Technical Controls:

The technical controls have sections as per the security requirements and have a list of documents adhering to security standards.

Documents are several years outdated and require review.

1. Unique User Identification
   1. TS0005, *User Account and Password Management*

Recommendations:

1. Detailed documentation for account distribution along with password confidentiality and user responsibility:
   1. Users must not allow another user to use their unique user identification or password.
   2. Users must ensure that their user identification is not documented, written, or otherwise exposed in an insecure manner
   3. If a user believes their user identification has been comprised, they must report that security incident to their manager.
2. Documents that meet requirements for Password Best Practices Policy:
   1. Passwords must be a minimum of eight characters in length
   2. Passwords must not be words found in a Dictionary
   3. Passwords must not include easily guessed information such as personal information, names, pets, birth dates, etc.
3. Change of the password periodically (every 90 days)
4. Disabling the user identifier after 90 days of inactivity.
5. Authenticator management:
   1. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation
6. Transmission Security
   1. TS0006, *Electronic Communications and Data Transmission Policy*
   2. TS0006.02, *Electronic Communications and Data Transmission Standard*

Recommendations:

1. Guidelines for a variety of data transmission methods and addresses the need of authentication, authorization and encryption in each.
2. The transmission permission of UFHSC to an outside entity via an email or messaging system Policy:
   1. The sender and receiver are able to implement a compatible encryption mechanism.
   2. The receiving entity is aware of the transmission and is ready to receive said transmission.
3. Additional Requirements for Electronic Transmissions: All encryptions mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.