



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.
- 
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 multifactor 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.

International Standards Organization (ISO/IEC 27002:2022, Clause 5 Organizational Controls)

[University Policy 117 Information Security](#)