Multi-Factor Authentication (MFA) Policy

1. Purpose

The purpose of this policy is to define requirements for accessing Racine County's network and information systems. These standards are designed to minimize the potential security exposure to Racine County from damages which may result from unauthorized use of Racine County resources. Multi-factor authentication (MFA) adds a layer of security which helps deter the use of compromised credentials.

2. Scope

This policy applies to all members of the Racine County community, with a County-owned or personally-owned computer or workstation used to connect to the County network and technology resources. Many systems in Racine County may be protected by multi-factor authentication (MFA). This policy applies to any system that requires an additional layer of protection, as determined by the Racine County Information Technology Department.

3. Contacts

Direct any general questions about this guideline to your Information Technology Department. If you have specific questions, please contact Racine County Help Desk at ITHelpDesk@RacineCounty.com or at 262-636-3777

4. Policy

4.1 Register a device or alternative contact to provide a secure method for Racine County to contact you during the authentication (logon) process, such as a cellphone that can receive texts, a smart phone app, or a hardware token. If you do not register, you will not be able to use MFA - if MFA is required for that system or service, you will not be able to use that system or service.

4.2 When you attempt to log into a Racine County system protected by MFA, the system will "challenge" you by requesting a secret security code or you will be prompted to "accept" using the smart phone app. If you enter the correct code or accept the smart phone app prompt, you will be allowed into the system. Failed attempts will be handled according to current account policies and procedures referenced in the **Network Connection Policy**.

4.3 The Racine County Information Technology Department will register users and their authentication method for use of MFA. The IT Department will also work with each user to install the Duo Mobile MFA application, if applicable.

4.4 If you have had a device or data stolen, have lost data, or believe that a device has been compromised, contact the IT Help Desk IMMEDIATELY at ITHelpDesk@RacineCounty.com or at 262-636-3777.

5. Policy Compliance

5.1 Compliance Measurement
The Racine County Information Technology Department will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions
Any exception to the policy must be approved by the Racine County Information Technology Department in advance. Please contact: ServerGuys@RacineCounty.com

5.3 Non-Compliance
Any employee who attempts to disable, defeat or circumvent this policy or any other information security policy may be subject to disciplinary action.

6. Vendors

6.1 Vendors used for MFA are: Duo, RSA, Office365

[Racine County Information Technology Department reserves the right to change vendors should it deem necessary.]

7. Related Standards, Policies, and Processes

- Network Connection Policy

ISO/IEC 27002
https://www.iso.org/isoiec-27001-information-security.html

Duo
http://guide.duosecurity.com/enrollment

8. Revision History

Date of Change	Responsible	Summary of Change
October 2019	IT Dept	Updated and converted to new format.