Internal Control and Data Security Audit of Drivers’ License and/or Motor Vehicle Record Data Exchange Usage by the Seminole County Clerk of the Circuit Court and Comptroller’s Office (MOU No. HSMV-0355-23)

REPORT NO. 2024-002

DISTRIBUTION LIST

Mr. Tony Landry	Chief Information System Officer
Ms. Deborah Taylor	Government Analyst

Division of Inspector General
Seminole County Clerk of the Circuit Court and Comptroller

DIVISION OF INSPECTOR GENERAL
Grant Maloy, Clerk of the Circuit Court and Comptroller
Seminole County, Florida

March 6, 2024

To: The Honorable Grant Maloy, Clerk of the Circuit Court and Comptroller

At the request of management, the Division of Inspector General conducted an audit of the internal controls over the Seminole County Clerk of the Circuit Court and Comptroller ("Clerk") office's access and usage of the Drivers' License Transcript and/or Motor Vehicle Record Data Exchange (Data Exchange) provided by the Florida Department of Highway Safety and Motor Vehicles (FLHSMV).

The objectives of our review were to determine whether the internal controls and data security for the Data Exchange complies with the terms of the Memorandum of Understanding (MOU), No. HSMV-0355-23, with FLHSMV.

We conducted the audit in accordance with standards that require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on or audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions on our audit objectives.

We greatly appreciate the cooperation and support received from Tony Landry, Chief Information Officer, and the IT Division.

Respectfully submitted,

Randall Nunley, CPA, CIA, CGAP, CRMA, CGMA
Inspector General

Approved by:

Honorable Mr. Grant Maloy
Clerk of the Circuit Court and Comptroller
Seminole County, Florida

Internal Control and Data Security Audit of Drivers' License and/or Motor Vehicle Record Data Exchange Usage by the Seminole County Clerk of the Circuit Court and Comptroller's Office
(MOU No. HSMV-0355-23)
Report No. 2024-002

GRANT MALOY
CLERK OF THE CIRCUIT COURT AND COMPTROLLER

Randall Nunley, CPA, CIA, CGAP, CRMA, CGMA
Inspector General

Division of Inspector General
Seminole County Clerk of the Circuit Court and Comptroller

Table of Contents

Executive Summary 1

Background 2

Network Diagram – FLHSMV (Exhibit A) 3

Physical Security Controls (Exhibits B – E) 4

Scope and Methodology 6

Audit Objectives 7

Overall Evaluation 7

IT Division Control Objectives and Techniques (Exhibit F) 8

Clerk of the Circuit Court & Comptroller IT Policies 12

Executive Summary

At the request of management, we conducted an audit of the Seminole County Clerk of the Circuit Court and Comptroller's (Clerk's) Memorandum of Understanding (MOU) with the Florida Department of Highway Safety and Motor Vehicles (FLHSMV). The request for the audit was to ensure compliance with the MOU No. HSMV-0355-23, which was executed on February 23, 2023.

The objectives of the audit were to:

- Ensure compliance with the data security requirements in the MOU and applicable data statutes and Clerk policies.
- Determine the adequacy of the Clerk's policies and procedures, in place, to protect personal data provided by the FLHSMV through the driver license transcript process.
- Determine the adequacy of security over the access of the Clerk's Office and FLHSMV data.
- Confirm there is appropriate security over the distribution, use, modification, and disclosure of FLHSMV data obtained through the driver license transcript process.

It is our opinion, the internal controls governing the use and dissemination of personal data obtained from the driver's license data exchange have been evaluated and meet the requirements of the FLHSMV MOU and all of the applicable laws and are adequate to protect the personal data from unauthorized access, distribution, use, modification, and disclosure.

The Clerk's Office and the Courts use the FLHSMV driver license transcript data exchange solely for court purposes and during court proceedings. We evaluated the policies and procedures for personnel to follow and the data security policies and procedures in place to protect personal data. The IT security policies and procedures have been reviewed by an IT security professional and found to be acceptable to protect personal data.

