



Cyber Tree Systems

A Business IT Solution Company

POLICY NAME	Password		
DATE OF LAST REVISION:	9/4/2003	VERSION NO.	1.43
ADMINISTRATOR RESPONSIBLE	Kevin McKnight		

Purpose

This policy provides the requirements for creating and retrieving usernames and passwords (i.e., credentials) for use by employees that require authentication and access resources on CTS's network.

These credentials are meant to restrict access based on privileges as assigned by the IS/IT/InfoSec department and can be compromised when the credentials are improperly stored.

Scope

This policy applies to all users that will access CTS resources locally and through VPN/remote access.

Policy Statement

- General Guidelines

To maintain the security of CTS's internal resources, access by user must be granted only after authentication on one of 3 Active Directory Domain Controller servers.

- Specific Requirements

- Username & Password Creation Retention
 - Usernames will consist of an employee's first initial and last name.
 - Passwords will be 8 to 12 characters in length.
 - Passwords will be a combination of upper- and lower-case alphanumeric values, which can include common symbols.
 - Passwords will be valid for 45 days.
 - A minimum of 12 passwords will be kept in the system's history, not to be repeated.
 - Passwords must be stored using reverse encryption.
- Retrieval of Usernames and Passwords
 - If a user forgets his/her password, they should contact the CTS technical support center (TSC) and request their password reset. The TSC will not have access to a user's password and therefore be unable to directly access a user's account without creating an audit log entry.
 - When a member of the CTS TSC resets a user's password, an entry will be made into the system audit logs and said logs will be maintained for a period of one (1) year.
 - Usernames consist of a standard format, as previously stated of first initial and last name. In the event of duplication, the user's first name initials will be used until such that duplication will not exist.

Enforcement

Any employee found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

Terms and Definitions

Define any acronyms, jargon, or terms that might have multiple meanings.

TERM	DEFINITION
Credentials	Something you know (e.g., a password or passphrase), and/or something that identifies you (e.g., a username, a fingerprint, voiceprint, retina print). Something you know and something that identifies you are presented for authentication.
Entitlement	The level of privilege that has been authenticated and authorized. The privileges level at which to access resource
Executing Body	The series of computer instructions that the computer executes to run a program.
Hash	An algorithmically generated number that identifies a datum or its location.
Name Space	A logical area of code in which the declared symbolic names are known and outside of which these names are not visible.

Revision History

Revisions made 9/4/2023
