

User Identification and Authentication

(AAP recommended policy modified by PCC)

Security Policy:

Access is the ability to interact with a computer system (e.g., use, change, or view). Users of the our computer system must have access to certain information in order to adequately perform their assigned duties, pursuant to their individual job description.

Our practice uses user IDs and unique passwords to control access to our computer system. Our practice expects practice information to be available when it is needed, to be accurate, and to be safeguarded from access by unauthorized individuals. We have established management controls for granting, changing, and terminating access to the computer system. These controls are essential to the security of our information system.

Security Procedures:

Our practice requires all of its employees to have effective and secure user IDs and passwords for access to our computer system. The Security Official or System Administrator will provide oversight of the process for administering and maintaining user IDs and passwords as follows:

All employee passwords, even temporary passwords established for new and temporary employees, should meet the following characteristics:

Be easy for the employee to remember, but difficult for an unauthorized user to guess.

Be at least six characters in length.

Consist of a mix of alpha and at least one numeric or special character.

Be easy to type quickly.

Not be portions of associated account names (e.g., user ID, log-in name).

Not be portions of the employees name (e.g., first name or last name in any form).

Not be the employees spouse, children, or pets name in any form.

Not be information easily obtained about the employee (i.e., license plate numbers, telephone numbers, social security numbers, the brand of his/her automobile, the name of the street he/she lives on, date of birth, email name, etc.).

Not be character strings (e.g., abc or 123)

Assign each employee, including new and temporary employees, a unique user identification (user ID).

Assign each employee, including new and temporary employees, a unique temporary password.

Furthermore, employees are required to select a new password immediately after their initial log on to the computer system using the temporary user ID and password. The

Partner server will make this step happen automatically.

Coordinate changing passwords at least every ____ months. Previously used passwords will not be re-used within x time period (e.g. every 2 yrs. or 4 password changes).

Review the Partner Server Account Report. Make sure that every active user ID has a valid password. Make sure that the user IDs for all former employees and contractors have been disabled. Make sure that all active user IDs change their passwords as prescribed above.

Passwords will not be embedded in automated programs, utilities, or applications, such as: autoexec.bat files, batch job files, terminal hot keys.

Instruct employees to keep passwords confidential. Employees will be instructed to not share his/her password with anyone, including other employees, temporary employees, and contractors.

Remove default and service passwords from new computer systems and assign proper passwords to all computer systems immediately upon installation at our office. Proper passwords adhere to the above guidelines.

Passwords will not be visible on a data entry screen or display or documented in writing in any form (e.g., on a post-it note, on a message pad, on a calendar, on personal digital assistant (PDA), etc.).

Change passwords and disable user accounts promptly upon employee termination, including temporary employees, regardless of whether the termination was mandatory or voluntary. Users should immediately change their password if they suspect it has been compromised.