We would like to acknowledge Tony Landry, Chief Information Systems Officer and his entire staff for their assistance in the performance of this audit.

The results of the review are included in the report that follows.

Background

On February 23, 2023, a Memorandum of Understanding (MOU) was entered into between the Seminole County Clerk of Court and Comptroller (Clerk' Office) and the Florida Department of Highway Safety and Motor Vehicles (FLHSMV). The referenced MOU contract number is HSMV-0355-23.

The FLHSMV collects and maintains personal information that identifies individuals. The purpose of the MOU is to establish the conditions and limitations under which the FLHSMV agrees to provide electronic access to driver's license and motor vehicle information.

The MOU requires the Clerk's Office to maintain the confidential and exempt status of any and all information and also to ensure that any Third-Party End Users comply with the same confidentiality requirements.

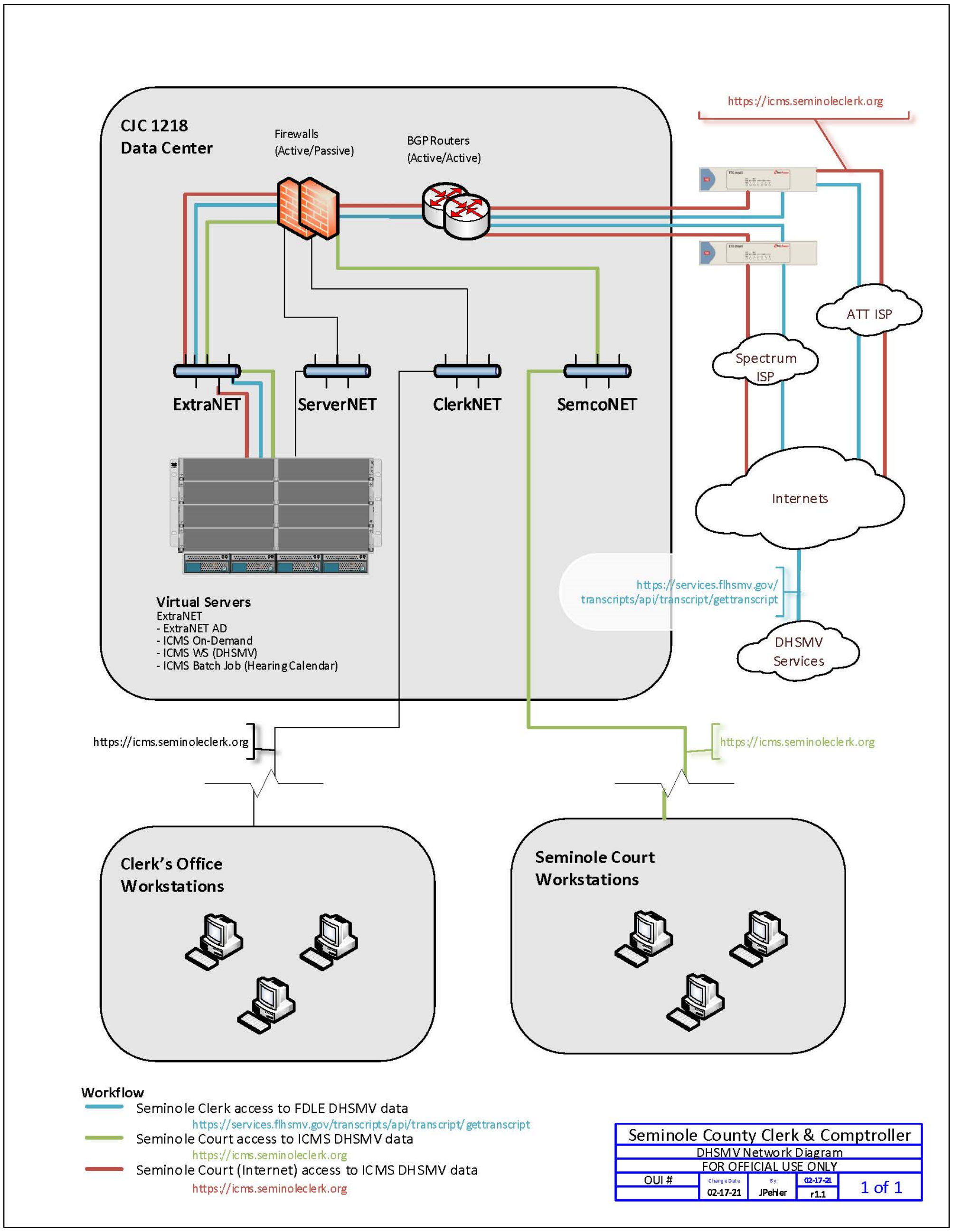
The FLHSMV as the custodian of the state's driver and vehicle records, is required to provide access to records permitted to be disclosed by law. More specifically the following provision:

