Information Security Standard 9.2b

GENERIC USER ACCOUNT STANDARD

Initially Approved: Dec. 3, 2013
Revised: May 10, 2018
Revised: July 1, 2020 (as the Generic User Account Standard)
Administering Office: Office of the CIO

I. STANDARD STATEMENT

This standard, operating under University Policy 117 Information Security, defines and establishes governance for the creation and maintenance of generic user accounts for network, system, application, and email access on all of Western Carolina University's systems.

Security depends on personal accountability. Generic accounts for personal or departmental usage will only be allowed with a specific business need and written justification. The Division of IT will work with users requesting such accounts to discuss alternatives before creating a generic account.

II. SCOPE AND APPLICATION OF THE STANDARD

This standard applies to the use of generic login and generic Email accounts by the University.

III. DEFINITIONS

"Generic login account" shall mean any non-person account that may allow multiple users to use a single account to authenticate to the network, application or other university resources. These accounts will not have email access, i.e. kiosk and check-in accounts. A generic login account used to gain computer access will not be given an email address.

"Generic Email account" shall mean any Email account used by a department or unit that does not uniquely identify an individual person or people.

IV. GENERIC USER ACCOUNT STANDARD

A. Generic Login Accounts

1. 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.

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

3. The generic login account must be protected by multi-factor authentication and will follow the normal user password account change standard. Additionally, the password must be changed whenever the owner of this account changes or any user changes.

4. The generic login account is owned by a department or unit. It is requested and renewed via the Non-person Access process.

B. Generic Email Accounts

1. 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 to this must be approved by the CIO, must be protected by multi-factor authentication and will follow the normal user password account change standard.

2. Additional delegate access to the account Email must be requested by the account owner to the IT Help Desk.

3. A retention policy of 30 days will be set for messages in a generic Email account.

4. A generic Email account is owned by a department or unit. It is requested and renewed via the Non-person Access process.

V. REFERENCES

International Standards Organization (ISO/IEC 27002, 9.2, User Access Management)

University Policy 117 Information Security