University of Kerala

Data Backup Policy

Introduction

Information security is becoming increasingly important to the University, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that the University's ICT systems, data and infrastructure are protected from risks such as unauthorised access, manipulation, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data.

The Backup procedure responsible for ensuring that University data stored on approved systems within the Over strand environment is recoverable in the event of accidental loss or damage.

Objective

The primary objective of the policy is to protect the University's data. This policy seeks to outline the data backup and recovery controls for University employees so as to ensure that the data is correctly and efficiently backed up and recovered in line with best practice.

Aim

The aim of this policy is to ensure that the University conforms to a standard backup and recovery control process in such a way that it achieves a balance between ensuring IT compliance, best practice controls, service efficiency. In addition, it seeks to define controls to enforce regular backups and support activities, so that any risks associated to the management of data backups and recovery are mitigated.

Scope

This policy repeals any previous ICT Backup and Disaster Recovery policies. This ICT Data Backup and Recovery Policy has been created to guide and assist the University to align with internationally recognised best practices, regarding data backup, recovery controls and procedures. This policy recognizes a diverse in nature, and therefore adopts the approach of establishing and clarifying principles and practices to support and sustain the effective control of data backup and recovery.

The policy applies to everyone in the University, including its service providers and consultants. This policy is regarded as crucial to the effective protection of data, of ICT systems of the University. University IT team must develop their own Data Backup and

Recovery controls and procedures by adopting the principles and practices put forward in this policy.

Administrative Policy

The System Manager at University Computer Centre is responsible for maintaining and ensuring compliance to this policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and where applicable, changes approved by the Syndicate. In absence of System manager, one of the senior system administrator will act as the backup manager who is appointed by the vice-chancellor.

Goals

The main goal of this policy is:

- To define and apply a clear backup and restore standard for University's informational systems;
- To prioritize systems accordingly to data sensitivity;
- To definition backup and recovery standards per data prioritization;
- To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster;
- To permit timely restoration of information and business processes, should such events occur;
- To manage and secure backup and restoration processes and the media employed in the process;
- To set the retention periods of information contained within system level backups designed for recoverability and provide a point-in-time snapshot of information as it existed during the time period defined by system backup policies.
- Backup retention periods contrast with retention periods defined by legal or operational requirements.

Principle

The following principles direct this policy:

- Proper backup, storage, and handling of data are necessary for all departments to achieve their objectives.
- Staff must accurately follow the policy and protect the availability, confidentiality, and integrity of data.

- Critical data, which is critical to the University, must be defined by the Business in consultation with ICT and must be backed up.
- Backup data must be stored at a backup location that is physically different from its original creation and usage location (i.e. The Disaster Recovery Site). The medium will dictate when schedule.
- Data restores must at least be tested quarterly.
- Procedures for backing up critical data and the testing of the procedures must be documented by the University Computer Centre. These procedures must include, as a minimum, for each type of data and system:

    (a) A definition of the specific data to be backed up;

    (b) The type(s) of backup to be used (e.g. full back up, incremental backup, etc.);

    (c) The frequency and time of data backup;

    (d) The number of generations of backed up data that are to be maintained (both on site and off site);

    (e) Responsibility for data backup;

    (f) The storage site(s) for the backups;

    (g) The storage media to be used;

    (h) Any requirements concerning the data backup archives;

    (i) Transport modes; and

    (j) Recovery procedure of backed up data

Data Backup Selection

- All data and software essential to the continued operation of the University, as well as all data that must be maintained for legal purposes, must be backed up.
- All supporting material required to process the information must be backed up as well. This includes programs; control files, install files, and operating system software.
- The application owner, together with the ICT, will determine what information must be backed up, in what form, and how often.

Backup Type

Backup data included that source code, database, required data folder other than source code.

- Full backups should be run weekly as these datasets will be stored for a longer time period. This will also aid in ensuring that data can be recovered with the minimal set of media used at that time. Once a month, a full backup should be stored off site. This statement will be subject to the review of the ICT DR Business Impact and Risk Analysis requirements are updated with input from System Administrators or System Manager.
- Differential/Incremental backups must be used for daily backups. This ensures that the backup time window is kept to a minimum during the week while allowing for maximum data protection.
- In the event that a system requires a high degree of skill to recover from backup, consideration must be given to making full images of such servers as a backup. This will ensure that the system can be recovered with minimal knowledge of the system configuration.
- For clarification purposes the ICT division may create a summary of backup types, along with their advantages, disadvantages and frequency and attach it to this policy as decided by the system Manger.

