Lawrence County
Multi-Factor Authentication Policy

Overview

The purpose of an Enterprise Multi-Factor Authentication (MFA) Policy is to enable a means of strong authentication for all users with access to information systems resources, while ensuring ease of use and adoption for users. The adoption of an enterprise Multi-Factor Authentication (MFA) Policy will significantly reduce the likelihood of unauthorized access, and provide demonstrated compliance with regulatory and industry mandates.

Scope and Authority

This policy serves as a component of the *Lawrence County Information Systems Security Policy*, and applies to all Lawrence County personnel. contractors, partners, vendors, or anyone authorized access to Lawrence County network resources.

Policy

All offices shall ensure that their employees, and any contracted staff, utilize approved Multi-Factor Authentication (MFA) for local and network access, as well as remote access, for all user accounts on Lawrence County managed systems.

Technology

Lawrence County has deployed a fingerprint-based identification system to serve as a method of specifically identifying individuals. Each system will be configured to utilize this additional method of authentication before granting users both local and network access. The choice of a biological identification method is that users are not required to possess any hardware or technology in order to provide a second factor of identification; only their finger is required. For off-premises remote access, approved users connect via a secure VPN (Virtual Private Network), or other technology for Law Enforcement personnel, are required to utilize a one-time token along with their credentials in order to connect to systems.

Biometric Security

During the biometric enrollment, the registration software takes the image of the end user's finger, and at the point of capture on the client, that image is processed through bio-verification solution's algorithm to convert the image data into a discrete set of encrypted data points that can be used to make comparisons for identity verification. This capture is not usable outside of bio-verification solution, it is not reversible to a visual finger image, and the original capture is deleted from memory and overwritten for security purposes.

Terms and Definitions.

Multi-Factor Authentication (MFA, sometimes referred to as two-factor authentication or 2FA) is a security enhancement that allows you to present two pieces of evidence when logging in to an account.

Local Access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks.

Network Access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses).

Remote Access is a type of network access that involves communication through external networks (e.g., the Internet, and Virtual Private Networks (VPN), or remote control, such as "screen sharing".

Change Control.

This policy is administered by the Director, Information Systems and Technology. Changes to this policy will be submitted by the Director, Information Systems & Technology for approval by the Board of Commissioners.

Revision History.

Effective Date (Approval):	*Revised Date:*	*Author(s) / Editor(s):*	*Reviewer(s):*	*Summary of Changes*
04/12/2022		Gregory Dias Director Information Systems & Technology	Steven Kline, Deputy Director Information Systems & Technology Bruce Outka, County Attorney/Commissioner's Assistant Brenda McGruder, Auditor	Initial policy.

Dated this 12th day of April, 2022.

FOR THE BOARD:

_____

Randall Rosenau, CHAIR

ATTEST:

_____

Brenda McGruder, AUDITOR