KENOSHA COUNTY
BOARD OF SUPERVISORS

RESOLUTION NO. _____

Subject**: Resolution to Approve the Identity and Access Management Policy.**			
Original ☒	Corrected ☐	2nd Correction ☐	Resubmitted ☐
Date Submitted: May 4, 2019		Date Resubmitted	
Submitted By: **Finance/ Admin Committee**			
Fiscal Note Attached:		Legal Note Attached ☐	
Prepared By: Martin Lacock, Chief Information Officer		Signature:	

WHEREAS, Kenosha County is committed to implementing policies to protect the County from forces which may access and potentially compromise the security of all operations managed by Kenosha County Information Technology Department ("IT"); and

WHEREAS, information systems use credentials to grant access to technology and the most common form of credentials is the combination of a username and password; and

WHEREAS, without the proper authorization, identification and authentication controls, the potential exists for information systems to be accessed inappropriately and for the security of those information systems to be compromised; and

WHEREAS, Kenosha County IT systems has established appropriate usage guidelines and defined appropriate controls and standards required for access to Kenosha County systems, technologies, and hosted services through an authentication and credential management system; and

WHEREAS this policy is written to respond to this situation, and address the credentials management, minimum password and auditing requirements; and

WHEREAS, the Finance and Administration Committee has reviewed the Kenosha County Identity and Access Management Policy and found it to be a valuable policy worthy of inclusion with other County policies.

NOW, THEREFORE BE IT RESOLVED, that the Kenosha County Board of Supervisors adopts the Kenosha County Identity and access Management Policy.

Respectfully Submitted:

FINANCE/ADMINISTRATIVE COMMITTEE

	Aye	No	Abstain	Excused
_____	☐	☐	☐	☐

Supervisor Terry Rose, Chair

_____ Supervisor Ron Frederick, Vice Chair	☐	☐	☐	☐
_____ Supervisor Michael Goebel	☐	☐	☐	☐
_____ Supervisor Jeff Wamboldt	☐	☐	☐	☐
_____ Supervisor Jeffrey Gentz	☐	☐	☐	☐
_____ Supervisor Edward Kubicki	☐	☐	☐	☐
_____ Supervisor John O'Day	☐	☐	☐	☐

Kenosha County Identity and Access Management

This policy outlines the use of security systems and credentials used to access Kenosha County systems and data. This policy is to be used in conjunction with other Kenosha County policies.

Purpose

Information system credentials are the only legitimate method by which Kenosha County information systems may be accessed. System credentials can be any combination of methods used to grant access to systems. The most common form of credentials is the combination of a username and password but may also include advanced forms such as multi-factor authentication.

The use of authorization, identification, and authentication controls ensures that only known users make use of information systems. Without authorization, identification, and authentication controls, the potential exists that information systems could be accessed illicitly, and that the security of those information systems can be compromised. Kenosha County is using Microsoft Active Directory and Microsoft Azure AD Premium to centralize account/identity management.

Passwords are the primary form of user authentication used to grant access to Kenosha County's information systems. To ensure that passwords provide as much security as possible, they must be carefully created and used. Without appropriate usage guidelines, the potential exists that passwords will be created that are easy to break. This would allow easier illicit access to Kenosha County's information systems, thereby compromising the security of those systems.

Scope

This Identity and Access Management (IAM) Policy applies to all information systems and information system components as well as all users of all information systems and information system components of Kenosha County. Specifically, it includes:

- Mainframes, servers, and other devices that provide centralized computing capabilities.
- SAN, NAS, and other devices that provide centralized storage capabilities.
- Desktops, laptops, mobile devices and other devices that provide distributed computing capabilities.
- Routers, switches, firewalls, and other devices that provide network or dedicated security capabilities.
- Applications (on-premise and Cloud).
- All devices connecting to, using, or storing Kenosha County data regardless of ownership by Kenosha County, personally owned, or by another company or agency.
- All employees, contractors, and third parties whether employed or working on behalf of Kenosha County on a full-time or part-time basis by Kenosha County.
- All employees of partners.

Policy Statements

General Policy

Kenosha County maintains a variety of Information Systems each requiring some level of credentials and access controls. The County has standardized and centralized credentials management on a combination of Microsoft Active Directory and the Microsoft Azure AD Premium technologies, henceforth known as the Kenosha County Enterprise Credentials System (KCECS). These systems combine to provide a stable and secure enterprise credentials system capable of integrating with many other applications and services through various technologies.

