STAMFORD INTERNATIONAL UNIVERSITY
The Difference is Real
A member of LAUREATE INTERNATIONAL UNIVERSITIES

USER ACCOUNT MANAGEMENT POLICY

IT-P-010

Date: March 3, 2014

Users Account Management Policy
Department of Information Technology

Purpose

The purpose of this Policy is to establish the rules for the requesting, reviewing, approving, maintaining and terminating user accounts.

User access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorized use.

Formal procedures must control how access to information is granted and how such access is changed.

Scope

This policy applies to all users of STIU's information assets to include all divisions, departments, business units, vendors, consultants, subcontractors, staff, faculty or students regardless of geographic location. This policy covers all information assets operated by STIU or those contracted with third parties by STIU. The term "information asset" defines electronic and non-electronic assets and includes, but it is not limited to all documentation, business processes, data, products, hardware (e.g. desktop, network devices), and software.

Procedure Information

Responsible Office: Department of Information Technology, Stamford International University
Issued Date: March 3, 2014

Revision History

Revision Number	Document Number	Description	Effective Date
00	IT-P-009	New Release	December 24, 2013
01	IT-P-010	Release 1	March 3, 2014

Contents

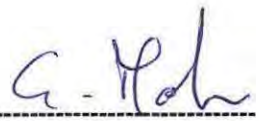
Recommendation and Approvals

Prepared by:

Name: Stella Root
Position: Business Analyst
Date: March 3, 2014

Approved by:

Name: Sourjya Sankar Sen
Position: Director, Information Technology
Date: March 3, 2014



Name: Gilles Mahe
Position: CEO, Stamford International University
Date: March 3, 2014

Name: Dr. Boonmark Sirinaovakul
Position: President, Stamford International University
Date: March 3, 2014

User Access Management

All internal and external users should be uniquely identified and authenticated prior to accessing STIU's information assets in order to provide accountability for the user's actions. The IT Department shall ensure that appropriate access controls are implemented to protect all of STIU's information assets.

Access to information assets should be permitted only for validated business roles, responsibilities, and requirements and should be formally authorized by HR Department. Users should be associated with roles that should only have the minimum access rights and privileges needed to perform a particular function or transaction. Users should be prevented from gaining access to information assets for which they do not possess a validated business requirement.

User Identification

Access to STIU information assets should be restricted to authorized users only. The designated owner of the information asset should authorize role entitlements only on a 'need to know' basis and users should be associated with these roles. IT and HR Departments should verify user's identity as a condition for providing them with access to STIU information assets.

This policy establishes STIU's user account management policy for administering the accounts of system users to include accounts, passwords, privilege management, and user transfer/termination.

User Verification/Registration

HR department should submit a request for user access for each new user. An "Employee Setup Request Form" should be used to document the user access request. Requests from unauthorized users should be returned to the requestor.

The following guidelines should be followed in registering authorized users:

- No users are to be provided access without a request from HR Department;
- User access rights must be reviewed to ensure that the appropriate rights are still allocated;

User ID Composition

Each new user should be assigned a unique User ID generated by the IT Department based on user's First and Last names.

Generic Accounts

A "generic" user account that is designated for use by either multiple users, anonymous users and/or departments, without enabling individual authentication and accountability, is not allowed. Exceptions to this policy require the documented approvals from both the owner of the information asset or business process, and from IT Department Director.

Default System Accounts

The default accounts shipped with software should be disabled unless doing so would cause the software to malfunction. Immediately upon installation, if technically feasible, all administrator equivalent user accounts should be renamed and password should be changed or disabled/removed if not required.

Privileged Accounts

Users that are granted privileged access (i.e., access to system security mechanisms, etc.) will use a different unique account name assigned to a unique user when exercising those privileges. Otherwise, a user id with more standard privileges should be utilized. Users will:

- Maintain one ID with normal user privileges for everyday use.
- Maintain at least 1 additional ID solely for exercising higher system privileges.

Least Privileges

Privileges should be provided to align risk commensurate with that which is necessary to conduct business. This should be accomplished by minimizing the access rights and privileges of users to the level needed to complete their assigned and approved responsibilities. The level of systems access granted to any user should be appropriate for the business purpose.

User Transfer/Termination Standard

This section establishes the standard process to be followed, in the event an authorized user is terminated or transferred.

Designated user managers and the HR Department are required to inform the IT Department immediately of changes in the employee's job function and/or employment termination in order to ensure that access privileges are appropriately adjusted in a timely manner.

Detailed procedures should be developed and followed for user transfer and termination process.

Notification

The institution's management will notify the HR Department of any changes in personnel status. Then HR will notify the IT Department within a reasonable time frame upon the resignation, termination or transfer of users to ensure that their access to critical applications is revoked or adjusted as needed.

Revocation

Upon a user's termination or resignation, user IDs and passwords associated with that user should be disabled immediately.

User Job/Function Change Notification

The institution's management will notify the HR Department of any function changes in personnel status. Then HR will notify the IT Department within a reasonable time frame following the employee job/function change or transfer of users to ensure that their access to critical applications is revoked or adjusted as needed.

Termination Report

The termination report generated by HR Department will be obtained and reviewed periodically by IT department. A ticket will be generated in the HelpDesk system three times a year to review the accounts against HR records of active/terminated employees.

All user access rights belonging to terminated employees that are still active should be disabled immediately.

Password Management

All STIU information assets should be protected by the appropriate authentication controls. Passwords are the most common form of the authentication controls for electronic information assets. Users should supply valid user-ID and password in order to be granted access to the STIU electronic information assets.

Additional details regarding password settings, standards and management has been defined in the STIU Security Policy.