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

DATA CENTER ACCESS PROCEDURE

IT-P-008

Date: 8 January, 2014

Data Center Access Procedure
Department of Information Technology

Purpose

The following procedure is to be followed to limit physical access to IT Systems and associated services that reside in the Data Centers of Stamford International University. These systems and services are maintained by the Department of Information Technology. This procedure provides guidance in obtaining access, reviewing access, and authorizing access to these secure areas.

The following areas have been identified as critical security points and are controlled by finger scan locks managed by Department of Information Technology:

Area	Responsible Personnel
Data Center, Floor 6, Building 2, Bangkok Campus	Department of Information Technology, Bangkok
Data Center, Floor 3, Main Building, Hua-Hin Campus	Department of Information Technology, Hua-Hin

Procedure Information

Responsible Office: Department of Information Technology, Stamford International University
Issued Date: 8 January, 2014

Revision History

Revision Number	Document Number	Description	Effective Date
00	IT-P-008	New Release	8 January, 2014

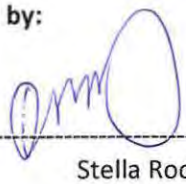
STAMFORD INTERNATIONAL UNIVERSITY
The Difference is Real
A member of LAUREATE INTERNATIONAL UNIVERSITIES

Contents

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

Recommendation and Approvals

Prepared by:



Name: Stella Root
Position: Business Analyst
Date: 8 January, 2014

Approved by:

Name: Sourjya Sankar Sen
Position: Director, Information Technology
Date: 8 January, 2014

Name: Gilles Mahe
Position: CEO, Stamford International University
Date: 8 January, 2014

Name: Dr. Boonmark Sirinaovakul
Position: President, Stamford International University
Date: 8 January, 2014

Access Process Description

Access to Data Centers are protected by Biometric (Fingerprint Recognition) Access Control Systems.

Staff members of the Department of Information Technology who are authorized to access the Data Centers will be registered in their respective Fingerprint Recognition Systems.

Non-IT staff & third-parties requiring access will not be registered in the Fingerprint Access Control System but will be granted supervised access through a different process explained in the next section of this document.

Request for Access Process

IT Department Staff

Only full-time IT Department employees - whose job role dictates physical access to the IT systems housed in the Data Centers – will be duly authorized for access and will be registered in the Fingerprint Access Control System. Such access will only be granted as per request from the HR Department during the new hire process.

Non-IT Staff and Third-parties

Non-IT Department employees and third-parties such as IT vendors, visitors, guests who require access to the Data-Center for implementation, integration and/or maintenance work shall only be permitted access under constant supervision of an authorized IT Department employee with explicit written permission from the IT Director. Requests for all such access must be accompanied with a full explanation of reasons for such a visit. On all visits, details of the visitors will be recorded by the supervisor in a log sheet, available inside the Data Center, along with check-in and check-out times. Only authorized IT Department employees are allowed to sign in visitors.

The IT Director will review all requests for access to determine if all required documentation has been received, all required information is complete, and the requested access is necessary or if the level of access is appropriate.

Once the access has been established for an applicant, the IT Staff will notify that person and provide them with any necessary access information.

*The only exception allowed to the Data Center Security Policies and Practices is temporary suspension of these rules if it becomes necessary to provide emergency access to medical, fire and/or police officials.

Monitoring of Activities inside the Data-Centers

Access to the Data-Centers and activities conducted inside them are monitored 24/7 via the following ways:

1. CCTV camera placed outside the Data-Center door to monitor access vs. in and out timings.
2. Environmental sensors (unexpected changes in Temperature, Humidity, Audio) and CCTV camera placed inside the Data-Centers.

Logs from both the systems will be reviewed on a periodic basis as elaborated in the **Data Center Access Auditing and Review Process** section.

Termination of Access

Access to the Data Center may be removed at any time by request from the HR Department or the individual's supervisor.

If an employee from the IT Department resigns or transfers to another department, his/her access to the Data Center will be revoked as per the Termination/Transfer request from the HR Department.

An individual's access may also be immediately terminated if it is determined that they are violating appropriate access procedures for secured areas.

Data Center Access Auditing and Review Process

A review of the Fingerprint Access Control System logs, in conjunction with video feeds and sign-in sheet for the Data-Center will be conducted on a monthly basis by designated staff of the IT Department to spot check for any suspicious or inappropriate access or activities. Any questionable use of access will be investigated and the necessary staff will be contacted to appropriately resolve such incidents.

The Data Center sign-in sheet that provides information on individual access to the data center will be provided to the IT Director for monthly verification and review.

This process will be triggered by the automatic ticket in the FootPrints system. All the findings/resolutions will be logged to the ticket and ticket will be closed.