1. POLICY STATEMENT

The Community Solution Education System ("The System" or "System") maintains standards for the creation of strong passwords, the protection of those passwords, and the frequency of changing passwords.

2. PURPOSE

Passwords are an essential aspect of computer and information security. They are the front line of protection for user accounts and systems. This User Password Policy ("Policy") reduces our overall risk and aligns the System with standards we must follow to adhere to compliance requirements, such as those mandated by the Payment Card Industry (PCI). This policy specifies minimum components for a strong password, and requirements for maintaining the privacy of a user account password.

3. APPLICABILITY

All employees of the System and its Member Colleges who access one or more systems in connection with their job function. This includes information systems maintained by the System as well as by vendors and other third parties.

4. PROCEDURES

4.1. Password Complexity Requirements

- Must be a minimum length of at least eleven characters.
- Must contain an upper-case letter, lower-case letter, and a number or special character.
- Passwords may not include any part of the user's name.
- New passwords cannot be the same as any of the user's four previously used passwords.

4.2. Frequency of Change

- Passwords must be changed at least every 90 days.
- Users will receive notice 14 days prior to password expiration along with directions for how to change it.

4.3. Controls

- Accounts are temporarily locked-out after six invalid access attempts.
- Once a user account is locked out, it remains locked for 30 minutes or until a system administrator resets the account. Contact the Help Desk for assistance in unlocking an account.
- Requests to have a forgotten password reset will require verification of the

requester's identity or to use the automated password reset website, accessible from the IT Support Portal (https://helpdesk.tcsedsystem.edu).

- First-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use.

4.4. Protecting Passwords

- All passwords are to be treated as highly sensitive, confidential information, and are not to be shared with anyone else, including co-workers, managers, administrative assistants, IT staff members, or others. Everyone who needs access to a system will be given their own unique password.
- Employees may never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Do not use the "Remember Password" feature of applications (e.g., Outlook, or browsers such as Firefox or Internet Explorer etc.).
- Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information.
- Employees must refrain from writing passwords down and keeping them at their workstations.

4.5. Enforcement

- Violation of this policy may result in the removal of electronic resources access and/or discipline in accordance with the employee handbook.

4. RELATED DOCUMENTS

- Highly Sensitive Data Policy
- Privacy and User Awareness and Training Policy
- Data Incident Notification Policy
- Mobile End-User Device Policy

5. CONTACTS

- Information Technology