	Nick Hebel	Derrick Weathersby
Student	Ellen Weis	John-Herbert Jaffry
Student Financial Services	John Mejaski	Tena Jones

Appendix 2: ITS PRODUCT MANAGERS

<u>Department/Unit</u>	<u>Security Officer</u>	<u>Back Up</u>
Axiom	Maggie Waters	Bob Kovarik
Banner INB	Mary Ann Poitras	Jeff Kapp
Banner Self Service	Rena Davenport	Jeff Kapp
ODS/EDW	Renee Canavan	Elaine Sloan
Oracle	Noel Humphrey	Kevin Ballard
WebFOCUS	Renee Canavan	Elaine Sloan
Xtender	Pat Shoff	Tim Moser
Workflow	Maggie Waters	Rena Davenport

Appendix 3: ACCESS SECURITY REQUEST FORM APPROVAL LEVELS

<u>Department/Unit</u>	<u>Minimum Level Required for Access Security Request Form Approval</u>
Human Resources	Business Manager
Business & Finance	Business Manager
Student Financial Services	Associate Director
Advancement	Director
Student	Director
ITS	IT Administrator and/or Architect
Other University Departments	Business Manager

Note: A list of specific approver names is maintained by ITS. **(Include specific address to WebFOCUS link. Determine if accessible by everyone)**

Saint Louis University Logical Access Procedure

Appendix 4: Sample – Service Access Report

(Note: Actual report may be presented in alternate format)

User: Moser, Tim (MOSERTE) BannerID: 000041204
Org.: Z604-ITS-Client and System Services
Employment Status: Active -- E-Class: 30-FT Staff Salaried
Hire Date: 05/09/1988 -- Termination Date:

LogonID	Banner Class	Banner Direct Object	Workflow Name	Axiom Group Desc	XTENDER Desc.	WebFOCUS Role	WebFOCUS Domains	SelfService Role	FOBPROF Master Fund	FI M O
MOSERTE	BAN_ARSYS_C	FORMFUSION	Business Analyst			User	AR Finance Reconciliation Domain	ESEEPCON	Both	B.
MOSERTE	BAN_FINANCE_C	FORMFUSION_ARCHIVER	SysAdmin			User	Finance Budget Development	HRMANAGER		
MOSERTE	BAN_GENERAL_C	FORMFUSION_SERVER	Central Admin			User	Finance Development Domain	MASTERSALAPLANNER		
MOSERTE	BAN_PAYROLL_C	SOQMENU	WorkflowModeler			User	ITS Helpdesk	UMGTOOLS		
MOSERTE	BAN_POSNCTL_C	SPAPERS				User	Logical Access			
MOSERTE	BAN_STUDENT_C									
MOSERTE	SLU_AL_BASIC_NEEDS									
MOSERTE	SLU_AL_TECHNICAL									
MOSERTE	SLU_AL_VALIDATION									
MOSERTE	SLU_BXS_EXTENDER									
MOSERTE	SLU_FI_ADITS_VIEW_ONLY									
MOSERTE	SLU_FI_BASIC_NEEDS									
MOSERTE	SLU_FI_BURSR_CSHRNG_SPR_USR									
MOSERTE	SLU_FI_BURSR_CSHR_USER									
MOSERTE	SLU_FI_FINSRV_AMEX_REMIT									
MOSERTE	SLU_FI_FI_FABCHKZ									
MOSERTE	SLU_GENERAL_C									
MOSERTE	SLU_GEN_BASIC_NEEDS									
MOSERTE	SLU_HR_BASIC_NEEDS									
MOSERTE	SLU_HR_HR_PDP_SLU1									
MOSERTE	SLU_HR_HR_PDP_SLU2									
MOSERTE	SLU_HR_SALARY_PLANNER									
MOSERTE	SLU_PC_BASIC_NEEDS									
MOSERTE	SLU_PC_PC_NXPDYUP									
MOSERTE	SLU_ST_GOAMTCH_M									
MOSERTE	SLU_ST_STUDENT_BXS_Q									

