Section	Information Technology Services
Contact	Chief Information Officer

5. Access to data is on the basis of the business needs of the University to enable the University to achieve its mission. Employees will have access to the data needed to perform their responsibilities. Access to Personally Identifiable Information (PII) will have all required access controls applied and managed. Access does not mean privileges to modify or disclose the data.

6. The University's institutional data may often reside in university records or may of itself be a university record. The retention and disposal of this type of institutional data must be managed in accordance with the Records Management Policy and the approved Retention and Disposal schedule. Before decisions are made concerning data retention and data archiving, the appropriate Data Stewards must be consulted.

7. All institutional data must be managed and as such must have representation by all the groups mentioned below. These are delegated responsibilities.

   Data Leaders are representative of the University's Senior Leadership Team (SLT) and are accountable and responsible for:

   - providing strategic guidance for the institutional data in their area of responsibility
   - acting as a champion for data management and data-related initiatives
   - approving the policies associated with managing the University's data specific to a functional area
   - assigning Data Custodians.

   The Data Custodian is the authoritative head of the respective Faculty, School, Division or Unit within the University and is accountable and responsible for:

   - assigning Data Stewards for data in their area of responsibility and allowing time for them to complete relevant tasks
   - the business use of the data asset, and is given the authority to collect, create, retain, and maintain the data within their assigned area of control, coupled with the responsibility to protect it on behalf of the University
   - authorising and reviewing the security classification of Information
   - authorising access to assigned data and its usage in other systems
   - identifying and registering Personally Identifiable Information (PII) contained in data sources
   - ensuring that data is fit-for-purpose including defining data quality levels, metrics, business rules and facilitating data integration.

   The Data Steward(s) are individuals responsible for the day-to-day management of the data, including o8a within their assi