Section III of the MOU states:

> "Under this MOU, the Requesting Party [Clerk's Office] will be provided, via remote electronic means, information pertaining to driver licenses and vehicles, including personal information authorized to be released pursuant to Section 119.0712(2), Florida Statutes and DPPA. By executing this MOU, the Requesting Party [Clerk's Office] agrees to maintain the confidential and exempt status of any and all information provided by the Providing Agency [FLHSMV] pursuant to this MOU and to ensure that any Third-Party End Users accessing or utilizing said information shall do so in compliance with Section 119.0712(2), Florida Statues and DPPA. Highly restricted personal information shall only be released in accordance with DPPA and Florida law…"

The Clerk's IT Division has global protection security controls to ensure that all personal and confidential information is protected from misuse. With that being said, the Clerk's Office has implemented specific internal security control features to safe guard driver's license information relating to the MOU with FLHSMV. Exhibit A is the network diagram of the network and the workflow for access to the ICMS FLHSMV data.

EXHIBIT A
NETWORK DIAGRAM – (FL)DHSMV


CJC 1218
Data Center
Firewalls
(Active/Passive)
BGP Routers
(Active/Active)
https://icms.seminoleclerk.org
ATT ISP
Spectrum
ISP
ExtraNET
ServerNET
ClerkNET
SemcoNET
Internets
https://services.flhsmv.gov/
transcripts/api/transcript/gettranscript
DHSMV
Services
Virtual Servers
ExtraNET
- ExtraNET AD
- ICMS On-Demand
- ICMS WS (DHSMV)
- ICMS Batch Job (Hearing Calendar)
https://icms.seminoleclerk.org
https://icms.seminoleclerk.org
Clerk's Office
Workstations
Seminole Court
Workstations
Workflow
Seminole Clerk access to FDLE DHSMV data
https://services.flhsmv.gov/transcripts/api/transcript/gettranscript
Seminole Court access to ICMS DHSMV data
https://icms.seminoleclerk.org
Seminole Court (Internet) access to ICMS DHSMV data
https://icms.seminoleclerk.org
Seminole County Clerk & Comptroller
DHSMV Network Diagram
FOR OFFICIAL USE ONLY
OUI #
Change Date
02-17-21
By
JPehler
02-17-21
r1.1
1 of 1

The IT Division has established physical security controls including:

- Camera security to monitor the Clerk's enterprise computer system (refer to **Exhibit B**). Video is stored on two Network Video Recorders (NVRs) and recordings are retained for 30 days. In addition, Seminole County Sheriff's Office monitors the perimeters of the Clerk's office with video and on-site security 24 hours a day, 7 days a week.
- Access to the MIS department, which is secured with a second and more restrictive electronic badge (refer to **Exhibit C**).
- The enterprise computer system is locked in a physically secured location within the MIS Data Center. This provides a third layer of physical access control via a physical locked cage (refer to **Exhibit D**).
- The MIS Data Center, servers, network, environmental control, and workstations are protected from power loss with a redundant set of Uninterruptible Power Supply (UPS) devises. This is a redundant system in itself as the building's generator will provide power in the case of a utility supplied power outage (refer to **Exhibit E**).

