THINK IN OTHER TERMS

NUST BACKUP AND RECOVERY POLICY AND PROCEDURES

Approved July 2018

Table of Contents

1 Purpose:

The purpose of this policy is to protect University Data from loss or destruction by specifying reliable backups that are based upon the availability needs of each unit and its data. The policy will also define the standards for the data backup and restoration performed at NUST by the ICTS department.

2 Scope:

This policy applies to all NUST Data and the Information Systems used with it. The Policy does not apply to information stored locally by users on desktops, laptops, tablets and mobile phones. Device owners are responsible for appropriate backup of the data stored locally on their mobile devices , with the exception of data synchronised with the device and stored on NUST servers.

3 Policy:

1. University Data is backed up in a manner sufficient to restore any or all of an Information System in the event of a data loss, according to Recovery Time Objectives and Recovery Point Objectives.
2. Backups should be periodically tested to ensure that they are sufficient and reliable.
3. Backup systems and media should protect the confidentiality, integrity and availability of stored data.
4. Written procedures are maintained to allow ICTS personnel to recover data in the event of an emergency.

4 Definitions

DRP- Disaster Recovery Plan is a documented set of procedures describing the key activities that are necessary to recover minimum IT services, applications and data to continue critical business operations, and to fully recover such operations after a disaster affecting normal IT services

RTO -Recovery Time Objective refers to the maximum tolerable length of time that a computer, system, network, or application can be down after a failure or disaster occurs.

RPO-Recovery Point Objective refers to the maximum acceptable amount of data loss measured in time. It is the age of the files or data in backup storage required to resume normal operations if a computer system or network failure occurs.

5 Responsibilities:

1. ICTS department management are responsible for establishing Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), in conjunction with data users and owners, for all University Data collected, stored or maintained by the department. ICTS should verify that Data used by the unit, but collected, stored or maintained by others, have appropriate backup plans.
2. ICTS department management are also responsible for the drafting and continuous updating of the following documents :

   a. Back Up Plan
   b. IT Disaster Recovery Plan

3. ICTS department engineers are responsible for implementing backup systems and processes to ensure that RTO and RPO can be met for all data collected, stored or maintained on unit Information Systems. ISs document backup system operation and test recovery capability.

6 Guiding Principles:

IT systems that are critical to Institution activities must be clearly identified, as well as the potential risks of disruption that apply to them.

IT continuity, backup and recovery must be managed in accordance with the outlined procedures in this policy

Recovery Time Objectives (“RTOs”) of critical systems must be formally defined as per the business needs.

Procedures and technology must be in place and tested regularly to ensure:

- Prevention against IT system disruption.
- Regular and comprehensive backup of critical systems, applications and data.
- Timely recovery of critical systems, in line with the business expectation or RTO.

7 Guidelines:

1. ICTS uses best practices in storage management to automate the data backup process – Individual servers will run incremental, daily, weekly, monthly, semester, and annual backups
2. In the event of an emergency; e.g., fire, earthquake; ICTS will prioritize the restoration based on the nature and extent of the situation, and the importance of the individual systems to the continued operation of the University.
3. Data stored on NUST servers must be on the servers for a minimum of 8 hours in order to be recoverable – files accidentally deleted, corrupted, or overwritten on servers that have not made it into the backup cycle cannot be recovered
4. Individual file restoration is a best effort service and can take from several hours to several days

Procedures

7.1 Backup Plan

1. Server backups will be performed every night.
2. The last backup of every month will be considered the monthly backup and kept for a year before recycling.
3. Monthly backup tapes/HDD/DVD will be stored in a fireproof safe off campus.
4. Backups will be performed and monitored by a fulltime ICT staff member.
5. Backups will be automated to occur every 12 hours .
6. Tapes/HDD/DVD will be inserted routinely every night before leaving work.
7. Backup failures will be reported to the Director of Information Technology and action will be taken quickly to fix the problem.
8. Backups will always be performed before upgrading or modifying a server.

7.2 Loss of data

1. If loss of data is discovered, evaluation and investigation by ICT staff is immediately dispatched.
2. In most cases, loss of data is related to file corruption, virus, security or human error.
3. If loss of data is related to data corruption, ICT Staff must troubleshoot and determine if the problem is hardware or software related to prevent addition file corruption.
4. If the loss of data is related to a virus, ICT Staff must determine the extent of the virus and remove it to prevent further loss of data.
5. If the loss of data is related to security or a compromised system, ICT Staff must determine the extent of the compromise and fix the vulnerability quickly to prevent further loss of data.
6. If the loss of data is related to human error, ICT Staff must immediately inform and train the appropriate personnel to avoid further loss of data.
7. Once the problem has been determined and loss of data minimized, ICT Staff should proceed to restoration of data from backup media.

7.3 Restoration of data

1. Once loss of data is discovered, evaluated and minimized, ICT Staff will proceed to restoration of data from backup media.
2. ICT Staff will determine the time and date of the lost data.
3. ICT Staff will determine the appropriate backup media to restore the data.
4. ICT Staff will insert the backup media into the appropriate server.
5. ICT Staff will invoke the Backup/Restore software.
6. ICT Staff schedule the restore of the appropriate data within the Backup/Restore software.
7. ICT Staff monitor the restore of data.
8. Upon restore, ICT Staff evaluate the integrity of the restored data.
9. ICT Staff will contact the end-user of the data to finalize restore.
10. Upon approval from the end-user, the restore is considered finished.

7.4 Disaster Recovery

1. If a disaster is discovered, ICT Staff will determine the extent of the problem and proceed accordingly.
2. If the disaster is hardware related, ICT Staff will replace the failed hardware and restore according to the steps outlined above.
3. If there is a natural disaster, such as water, fire, tornado, earthquake, or other, the hardware will be replaced and the server will be restored using the offsite backup media according to the steps outlined above.

4. Upon restoration of data, ICT Staff will check the data for integrity and validity.
5. ICT Staff will contact the end-user of the data to finalize restore.
6. Upon approval from the end-user, the restore is considered finished.

Effective Date:

Policy Number: