Information Technology Services
Security Control Standards

NIST Control Family – Access Control

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVISION DATE	NEXT SCHEDULED REVIEW DATE
AC-5	Separation of Duties	P1	4/15/2020	4/15/2021

I. Statement

This Control addresses how information resource owners and custodians shall ensure that principle of Separation of Duties is implemented to prevent errors and/or fraud. It also provides procedures for appropriately managing the creation, use, monitoring, control and removal of accounts with special access privileges based on the duties of staff. Separation of Duties is achieved by disseminating the tasks and associated privileges for a specific security process among multiple users and chains of command. This ensures no single individual or organization should be in a position to both perpetuate and conceal irregularities resulting in unauthorized or unintentional modification or misuse of the university's information resources. Technical support staff may have special access account privilege requirements in comparison with typical users.

II. Applicability

The owner of an information resource, or designee, is responsible for identifying the relevant information technology roles for custodians or users of their information resources.

Separation of duties must be implemented such that operational information resource functions are separated into distinct jobs to prevent a single person from harming a development or operational information resource or the services it provides, whether by an accidental act, omission, or intentional act.

III. Risk Statement

The lack of user segregation of duties may result in unauthorized or unintentional modification or misuse of the organization's information assets.

IV. Implementation

Each individual who uses administrator or special access accounts shall use the account or access privilege most appropriate for the requirements of the work being performed (e.g., user account vs. administrator account).

Custodians shall maintain a list(s) of personnel who have administrator or special access accounts for information resources. System owners or management with appropriate oversight shall reviewed the list(s) at least annually.