

Policy Directory

Responsible Division: Finance and Administrative Services

Responsible Office: CITS

Issue/Revision Date: 02/20/2019

**Retention and Disposition Policy**

Policy:

**Purpose**

This policy establishes the retention period of data within systems owned by CITS and for which CITS is responsible for the disposition of deleted data. This includes system access and log files that are a routine record of events on systems.

**Scope**

This policy addresses user data that has been deleted by the user from the system as well as system access and log files that provide hardware or operating system event data used to diagnose problems. This policy does NOT include retention of data records not owned by CITS such as financial records, Human Resource documents, student records, and health data which are governed by specific legal requirements and under the purview of those departments.

**Roles**

The retention of data and determination of useful retention of system logs is determined by system administrators under the direction of the Director of Enterprise Architect. System administrators and database administrators are responsible for the execution of retention and adherence to the schedule.

**Record Types**

This policy addresses electronic data generated by systems in various formats (.txt, .tar, .zip, etc.), faculty and staff deleted email in Outlook Exchange and all systems provided for the user for the storage of data. For user-generated data, retention refers to the length of time a document is available for recovery once deleted by the user from the system.

**Litigation Hold**

When CITS receives a litigation hold for electronic data, the data and email, as well as any associated backups as of the day of the hold, are copied and quarantined. Any backup retention policies that would delete files older than 30 days are removed so that files are retained. At the time, the University is required to supply electronic documents, data from the frozen copies and any relevant data from the intervening period. Circumstances from each case will dictate the parameters of the data required.

**Data Retention**

CITS has a document outlining the retention of system logs, responsible party and location.

User data, for the purpose of this document, refers to data or emails that have already been deleted by the user. User data is retained via backup copies for a period of 5 years. When an employee either retires, is terminated, or resigns, his/her Active Directory account and INB (Banner) will terminate on the date that the employee is no longer employed by the University. Data that resides on user desktops/laptops is retained until that computer is decommissioned or another employee takes over the workstation, then that computer is reimaged to erase all previous data. Data that resides on CITS-provisioned storage (shared network drives) is retained for 120 days beyond deletion.