UF UNIVERSITY of FLORIDA
Information Technology

Standard: Auditable Events and Record Content

Purpose:

In order for Information Technology activity and audit logs to be useful, they must record sufficient information to serve the operational needs, preserve accountability, and detect malicious activity. This standard defines these events and content.

Standard:

1. All information systems will produce audit records for at least the following events:
    a. System startup and shutdown
    b. User logon and logoff
    c. Privilege escalation
    d. Account creation
    e. Password changes
2. Information systems should produce audit records for the following event types, depending on system capabilities:
    a. Starting and stopping of processes and services
    b. Installation and removal of software
    c. System alerts and error messages
    d. System administration activities
    e. Access to and modification of Restricted Data
3. Log records will include at least the following elements:
    a. Identifier of the system that generated the event
    b. Timestamp of the event

c. The action or type of event and any relevant data

d. Success or failure of the action

e. The user associated with the event

f. Remote address, if the event occurs over a network connection