POLICY TITLE: Data Security

DATE DRAFTED: 11th December 2009

DATE APPROVED:

DATE REVISED:

PURPOSE

The purpose of this policy is to identify and disseminate the University's framework and principles that guide institutional actions and operations in generating and sharing confidential information. Information assets in all forms and throughout their life cycle will be protected through information management policies and actions that meet applicable regulations, laws and contractual requirements to support the University's mission, vision, core values and philosophy.

SCOPE

This policy applies to all staff, students, vendors, volunteers, interns, contractors or other affiliates of Makerere University with access to confidential institutional information. The scope of the information includes all electronic data elements, which belong to the University and that satisfy one or more of the following criteria:

- The data is relevant to planning, managing, operating, or auditing a major administrative function of the university
- The data is referenced or required for use by more than one organizational unit
- The data is included in an official university administrative report
- The data is used to derive a data element that meets these criteria

USER RESPONSIBLITY

The electronic data of the university either reside on central university servers or on desktops, laptops and other mobile devices belonging to individual users. In either circumstance, users must be aware of policy issues governing their protection and access. The following policy statements thus apply:

1. All University data as specified in section 4.1 should be stored on centrally maintained corporate networked disc storage. In the event that such data is stored on user desktops, laptops and other mobile devices, it is the responsibility of the user to ensure its security, confidentiality and integrity in respect to this policy such as regular backup, password protection etc.

2. All access to data stored in central administrative databases must be through standard interfaces provided for by the various information systems (example *ITS* as staff interface to ARIS/FINIS/HURIS; *iEnablers* as students/lecturer interface to ARIS). Any attempt to gain access through any other means other than those sanctioned by the university constitutes security breech.

3. Requests for Access to all administrative data and the central systems in general must be authorised by the relevant Data Owner (i.e. Academic Registrar for ARIS, University Bursar for FINIS, and Director Human Resources for HURIS) after recommendation by the head of department. The granting of access is effected by the Systems Manager, DICTS.

4. In the event that confidential information is protected by technical security mechanisms (physical or electronic) using safes, passwords etc and these mechanisms fail or are absent, users are obliged to protect confidential information from public access. Lack of security mechanism should not warrant a breach of data security, such as making private information, public.

TECHNICAL STAFF RESPONSIBLITY

The responsibility for protecting all corporate data stored in central university systems (servers, database, network storage etc.) is the mandate of the University Database Manager. The guiding policies for this role are as stipulated in the following Section. It must be noted that each of these policy statements are further detailed in the ***University Backup Policy*** and ***Disaster Recovery Plan***.

5. All University data residing on the central network storage must be backed up on a regular basis. Frequency of backup is determined by the frequency with which the data changes and the effort required to recreate the information if lost. Standards apply to the backup of data from all University systems. Backup must be tested periodically to ensure that they support full system recovery. All restore procedures must be properly documented and tested on a regular basis, at least annually. Backup media must be stored in an off-site location and retrievable within 24 hours, 365 days a year. Off-site is synonymous with “out of the building”. The off-site storage location must provide evidence of adequate fire and theft protection and environmental controls. A site visit should be undertaken on an annual basis and where appropriate, a formal Service Level Agreement (SLA) must exist with the off-site storage provider.

6. Backup and recovery procedures must be developed and maintained for all administrative computing systems and data. The following requirements must be met:

    - Provisions for regular backup of data residing on the system.

- Storage of backup media at a location remote from the processing centre.
- Approved Disaster Recovery Plan written and implemented to cover situations in which hardware and/or software cannot run in its normal environment.

7. Data owners in their role as custodians of University data are responsible for defining and documenting the length of time data must be retained. The retention period, legal requirements, responsible parties, and source of legal requirement should be specified. DICTS is responsible for ensuring that these requirements are adhered to.

8. Database management software used for administrative application development should meet the following features:

    - Ability to designate the database “private” or “public”
    - Access capabilities which can be restricted at the table and field levels
    - Access capabilities which can be restricted based on user, time of day, day of week
    - Audit trails/journals which record important system activity
    - Control checkpoints