	Administrative Policies And Procedures Tennessee Supreme Court Administrative Office of the Courts	Index #: 1.04	Page 1 of 2
		Effective Date: May 13, 2024	
		Supersedes: New Policy	
Approved by:	Chief Justice Holly Kirby and Director Michelle J. Long		
Subject:	Password Policy		

I. Authority: T.C.A. §§ 16-3-803 & 805

II. Purpose: To safeguard against unauthorized use and access that establish the requirements for creating strong complex passwords, the protection and management of passwords, the frequency passwords are to be changed, and password privacy.

III. Application: This policy applies to all users who have been provided access rights to ITSD resources, an AOC email (i.e., an email address that ends in @tncourts.gov) and/or internet via agency issued network or system User ID's.

IV. Definition:

Network – method of interconnecting several computers for the purpose of sharing data, resources, and/or file storage.

V. Policy: Users will be required to reset their passwords, including network and/or email passwords, every 90 days. If network password is not reset within 90 days, user will be locked out of the network, and they will need to contact the AOC Help Desk at AOCHelpDesk@tncourts.gov or at (615) 532-9503 or (800)-448-7980.

VI. Effective Date: This policy will become effective on the date the user (as set forth in Section III) is migrated from GroupWise email to Outlook email.

VII. General Password Construction Guidelines:

A. Strong password requirements include:
- Must be a minimum of twelve (12) characters or more in length;
- Must contain at least 1 uppercase letter (A-Z);
- Must contain at least 1 lowercase letter (a-z);
- Must contain at least 1 or more numbers (0-9);
- Must contain 1 special character (@, #, $, %, ^, &, or *); and
- Must be unique and not contain any of the last 6 passwords

B. Additionally, the construction of passwords should **not**:
- Include a word in any language that contains slang or jargon, etc.
- Be based on personal information, username, names of family, birthdates, etc.
- Re-use a currently active password (i.e. banking, shopping, Facebook, etc…)

C. Weak passwords have the following characteristics:
   - Forms a word found in a dictionary or is a common usage word such as:
     - Names of family, pets, friends, co-workers, fantasy characters, etc.
     - Computer terms and names, commands, sites, companies, hardware, software.
     - The words AOC, Justice, Judge, Law, or department name.
     - Birthdays and other personal information such as addresses and phone numbers.
     - Word or number patterns like aaabbb, qwerty, 123321.
     - Uses any of the words referenced above spelled backwards.
     - Uses any of the above preceded or followed by a single numeric digit (e.g. password1, 1password).