GENERIC USER ACCOUNT STANDARD (SEC-S002)

Austin Peay State University

1.0 OBJECTIVE:

1.1 Austin Peay State University (APSU) is responsible for ensuring the confidentiality, integrity, and availability of data stored on its systems. This standard, operating under University Policy 4:042 Information Security and Data Classification, defines and establishes governance for the creation and maintenance of generic user accounts for network, system, application, and email access on all of APSU's systems.

2.0 RESPONSIBILITY:

2.1 Director, Information Technology Security

3.0 APPROVAL AUTHORITY:remo

3.1 Chief Information Officer

4.0 SCOPE:

4.1 This standard applies to the use of generic login and generic email accounts by the university. Users are prohibited from accessing other users' accounts by APSU Policy 4:029: Acceptable Use of Information Technology Resourses. However, in some situations and to support the functionality of a business process, system, device, or application, a shared account may be justified.

5.0 DEFINITIONS:

5.1 Generic login account – any non-person account that may allow multiple users to use a single account to authenticate to the network, application, or other university technology resources. These accounts will not have email access.

5.2 Generic email account – any email account used by a department or unit that does not uniquely identify an individual person or people.

6.0 REQUIREMENTS:

6.1 Generic Login Accounts

a. Generic login accounts will be restricted as much as possible and will be assigned the least privileges required to do the job they are intended for. Because these accounts will not have email access, they will not be visible in the campus directory.

b. Generic login accounts will not be approved for access to university financial or credit card information or to personnel records.

c. The generic login account must be protected by multi-factor authentication and will follow the normal user password account change policy. Exceptions to this requirement must be approved by the IT Security director or CIO.

d. The generic logon account is owned by a department or unit and must have a designated owner who is responsible for the account from that department or unit.

e. Request for a generic login account is made with the Generic Email Account Request and must have a short description of the business case requiring the creation of the account. Requests for a generic login account will be approved or disapproved by the Information Technology Security Director.

f. The password must be changed whenever the owner or any other user of the generic logon account changes.

g. The owner of the generic login account is responsible for periodically reviewing the generic login account for need and usage. If the account is determined to not be needed, the owner of the generic login account must request to have the account disabled.

h. Generic login accounts will be audited annually by the Information Technology Security department for appropriateness of access and ongoing need.

6.2 Generic Email Accounts

a. A generic email account must be configured so that it can only be used by delegate access. A user must not be able to directly enter the username and password (interactive login) to gain access to the generic email account. Exceptions must be approved by the IT Security Director or CIO, must be protected by multifactor authentication and will follow the normal user password account change standard.

b. Additional delegate access to the account email must be requested by the account owner to the IT Help Desk (GovsTech).

c. A retention policy of 30 days will be set for messages in a generic email account. (?)

d. The generic email account is owned by a department or unit and must have a designated owner who is responsible for the account from that department or unit.

e. Request for a generic email account is made with the Generic Email Account Request and must have a short description of the business case requiring the creation of the account. Requests for a generic email account will be approved or disapproved by the Information Technology Security Director.

f. The owner of the generic email account is responsible for periodically reviewing the generic email account for need and usage. If the account is determined to not be needed, the owner of the generic login account must request to have the account disabled.

g. Generic email accounts will be audited annually by the Information Technology Security department for appropriateness of access and ongoing need.

7.0 ASSOCIATED DOCUMENTS:

7.1 4:042 Information Security and Data Classification Policy

7.2 4:029: Acceptable Use of Information Technology Resourses

8.0 RECORD RETENTION TABLE:

Identification	Storage	Retention	Disposition	Protection
OITManagers Network Share	Electronic	Perpetual	Delete	Electronic Back-up

9.0 REVISION HISTORY:

Date:	Rev.	Description of Revision:
6/28/2021		Initial Release

*** * * E n d o f S t a n d a r d * * ***