29.01.99.E1.03  Information Resources – Account Management

Approved January 20, 2004
Revised November 21, 2006
Revised September 15, 2009
Revised June 5, 2013
Next Scheduled Review: June 5, 2016

Supplements TEES Rule 29.01.99.E1

Standard Administrative Procedure Statement
The scope of this procedure is to create, control, and monitor all computer accounts.

Reason for Standard Administrative Procedure
The purpose of the account management procedure is to establish the process for the creation, monitoring, control and removal of user accounts.

Procedures and Responsibilities

1. CONTROLS AND RESPONSIBILITIES

1.1 An approval process is required prior to granting access authorization for an information resource. The approval process shall document the acknowledgement of the account holder to follow all terms of use (see TEES SAP 29.01.99.E1.02, Acceptable Use) and the granting of authorization by the resource owner or their designee.

1.2 Each person is to have a unique logon ID and associated account for accountability purposes. Role accounts (e.g., guest or visitor) are to be used in very limited situations, and must provide individual accountability when used to access mission critical and/or confidential information.

1.3 Access authorization controls are to be modified appropriately as an account holder’s employment or job responsibilities change.

1.4 Account creation processes are required to ensure that only authorized individuals receive access to information resources.

1.5 Processes are required to disable logon IDs that are associated with individuals that are no longer employed by, or associated with TEES. In the event that the access privilege is to remain active, the division (e.g., owner, division head) shall document that a benefit to TEES exists.

1.6 All new logon IDs that have not been accessed within a reasonable period of time from the date of creation will be disabled.
1.7 All logon IDs having access to mission critical and/or confidential resources that have not been used/accessed within a period of six months, shall be disabled. Exceptions can be made where there is an established division procedure. These actions shall be reviewed and approved by the division head or designee. Documentation shall be maintained by the system administrator or other designated responsible official.

1.8 Passwords associated with logon IDs shall comply with TEES SAP 29.01.99.E1.14, Password/Authentication.

1.9 System Administrators or other designated staff:

1.9.1 Shall have a documented process for removing the accounts of individuals who are no longer authorized to have access to TEES information resource.

1.9.2 Shall have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.

1.9.3 Shall have a documented process for periodically reviewing existing accounts for validity.

Related Statutes, Policies, or Requirements
TAMU SAP 29.01.99.M1.03, Information Resources – Account Management

TEES Rule 29.01.99.E1, Security of Electronic Information Resources

TEES SAP 29.01.99.E1.02, Information Resources – Acceptable Use

TEES SAP 29.01.99.E1.14, Information Resources – Password/Authentication

Contact Office
Information Technology Services
(979) 847-8585