Backup Schedule

- Choosing the correct Backup Schedule: (a) Backup schedules must not interfere with day to day operations. This includes any end of day operations on the systems. (b) A longer backup window might be required, depending on the type of backups.
- Frequency and time of data backup:

  (a) When the data in a system changes frequently, backups needs to be taken more frequently to ensure that data can be recovered in the event of a system failure.

  (b) Immediate full data backups are recommended when data is changed to a large extent or the entire database needs to be made available at certain points in time. Regular, as well as event-dependent intervals, need to be defined.
- Previous versions:

  (a) The System Manager should determine the quantity of previous versions of operating systems and applications that must be retained at the Backup and Disaster Recovery location. In the absence of System Manager, a senior System Administrator must do this.

(b) Annual, monthly and weekly backups must be retained at the Backup and Disaster Recovery location. Weekly, Monthly and Annual backup media may be re-used to take new backups.

Backup Method

As for the backup processes performed, the following are considered acceptable by the University when conducting backups of all necessary data:

a) Manual – Manual backups are those performed by choosing what data to back up, when to backup, and to what device – all in a manual process.
b) Semi-Automated – Semi automated backups are those performed using backup tools and software, but still require somebody to initiate and launch the backup process itself.
c) Completely Automated – Completely automated backup processes have fast become the norm in many environments, as they effectively ensure the backup process is run on a regular scheduled time, complete with reporting metrics and other critical information.

Storage Medium

- When choosing the data media format for backups, it is important to consider the following:
  a) Time constraints around identifying the data and making the data available;
  b) Storage capacity;
  c) Rate of increasing data volume;
  d) Cost of data backup procedures and tools vs. cost if restored without backup;
  e) Importance of data;
  f) Life and reliability of data media;
  g) Retention schedules; and
  h) Confidentiality and integrity.
- Should high availability be required, a compatible and fully operational reading device (e.g. tape drive, CD, DVD or Blue ray disk) must be obtainable on short notice to ensure that the data media is usable for restoration even if a reading device fails.
- The Backup can be obtained from SAN or Network storage medium
- Maintain Register for secondary storage medium details.

The Data Owner

- Registrar is the sole authority of the entire digital data maintained and managed by the University.
- Concerned officials shall be responsible for integrity and security of the data pertaining to that section.
- The University should ensure that sufficient ICT capacity is available to maintain the Backup and Disaster Recovery procedures, so to ensure a segregation of duties and responsibilities and to mitigate the risk of systems and data losses.
- The System Manager has the discretion to assign at least two ICT staff members (One primary, one secondary) to ensure each backup schedule is maintained.

Recovery of Backup data

- Backup documentation must be maintained, reviewed and updated by the Manager, Systems Development periodically to account for new technology, business changes, and migration of applications to alternative platforms. This includes, but is not limited to:
  a) Identification of critical data and programs; and
  b) Documentation and support items necessary to perform essential tasks during a recovery process.
- Documentation of the restoration process must include:
  a) Procedures for the recovery
  b) Provision for key management should the data be encrypted.
- Recovery procedures must be tested at least quarterly and Disaster Recovery procedures must be tested at least yearly.
- Recovery tests must be documented and submitted to the Manager, Systems Development.

Backup Strategy

- Data will be protected by regular backups.
- Backup copies must be stored in a protected and access controlled secure offsite location.

- Stored copies must be stored with a short description that includes the following information: Backup date / Resource name / type of backup method (Full/Incremental).
- Backup can be made available upon authorized request: The request must be approved by an official nominated by the Head of Department/Statutory officer.
- Backup copies must be maintained in accordance with the University's Retention and Disposal Schedule. The backup schedule will determine the status of the information, as to whether it can be disposed of, cycled back into production or remain in archive storage.
- Before the backup media retired and disposed the System Manager should ensure the following facts:
  a) The media no longer contains active backup images;
  b) Unauthorized person may not be read or recovered the media's current or former contents;
  c) System Manager will ensure the physical destruction of media prior to disposal.

- Daily Backups stored in Storage System. Hence it can be kept approximately 250 days. If any wing required daily backup for later use may be arrange any secondary media in their own hand. A full backup of all the data base in monthly base will be kept at Computer centre as a secondary recovery system as long as any physical destruction of the media occurred.
- CCTV backup only stored for 30 days. It may have varied two or three days depends on storage space allotted for CCTV.
- Log details related with internet usage, Wi-Fi, firewall system etc. may be available for 1 year at University. If backup system available, it can be stored up to 3 years.
- All relevant department backups should be verified periodically and report on its a storage ability to recover data (relevant for Logical/Cloud-based backup procedure).
- The Wi-Fi, internet credentials and official mail ids are removed by getting request from the corresponding officials at the time of retirement or University transfer of an employee.