



TUSKEGEE UNIVERSITY

OFFICE OF INFORMATION TECHNOLOGY

Tuskegee Backup and Offsite Policy and Procedures

Purpose

This policy defines how to safeguard the information assets of the University and how copies of stored Tuskegee data on external media are warehoused in a location physically outside the borders of the University, as part of the broader disaster recovery plan. It also defines the expectations of the storage vendor as to how they handle and store Tuskegee storage media.

Scope

The intended recipients of this policy are internal departments that house their hardware in the University's Enterprise Data Center and all IT data that is being backed up in the Data Center.

Policy

The IT department recognizes that the storage of data backup copies in an offsite location are critical to the viability and operations of the respective departments and the University in its entirety. It is essential that certain basic standard practices be followed and expectations met to ensure that data be available in the case of a catastrophic event.

Backup Content

The content of data backed up varies from server-to-server. The primary data that will be backed up are: Data files designated by the respective owners of the servers and 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 "Data Sources Manifest" in appendix A. Because it is impractical for the Systems Support to backup every bit of data stored on the servers, the only critical data which is explicitly listed in the "Data Source Manifest".

Backup Types Stored

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 daily **incremental** backups.

Incremental backups: Includes only files that have changed since the last Full (Clear Archive Bit) or Incremental backup. The next time an incremental backup is done, this file is skipped (unless it is modified again).

We use the GFS (Grandfather-Father-Son) rotation for backups.



TUSKEGEE UNIVERSITY

OFFICE OF INFORMATION TECHNOLOGY

Daily backups (Son) take place on a five-day rotation.
Weekly backups (Father) take place on a five-week rotation.
Monthly backups of high availability servers occur the last calendar day of the month and are on a twelve-month rotation.
Special backups may be made for longer retention periods during special situations such as system upgrades and major projects.
Our Unix systems will be backed up on tapes consistent with the backup types and the rest of our servers will be backed up to an external hard drive.

Offsite Storage of tapes

Any data that requires offsite storage must be properly labelled. Daily, weekly and monthly tapes will be represented by yellow, green and blue labels respectively. Individual tapes will be marked with the following designation:

D1212017-1: with the first letter representing the type, the numeric characters that follow represent the date and the numeric characters that follow the dash be the tape number.

TYPE	COLOR	NAME
DAILY =	YELLOW	D01212017-1 – D01212017-15
WEEKLY =	GREEN	W01212017-1 – W01212017-50
MONTHLY =	BLUE	M01312017-1 - M01312017-25

All storage media must be logged for pickup and deliver by date and batch number.

Encryption

Both tapes and hard drives with data may not leave the data center without being encrypted. All media must have Symantec Endpoint Encryption with PGP technology installed on them.



TUSKEGEE UNIVERSITY

OFFICE OF INFORMATION TECHNOLOGY

Offsite Backup Procedures

The CIO is responsible for ensuring that this policy is carried out. Exceptions to the standard Offsite backup procedure are permitted when justified. All exceptions must be fully documented. The standard procedure for Offsite backup is as follows:

- I. A full and incremental systems backup will be performed with sufficient frequency so that the entire system and all data from all servers are backed up. This data should be sufficient for a complete restoration of all systems if necessary.
- II. Data to be backed up include the following information:
 1. User data stored on the hard drive.
 2. System state data
 3. The registrySystems to be backed up include but are not limited to:
 1. File server
 2. Mail server
 3. Production web server
 4. Production database server
 5. Domain controllers
- III. The last full backup of the month will be saved as archival records.
- IV. *Monthly backups* will be saved for one year, at which time the media will be recycled or destroyed.
- V. *Incremental backups* of new data will be performed daily. Incremental backups will be retained for sufficient time to restore data for at least a week, at which time the media will be recycled or destroyed.
- VI. Copies of all backups will be stored in a secure, off-site location.
- VII. Currently, all weekly and monthly archives are stored on location at Teretek facilities.
- VIII. No drives or tapes can leave the data center without proper encryption
- IX. Teretek will make weekly pickups of backup copies: pickups will be made every Friday by the close of business.
- X. Backup copies will be stored in a lock safe.



TUSKEGEE UNIVERSITY

OFFICE OF INFORMATION TECHNOLOGY

- XI. At the end of every month, a copy for that month will be archived and properly labelled.

Vendor Expectations

The vendor(s) storing Tuskegee storage media must meet the following criteria:

- I. Away from 100-year flood plain and known fault lines.
- II. Away from statistically high crime and fire areas; must not be within 50 miles of Tuskegee, city limits.
- III. Must not have any gas lines entering entire building.
- IV. Away from above-ground fuel storage tanks.
- V. Away from industrial train routes.
- VI. Must be accessible to multiple routes for entry and egress.
- VII. Must be at least 5 miles from computer location.
- VIII. Entire building must have 100% fire suppression coverage (includes any neighbors).
- IX. Must be access controlled (includes any neighbors).
- X. Must be near police and fire stations.
- XI. Must be in low-profile area away from high traffic routes.
- XII. Each vault must maintain acceptable temperature (60 - 70 degrees F).
- XIII. Each storage vault must maintain acceptable humidity (35% -45%).
- XIV. Temperature and humidity levels must be constantly monitored using a hygrometer.
- XV. Each vault must be tied directly to an alarm company to detect temperature variances.
- XVI. Vendor must have a written DR plan for its own facility.
- XVII. Vendor must have maximum 2-hour response on local emergency requests.
- XVIII. Vendor must be able to provide a bar code solution for tape movement.



TUSKEGEE UNIVERSITY

OFFICE OF INFORMATION TECHNOLOGY

Appendix A

Data Source Manifest			
Date:		Server Name:	

Type of Backup Agent Needed

	Windows	Version:		Type:	
	MAC	Version:		Type:	
	Unix	Version:		Type:	

List of Files/Folders to be Backed Up

Backup Client and Policy

Backup Client Installed On Client Server:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Backup Policy for Client Server:	<input type="checkbox"/> F M <input type="checkbox"/> F T <input type="checkbox"/> F W <input type="checkbox"/> F T <input type="checkbox"/> F F <input type="checkbox"/> F S <input type="checkbox"/> F S <input type="checkbox"/> D O <input type="checkbox"/> D U <input type="checkbox"/> D E <input type="checkbox"/> D H <input type="checkbox"/> D R <input type="checkbox"/> D A <input type="checkbox"/> D U <input type="checkbox"/> I N <input type="checkbox"/> I E <input type="checkbox"/> I D <input type="checkbox"/> I U <input type="checkbox"/> I I <input type="checkbox"/> I T <input type="checkbox"/> I N		
	Run Schedule for Policy:	AM:	PM:

Only One Full(F) followed by either a Differential(D) or an Incremental(I)



TUSKEGEE UNIVERSITY

OFFICE OF INFORMATION TECHNOLOGY

Retention and Offsite

Retention Period for Backup:	<input type="checkbox"/> 1 Week	<input type="checkbox"/> 2 Weeks	<input type="checkbox"/> 1 Month	<input type="checkbox"/> 2 Months
Offsite Storage:	<input type="checkbox"/> Yes		<input type="checkbox"/> No	

Signatures

Requestor's Signature:		Date:	
System/Backup Administrator Signature:		Date:	