



# IT Change Management Policy

Policy number: 800 -IT-5  
Policy owner: ITS

Date of initial publication: December 19, 2022  
Date of last tracked, to support continuity of IT services, and reduce negative impact on services and Users.

## SECTION II. SCOPE AND APPLICABILITY

This policy applies to all SITI systems (academic, administrative, and support systems), and all users of these systems.

## SECTION III. DEFINITIONS

Unless otherwise specified, the following definitions apply:

- a. Category III – Orange Data: Data that is sensitive but not classified as Critical Data. This includes data that is subject to FERPA, but not HIPAA, and data that is subject to the Freedom of Information Act (FOIA).
- b. Category IV – Red Data: Data that is highly sensitive and requires the highest level of protection. This includes data that is subject to HIPAA, and data that is subject to the Privacy Act.
- c. Change Advisory Board: A group of individuals who are responsible for reviewing and approving changes to IT systems.
- d. Change Control: The process of managing changes to IT systems, including the identification, analysis, and implementation of changes.
- e. Emergency Change: A change that is implemented immediately to address a critical issue or security threat.
- f. Normal/Standard Change: A change that is implemented through the standard change management process.

- . Planned Change a -a a a a , a , a  
a .
- . Routine Level Change a a a a a a , a  
a a a , a .
- . SaaS (Software as a Service) a b a a a  
a a b a 3 a . E a , M O 365, Ca a a  
Q a .
- . Tier 0 and Tier 1 Systems a a a 6.5 ( )-1.2 ( )- ( )-126 ( )



