West Texas A&M University

The Division of Information Technology
University Information Security Standards

NIST CONTROL FAMILY
AUDIT AND ACCOUNTABILITY CONTROLS

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVIEW DATE
AU-3	**Content of Audit Records**	**P1**	**07/09/2017**

I. STATEMENT

West Texas A&M University 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, where 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.

II. APPLICABILITY

This Control applies to all West Texas A&M network information resources. The intended audience for this Control includes all information resource owners, custodians, and users of information resources.

III. IMPLEMENTATION

Information systems must be configured to provide centralized logging managed by IT. Information systems must have endpoint security properly installed and configured. When information systems allow, proper group policies must be applied.

Monitoring is optional for Dev/Test servers.

Information systems that have update services are managed by IT by default. Automatic updating can be configured on a case by case basis.

Primary Custodians shall ensure that at least the following events are captured in audit logs:

a) All logins;
b) All logouts;

c) Changes to automated security rules, e.g., firewall settings, anti-virus settings, intrusion detection parameters;
d) Changes to audit and logging settings;
e) Privilege escalations (e.g. sudo).
f) System administration;
g) Establishing system accounts;
h) Configuring access authorizations (i.e., permissions; privileges);