GRAMBLING
STATE UNIVERSITY
GRAMBLING, LOUISIANA

Policy# 41004

DATA CLASSIFICATION POLICY

Effective Date: August 22, 2019
Responsible Office: Office of Distance Learning
Division: Academic Affairs

I. PURPOSE/OBJECTIVE

To protect the confidentiality, integrity and availability of university data and to comply with local, state and federal regulations regarding privacy and confidentiality of information in compliance with The Office of Distance Learning’s Data Classification Policy.

II. STATEMENT OF POLICY

All members of the university community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by the University, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form).

A. RESPONSIBILITY FOR DATA MANAGEMENT:

Departments are responsible and should carefully evaluate the appropriate data classification category for their information.

B. DATA CLASSIFICATIONS

Data owned, used, created or maintained by the University is classified into the following three categories: Public, Official Use Only and Confidential.

1. Public Data is information that may or must be open to the general public. It is defined as information with no existing local, state, national or international legal restrictions on access or usage. Public data, while subject to University disclosure rules, is available to all members of the University community and to all individuals and entities external to the University community.

2. Official Use Only Data is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Official Use Only Data is information that is restricted to members of

University community who have a legitimate purpose for accessing such data. Official Use only data must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure, must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use, must not be posted on any public website, and must be destroyed when no longer needed subject to the University’s Records Management Policy and electronic storage media shall be sanitized appropriately by overwriting or degaussing prior to disposal. Disposal of electronic equipment must be performed in accordance with the ODL’s Data Classification Policy.

The ITC Security Administrator must be notified in a timely manner if data classified as Confidential is lost, disclosed to unauthorized parties or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of the University's information systems has taken place or is suspected of taking place.

C. VIOLATIONS

Violations of this policy can lead to disciplinary action up to and including dismissal, expulsion, and/or legal action. Any known violations of this policy are to be reported to the university's Office of Distance Learning or Office of Academic Affairs.