

# County of Duplin Multi-Factor Authentication Policy

## Overview

The Duplin County IT Services department has enacted a common method of protection against unauthorized access to the County network and information systems by using 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 accounts. This process ensures better protection of a user's personal information, credentials, and other assets, while also improving the security posture around the resources the user can access. MFA should be universal for all standard user accounts, privileged accounts and administrator accounts.

## Purpose

The purpose of this policy is to provide guidelines for MFA connections to the County of Duplin's network and information systems. These standards are designed to minimize potential security exposure to the Duplin County Government from damages which may result from unauthorized use of county resources. MFA adds a layer of security which helps deter the use of compromised credentials.

## Scope

This policy applies to all individuals and entities, including but not limited to employees, affiliates, vendors, retired employees, and volunteers, that connect to or otherwise utilize the County's network or technology resources. This policy applies to any system accessing County data where MFA can be utilized.

## Definitions

Multi-factor authentication: Using two or more factors to validate the identity of a user.

Factor (of authentication): There are five types of factors used in combination together resulting in multi-factor authentication. They are:

- I. Something the user knows (username and password)
- II. Something the user has (an item the user physically carries with them) example; Phone or any other electronic device.
- III. Something the user is (biometrics: fingerprints, face scan, etc.)
- IV. Somewhere the user is (geo location, on premises)
- V. Something the user does (keystroke patterns)

## **Policy**

All individuals and entities are required to engage in one additional step beyond the normal login process to access County resources and the County network. Registration is required where individuals or entities are seeking to utilize additional electronic devices.

MFA is required on all new accounts created. Previously set-up accounts will be “grandfathered” until MFA has been enacted.

MFA is required for all externally-exposed enterprise or third-party applications, where supported. Enforcing MFA through a directory service is a satisfactory implementation of this safeguard.

MFA is required for remote network access (VPN).

MFA is required for all administrative access accounts, where supported, and on all enterprise assets, whether managed on-site or through a third-party provider.

## **Responsibilities**

It is the user’s responsibility to promptly report compromised credentials to the Duplin County IT Services Department.

It is the user’s responsibility to promptly report a lost or stolen MFA device to the Duplin County IT Services Department.

It is the user’s responsibility not to share authenticated devices.

## **Exemptions**

Any exemptions to this policy must be approved by the Duplin County Manager or the Duplin County IT Services Department Manager.

## **Enforcement**

This policy regulates the use of all MFA access to the County of Duplin’s network and users must comply with this policy.

Services will be disabled immediately if any suspicious activity is observed, and services will remain disabled until the issue has been identified and resolved to the satisfaction of the Duplin County IT Services Department.

Any individual or entity found to have intentionally violated this policy will be subject to loss of privileges. Intentional violation of this policy by a Duplin County employee will result in disciplinary action, up to and including termination of employment.

By choosing to use the County of Duplin’s service, the user agrees to all terms and conditions listed above.