Saint Louis University Logical Access Procedure

Appendix 5: Sample – Termination Report

Terminated Employee Report for the Finance module
11/18/07

<u>Name</u>	<u>SID</u>	<u>SLU Net ID</u>	<u>Employee Status</u>	<u>Termination/ Last Date</u>	<u>Security Class</u>
Groves, Matthew S.	000664140	GROVESMS	Last Day Prior Today	11-16-2007	SLU_FI_BASIC_NEEDS SLU_FI_REQ_UPDATE
Job: Project Manager		Report To: VP-Facil Mgmt & Civic Affairs, Facilities Planning & Management, Design & Construction			
Lodes, Kelly L.	000930886	KLODES	Terminated	11-09-2007	SLU_FI_BASIC_NEEDS SLU_FI_REQ_UPDATE
Job: Development Assistant		Report To: VP-University Advancement, University Development, Frost Development			
Morgenthaler, Wanda E.	000247989	MORGENWE	Last Day Prior Today	11-15-2007	SLU_FI_BASIC_NEEDS_QUERY SLU_FI_REQ_UPDATE
Job: Research Assistant, Sr.		Report To: Provost-Medical Center Divisions, School of Medicine, Comparative Medicine			
Primo, Elizabeth A.	000317376	PRIMOB	Terminated	10-31-2007	SLU_FI_BASIC_NEEDS SLU_FI_REQ_UPDATE
Job: Administrative Assistant, Sr.		Report To: E40, School of Medicine, Ob/Gyn/Women's Health Ob/Gyn-Administration			

Appendix 6: Sample – Position Change Report

Internal Change of Position Report for the Finance module
11/18/07

<u>Week(s) on Report</u>	<u>Name</u>	<u>SID</u>	<u>SLU Net ID</u>	<u>End Date Prior Job</u>	<u>Begin Date Current Job</u>	<u>Security Class</u>
Week #1	Hoffman, Charleta A.	000091250	HOFFMANC	11-18-2007	11-19-2007	SLU_FI_BASIC_NEEDS SLU_FI_REQ_UPDATE
	Current Job: Patient Coordinator	Report To: E40, School of Medicine, Ob/Gyn/Women's Health Ob/Gyn-Bellevue Practice				
	Prior Job: Patient Coordinator	Report To: VP-Student Development, Student Devel.-Business Admin., Student Health Center				
Week #2	Sayles, Latonya C.	000153654	LSAYLES	11-04-2007	11-05-2007	SLU_FI_BASIC_NEEDS SLU_FI_REQ_UPDATE
	Current Job: Administrative Assistant, Sr.	Report To: E40, School of Medicine, Ob/Gyn/Women's Health Ob/Gyn-Administration				
	Prior Job: Administrative Secretary	Report To: E40, School of Medicine, Ob/Gyn/Women's Health Ob/Gyn-Administration				
Week #3	Misuraca, Debra K.	000914427	DMISURAC	11-30-2007	11-01-2007	SLU_FI_BASIC_NEEDS SLU_FI_REQ_UPDATE
	Current Job: Academic Advisor	Report To: Provost, Cook School of Business, CSB-Undergraduate Admissions				
	Prior Job: Executive Assistant	Report To: Provost, Cook School of Business, CSB-Administration				
	Ernge, Keith J.	000885172	KEMGE	10-31-2007	11-01-2007	SLU_FI_BASIC_NEEDS SLU_FI_REQ_UPDATE
	Current Job: Business Analyst	Report To: VP-Business and Finance, Financial Management, Financial Planning and Budgeting				
	Prior Job: Human Resources Assistant	Report To: VP-Human Resources, Human Resources, Benefits Office, University				
	Morgan-Cox, Sandra L.	000037038	MORGANSL	10-31-2007	11-01-2007	SLU_FI_BASIC_NEEDS SLU_FI_REQ_UPDATE
	Current Job: Human Resources Specialist	Report To: VP-Human Resources, Human Resources, Employment/Employee Relations				
	Prior Job: Human Resources Generalist	Report To: VP-Human Resources, Human Resources, Employment/Employee Relations				
Week #4	Seemiller, Cheryl R.	000035092	SEEMILCR	10-21-2007	10-22-2007	SLU_FI_BASIC_NEEDS SLU_FI_REQ_UPDATE
	Current Job: Secretary, Administrative	Report To: Provost-Medical Center Divisions, School of Medicine, Pediatrics				
	Prior Job: Administrative Assistant	Report To: Provost-Medical Center Divisions, School of Medicine, Pediatrics				

Saint Louis University Logical Access Procedure

Appendix 7: Summary of Monitoring Reviews

Report	Review Timing	Responsible Parties
Service Access	Twice a Year – April and October	Business Process Owner Security Officer
Inactivity	Twice a Year – April and October	Business Process Owner Security Officer
Termination	Weekly	Security Officer
Position Change	Weekly	Security Officer