The Division of Information Technology
University Information Security Standards

NIST CONTROL FAMILY

AUDIT AND ACCOUNTABILITY CONTROLS

PROCEDURE NUMBER	CONTROL NAME	REVIEW DATE
IT.0300	Content of Audit Records	07/09/2019

I. STATEMENT

Texas A&M University – Kingsville (TAMUK) information systems must produce audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user associated with the event if applicable.

II. APPLICABILITY

This procedure applies to all TAMUK information resources. The intended audience for this procedure includes all information resource owners, custodians, and system administrators.

III. IMPLEMENTATION

Information systems must be configured to provide centralized logging managed by iTech.

Monitoring is optional for development and test servers.

Information systems must capture:

a) All logins;
b) All logouts;
c) Changes to automated security rules, e.g., firewall settings;
d) Privilege escalations (e.g. sudo).
e) Establishing service accounts;
f) Configuring access authorizations (i.e., permissions; privileges);