Exhibit B

CAUTION
THIS AREA IS PROTECTED BY A HFC-227ea EXTINGUISHING SYSTEM
DO NOT ENTER AREA DURING OR AFTER DISCHARGE
KEEP DOOR CLOSED AT ALL TIMES
MIS DEPARTMENT

Exhibit C

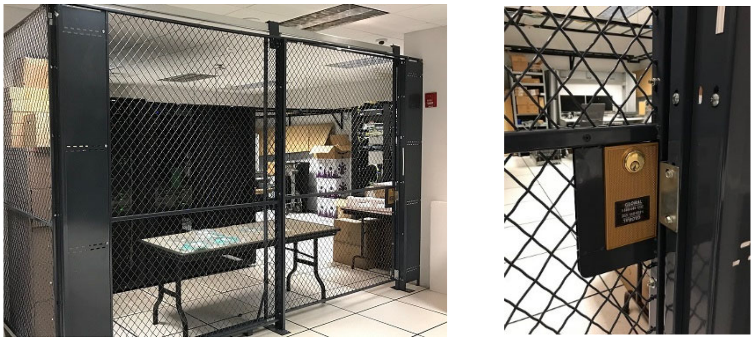


Exhibit D

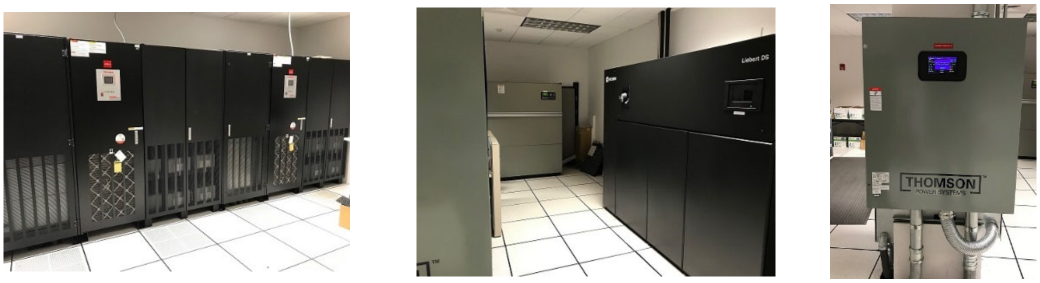


Exhibit E

At the request of the Clerk's Chief Information Officer, the Clerk's Office of Inspector General conducted an audit of the internal data security controls to ensure compliance with the requirements of the MOU.

Section VI (A) of the MOU states the following:

> "Internal Control and Data Security Audit – This MOU is contingent upon the Requesting Party [Clerk's Office] having appropriate internal controls in place at all times that data is being provided/received pursuant to this MOU to ensure that the data is protected from unauthorized access, distribution, use, modification or disclosure. The Requesting Party [Clerk's Office] must submit an Internal Control and Data Security Audit from a currently licensed Certified Public Accountant, on or before the first anniversary of the execution date of the is MOU or within one hundred twenty (120) days form receipt of a request from the Providing Agency [FLHSMV]. Government agencies may submit the Internal Control and Data Security Audit from the Agency's Internal Auditor or Inspector General. The audit shall indicate that the internal controls governing the use and dissemination of personal data have been evaluated in light of the requirement of this MOU, and applicable laws and are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. This includes both policies/procedures in place for personnel to follow and data security procedures/policies in place to protect personal data. This audit shall certify that the data security procedures/polices have been approved by a Risk Management IT Security Professional. The audit shall also certify that any and all deficiencies/issues found during the audit have been corrected and measures enacted to prevent recurrence…"

We conducted the audit in accordance with standards that require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on or audit objectives.

The results of the audit are included in the report that follows.

Scope and Methodology

The scope of this audit included the terms and conditions relating to the data exchange MOU between the Clerk and FLHSMV for the purpose of obtaining driver license transcripts.

Section VI. A. of the MOU requires the completion of an internal control and data security audit on or before the first anniversary of the execution date of the MOU.

Based on the applicable data protections laws and requirements referenced within the MOU, the scope of the audit was to assess the internal controls governing the use and dissemination of personal data obtained.

