ST. CLAIR COUNTY COMMISSION
POLICY # 74
MFA NETWORK SECURITY POLICY

NETWORK SECURITY POLICY – MULTIFACTOR AUTHENTICATION (MFA)

I. **Overview**

There are many ways an individual could gain unauthorized access to the St. Clair County computer network and information system. The St. Clair County Technology Division has enacted a common method of protection against unauthorized access by use of multi-factor authentication (MFA). MFA is a security process whereby users must provide at least two different authentication factors to verify their identities and access their accounts. This process ensures better protection of both a user's personal information, credentials, and other assets, while also improving the security around the resources the user can access. MFA should be universal for all privileged or administrator accounts.

II. **Purpose**

The purpose of this policy is to provide guidelines for MFA connections to St. Clair County network and information systems on and off county property. These standards are designed to minimize the potential security exposure to St. Clair County from damage which may result from unauthorized access and use of county technology resources. MFA adds a critical / basic layer of security for information networks.

III. **Scope**

The policy applies to all employees of St. Clair County and St. Clair County Sheriff's Office and all other persons utilizing the St. Clair County computer network. St. Clair County Information Technology staff will assist all applicable users with set-up and troubleshooting of MFA protocols.

Any users that access their County-issued Microsoft account (email, OneDrive, OneNote, etc.) on a mobile device (County owned or personal) or any off-site computer that is not connected via VPN (Virtual Private Network) will be required to use MFA to authenticate.

IV. **Authentication Factors**:

A. **Username and Password:** Users will use their username and password as their initial form of authentication on their desktop / laptop computer seeking access to the St. Clair County computer network.

In addition, all Users will select one (or more if desired and/or necessary) of the following Authentication Factors:

B. **Text Messaging (SMS)**: Users will receive a one-time access code via text message to their registered mobile phone number.
C. **Microsoft Authenticator**: Users will use the Microsoft Authenticator app to generate a time-based one-time password (TOTP) or approve authentication requests through push notifications.
D. **Voice Call**: Users will receive an automated voice call to the registered phone number and will be prompted to press # on their keypad.

V. **Configuration**:

a. Subject to the below and in addition to the Username and Password, Users are required to select and configure at least one authentication method: text message, the Microsoft Authenticator app on a cellular device, and/or voice call.
b. Depending on the authentication method selected by the User, a User will register their mobile phone number for text messaging, their desk phone number for voice calls, and/or install the Microsoft Authenticator app on their smartphone device.
c. The St. Clair County IT department will provide guidance and support for setting up and configuring the applicable MFA.
d. All users will be required to setup MFA initially, however, users that only access their county-issued Microsoft account from within the county network will not be prompted for MFA.
e. Once a User has been authenticated on a device, they will be allowed to login to their account until the authentication token expires. After the authentication token expires, they will be required to reauthenticate using MFA.
f. Users may be required to reauthenticate using MFA due to the 90 day password expiration policy in place.

VI. **User Training and Awareness**:

a. All Users will receive training on how to set up and use MFA, including step-by-step instructions for configuring voice calls, text messaging, and/or Microsoft Authenticator.
b. Regular reminders and updates will be provided to ensure that users remain aware of the importance of MFA and how to use it securely.

VII. **Exceptions and Overrides**:

a. Exceptions to the MFA requirement may be granted on a case-by-case basis, following an approval process involving IT security and management.
b. Overrides may be granted for emergency access situations, with additional verification steps required to ensure security.

VIII. **Monitoring and Auditing**:

a. MFA usage will be monitored, and access attempts will be audited to detect any suspicious activity or attempts to bypass MFA.
b. Any deviations from the MFA policy will be investigated, and appropriate action will be taken to address security concerns.

IX. **Personal or County-issued devices**

a. St. Clair County will not issue smartphones exclusively for users to use as multi-factor authentication devices.
b. If a user chooses to install the Microsoft Authenticator app on a personal device, St. Clair County Technology Division only supports the OTP app, not the smartphone itself. Each user is responsible for making sure his/her smartphone is in working condition. The St. Clair County Commission is not responsible for the cost of repairing or replacing the personal smartphones used as OTP devices or for any costs associated with data plan usage.
c. The St. Clair County Technology Division approved OTP app from Microsoft must be installed and used to generate the OTP.

d. Users are required to secure their county-issued mobile device via electronic security provided by said device, including but not limited to use of a screen lock utility to access their smartphones (e.g., PIN, Password, or biometric such as a fingerprint scan).
e. It is recommended that any users that use their personal device for MFA authentication should utilize a screen lock utility to prevent unauthorized access.

X. **Violations**

Use of MFA protocols for applicable users is prescribed by St. Clair County. Failure to abide by this Network Security Policy may result in disciplinary action, up to and including termination.

By implementing this Network Security Policy, the organization aims to enhance security by requiring users to authenticate using multiple factors, including text messaging, voice calls and Microsoft Authenticator, while also providing flexibility and usability for users accessing the organization's systems and data.

ADOPTED and **APPROVED**, this the 23 day of April, 2024.