ADMINISTRATIVE MEMO #22-01

To: All Registered Users of CSA IT Systems

From: Preetha Agrawal, Information Technology Director

Date: January 5, 2022

Subject: CSA system password requirement changes

Please be aware of the following changes to CSA IT systems to which you have access. These changes are necessary to conform with IT security standards and mitigate risks of unwanted access to our system.

User Password Management Responsibilities

Expired Passwords and Password Resets:

- CSA system users must change passwords every 42 days (90 days for Service Fee Directory users).
- All accounts without activity after 90 days (365 days for Service Fee Directory users) are disabled and require new Access Requests to establish access.
- The "3-strikes" security feature for accounts locks an account after three (3) consecutive incorrect password attempts. The "3-strikes" feature applies to all OCS information systems applications.

Strong Passwords:

All Users will utilize a strong password that:

- Is at least eight (8) characters, maximum length of 15 characters;
- Contains at least one numeric and one special character;
- Contains a mixture of at least one uppercase and one lowercase letter; and
- Cannot be reused.

Users of OCS information systems:

- May not share passwords;
- May change passwords at will, but no more than once every 24 hours; and
- Must change compromised passwords.

Lost, Stolen, or Compromised Passwords

Users must:

- Immediately change their password, if compromised.

Please contact the OCS Office at 804-662-9815 or csa.office@csa.virginia.gov in order to reset passwords for locked accounts.