1. **Integrated Authentication**: All systems will be integrated with the KCECS for credentials management, allowing access rights to be centrally managed. If a system is not capable of integration it must adhere to the minimum password policy requirements as documented within this policy. Additionally, it must be listed in the documented authentication systems exemptions within this policy.
2. **Credential Management**: All systems credentials will be actively managed by appropriate administrative staff. Active management includes the acts of establishing, activating, modifying, disabling, and removing credentials from information systems. If a system does not use the KCECS, a designated point of contact will be identified to IT.
3. **Least Privilege**: Credentials are to be constructed in such a way that limits access to the minimum access needed for the performance of the job. Further, accounts shall be created such that no one account can authorize, perform, review, and audit a single transaction to eliminate conflicts of interest.
4. **Access Authorization:** Prior to being granted access to a system, each user must be provided with formal authorization by an appropriate owner of the system or custodian of the data.
5. **Credential Protection:** Credentials are never to be shared and will be stored in a secure manner. Passwords are to be obscured during entry into information system login screens and are to be transmitted in an encrypted format.
6. **Application Programming / Configuration:** Clear text credentials must not be embedded in applications or any other system; use of corporate standard encryption or explicit exception is required and must be documented within this policy.
7. **Credential Sharing:** Credentials are to be individually owned and kept confidential and are not to be shared under any circumstances.
8. **Shared Credentials:** Community or shared credentials are not allowed or authorized unless specifically exempted by Department Director request and approval by the CIO.
9. **Vendor Passwords:** Vendor-supplied default and/or blank passwords must be changed immediately upon installation of the application, device, or operating system.

Minimum Password Policy Requirements

The default password policy for all information systems should meet or exceed the password policy of the KCECS.

If a specific information system is incapable of integrating with KCECS and is unable to meet the minimum password policy a formal exemption must be requested by a Department Director and approved by the CIO. The request should include business justification for ongoing use of the system

and a commitment from the vendor to implement a security and credentials system capable of integrating with KCECS or modifications that will meet the minimum password policy.

- Minimum Password Length: 7 characters
- Maximum Password Age: 90 days
- Minimum Amount of time between password change: 24 hours
- Complexity Requirements: Must include at least 3 of 4 characteristics:
    - Upper case letters
    - Lower case letters
    - Number
    - Special character (e.g. !@#$)
- Password History: 10
- Maximum password attempts before lockout: 3
- Minimum password lockout: 15 minutes
- Account Lockout Duration: 30 minutes
- Account Lockout Threshold: 3 invalid attempts
- Reset Account Lockout Counter: 30 minutes

Auditing Requirements

Standard auditing policies are outlined below. Additional auditing requirements may exist above and beyond these stated practices; the additional policies will be documented within individual policies.

System	Frequency	Description	Responsible Party
Kenosha County Enterprise Credentials System (KCECS) – Active Directory	Quarterly	Review all accounts inactive for at least 3 months	IT
AS/400 Accounts	Quarterly	Review all accounts inactive for at least 3 months	IT
Financial System Access	Quarterly	Review financial system access and authorities	Finance
Privileged System Access	Semi-annual	Review individual systems for ongoing access requirements	IT and Responsible Department / Division
Privileged Account Access	Monthly	Review all access attempts to privileged accounts in Secret Server	IT

Elevated Credentials

IT maintains systems and applications for the entire County. Many of these systems contain sensitive or confidential information; some may be protected through compliance, policy, or regulations. IT must

ensure it observes proper security policy ensuring elevated access is only granted on an as-needed basis for the purposes of providing support to our customers.

IT will observe all appropriate protections such as those outlined by the Criminal Justice Information Systems (CJIS) policies, Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), and any others. If an individual Department/Division has unique requirements governing access to the data or systems for their business they must notify IT.

Appendix A: Documented Authentication System Exemptions

The following applications have been granted exemption from direct integration to KCECS. The services listed below include further documentation including the type of integration, password policy and specific management information in the IT Change Management Database (CMDB).

AS/400 Authentication

The AS/400 represents a full infrastructure system to include multiple levels of access and authentication that is independent of the KCECS. The AS/400 runs several applications that rely on the centralized credential system and some of have an additional layer of security either through individual user profile assignment or their own credentials system.

County-hosted Applications

All County-hosted applications are integrated with the KCECS if possible. When this isn't possible the system should be configured to meet or exceed the policy of the KCECS. At times, this may not be possible. When it is not possible, the settings will be documented within this policy.

The following applications maintain an independent credential system that meet, or exceed KCECS:

Application / Service	Managed By
Kronos	Kenosha County IT
iSecure	Facilities
ActiveGolf	Golf

The following applications maintain an independent credential system that is not able to meet the KCECS policy:

Application / Service	Managed By
ESRI ArcGIS	Kenosha County IT
ECS	Brookside Care Center

Cloud-based Applications

All Cloud-based applications are integrated with the KCECS if possible. When this isn't possible the system should be configured to meet or exceed the policy of the KCECS. At times, this may not be possible. When it is not possible, the settings will be documented within this policy.

The following applications maintain an independent credential system that meet, or exceed KCECS:

Application / Service	Managed By
Ceridian Dayforce	Human Resources
ShiftHound	Brookside Care Center

The following applications maintain an independent credential system that is not able to meet the KCECS policy:

Application / Service	Managed By
AkitaBox	Facilities