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

IT BACKUP POLICY AND PROCEDURES
IT-P-005

Date: 7 November, 2013

Stamford International University
IT Backup Policy and Procedures

Purpose

This document is intended to provide data backup and retrieval operations procedures.

Scope

The intended recipients of this policy are internal departments that store their data in the Stamford International University's ("STIU") Enterprise Data Center.

Entities Affected By This Policy

All employees of Stamford International University

Policy Information

Responsible Office: Department of Information Technology, Stamford International University
Issued Date: 7 November, 2013

Revision History

Revision Number	Document Number	Description	Effective Date
00	IT-P-001	New Release	31 October, 2013
01	IT-P-001	Second Revision	7 November, 2013

Contents

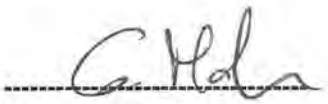
Recommendation and Approvals

Prepared by:

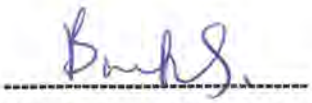
Name: Stella Root
Position: Information Architect
Date: 7 November, 2013

Approved by:

Name: Sourjya Sankar Sen
Position: Director, Information Technology
Date: 7 November, 2013



Name: Gilles Mahe
Position: CEO, Stamford International University
Date: 7 November, 2013



Name: Dr. Boonmark Sirinaovakul
Position: President, Stamford International University
Date: 7 November, 2013

1. Policy

The IT Department recognizes that the backup and maintenance of data is critical to the viability and operations of the organization. It is essential that certain basic standard practices be followed to ensure that data files are backed up on a regular basis and available for restoration.

2. Procedure

Backup Methodology

The backup server currently deployed has 4 x 1TB backup hard drives in Bangkok, 4 x 1TB backup hard drives in Hua-Hin and 2TB available in Loxinfo (cloud backup). The setup is designed to provide us with "real time" backup. The data from enterprise systems deployed at STIU (e.g. financial data, student records data, payroll data etc.) will be backed up in all three destinations.

The backup software used to control the backup processes on servers is CrashPlan.

Enterprise systems using database backend such as Oracle, MSSQL, MySQL are backed-up using database snapshot utilities, which create periodic snapshots of each database which are then automatically backed up by CrashPlan. The database snapshots are rotated over a 2 week period. Incremental backup of server images run after business hours and the generated images are backed up using CrashPlan as well.

The backup sets are auto-encrypted prior to uploading on the backup servers – be it on-site or off-site.

Backup Log Review and Monitoring

The IT Support team ensures that all backups are completed successfully and monitors the backup process on all servers. Failure notifications are sent to the Service Management System and assigned to one of the IT support staff members. Logs are maintained and reviewed every two weeks to verify the amount of data backed up and the unsuccessful backup occurrences. Any unusual behavior in the backup (unsuccessful backup) will be reported directly to the IT Department Director for a further investigation.

A Footprints ticket is generated every 2 weeks to verify that backups are successful and retrieval is tested.

Departmental Backups

Departmental Network Shares are automatically included in the backup sets. All files & folders placed on such network shares are backed-up in real-time onto the backup servers, as long as they adhere to the restrictions outlined in the "Backup Content" section. All files that contain important data to STIU business should be stored only on Network Shares and not on personal computers. Access to the shares should be given only to the owners of this data.

Each department has to specify employees who work with critical data and specify the files and folders on the Network Shares, access to which should be limited. Departments will fill a form requesting the access configuration and forward the form to the Help Desk for action.

Backup Content

The content of data backed up varies from server to server. The primary data that will be backed up are:

1. Data files designated by the respective owners of the servers.
2. In some instances System Data (Applications files for the server and other selected software installed on the server).

Data to be backed up will be listed by location and specified data sources. This will be stipulated in a separate document called "Backup Source Manifest" that'll be compiled based on the feedback from respective server owners, departments and/or primary stakeholder through a "Backup Request Form".

Certain restrictions apply when it comes to backup content:

- Only critical files will be backed up;
- Personal files will not be allowed in the backup sets;
- No multimedia files (mp3, jpeg, video etc.);

If any department wishes to backup multimedia files (e.g. Marketing, Admissions, PR), the department in question will be required to share the cost of backup storage space under a separate SLA (service-level agreement).

The only data that IT Support Services accepts responsibility for is the data which is explicitly listed in the "Backup Source Manifest".

Backup Types

Backup of servers will occur every day after regular business hours.

Full backup: Includes all the source files. This method ignores the file's archive bit until after the file is backed up. At the end of the job, all files that have been backed up have their archive bits turned off. Only one full backup will be done once a week followed by differential and/or incremental. This is mostly employed for backing up of critical applications & resources.

Real-time versioned backup: Includes all source files as well (except the ones excluded via filters as described in the Backup Content section). Files & folders are monitored in real-time and are backed up immediately following a change. Individual versions are retained up to the specified retention periods.

Data de-duplication: The backup system employs enterprise grade data de-duplication to make efficient use of the allocated storage space.

Backup Security & Retention

The backup mechanism encrypts all data with a choice of 448-bit Blowfish or 256-bit AES encryption prior to uploading data onto the backup servers or the cloud. The encryption process is transparent and takes place at each end-point (client-side).

All backup sets are retained unlimited duration unless the retention period is explicitly specified in the client configuration. Special backups may be made for longer retention periods during special situations such as system upgrades and major projects.

Offsite Storage

STIU uses Loxinfo (cloud backup) as an offsite storage facility.