The audit included examining the internal controls at the Clerk's Office to ensure that they were sufficient to protect the personal data from unauthorized access, distribution, use, modification, and disclosure. The audit period was February 2023 through January 2024.

We reviewed the following:

- The MOU and the applicable statutes, codes, and Clerk's IT policies and procedures;
- The IT program diagrams that identify the design and IT security controls;
- Interviewed appropriate IT personnel to determine the path the driver's license transcript data through FLHSMV, Clerk's Office, and the Courts;
- The IT Internal Control objectives and techniques;
- The internal controls that ensure FLHSMV transcript data is safely secured in the Clerk's Office;
- The security access controls; and,
- The physical security controls that restrict access to computer equipment and the device transcript application and FLHSMV.

Audit Objectives

The objectives of the audit were to:

- Ensure compliance with the data security requirements in the MOU and other applicable data protection statutes, codes, and policies;
- Determine the adequacy of the Clerk's policies and procedures in place to protect personal data provided by the FLHSMV through the driver license transcript process;
- Determine the adequacy of security over access to the Clerk's Office and FLHMVS data; and,
- Confirm there is appropriate security over the distribution, use, modification, and disclosure of FLHSMV data obtained through the driver license transcript process.

Overall Evaluation

It is our opinion that the Clerk's Office is following all of the data security requirements referenced in the MOU and also the applicable security statutes, codes, and policies.

Our audit found that the Clerk's Office has adequate policies and procedures to protect personal data provided by the FLHSMV for the driver's license transcript process. There are sufficient safekeeping controls over the distribution, use, modification, and disclosure of FLHSMV data obtained through the driver license transcript process. We also have concluded that the personal data was controlled and used solely for the 18th Circuit Court purposes.

We conducted the audit in accordance with standards that require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on or audit objectives. It included tests of records and other auditing procedures, as we considered necessary in the circumstances.

EXHIBIT F

CLERK'S IT DIVISION'S
INTERNAL CONTROL OBJECTIVES, TECHNIQUES, POLICIES AND PROCEDURES

On February 23, 2023, a Memorandum of Understanding (MOU) was made and entered into between the Clerk and FLHSMV (HSMV-0355-23).

The purpose of the MOU was to establish the conditions and limitations under which the FLHSMV agreed to provide electronic access to Driver's License and Motor Vehicle information to the Clerk. The following is the policy established to ensure information exchanged will not be used for any purposes not specifically authorized by the MOU with FLHSMV:

I. OVERVIEW

This policy, which is established by the IT Department, is designed to establish a secure and confidential Internal Control Environment that ensures that information exchanged will not be used for any purposes not specifically authorized by the Memorandum of Understanding (MOU). The IT Department of the Clerk of the Circuit Court and Comptroller ("Clerk" or "Clerk's Office") has developed security requirements and standards consistent with Florida Statutes, Florida Administrative Code and the Florida Department of Highway Safety and Motor Vehicles ("DHSMV").

II. PURPOSE

There are three sections of Internal Control Objectives that ensure compliance with the terms and conditions of the MOU between the Clerk's Office and DHSMV. The objectives include: A. Physical Controls; B. Data Transmission and Storage; and C. Logical Security. Included within these sections, the Clerk's Office has identified specific control techniques and has specific policies and procedures to address each of the controls.

III. PROCEDURES AND TECHNIQUES / INTERNAL CONTROL OBJECTIVES

A. Physical Control

1. Control Objectives: The control objective relating to Physical Control is to ensure that all Clerk computer systems and equipment reside in a physically secure location.

2. Control Techniques:

   a. To ensure the control objective listed above is addressed, the Clerk has installed a camera system that monitors servers and network hardware; and,

   b. All equipment is secured with key locks and electronic access. All employee entry is logged. A key and an electronic access card are required for entry into all secured areas.

3. Procedures:

   a. The Clerk operates a video camera system that provides 24-hour video coverage, with 30-day retention of the videos of all secured areas. Clerk management reviews the videotapes on an as-needed basis.

   b. The physical internal hardware is secured with security locks, and only authorized employees have access. Employees accessing the area are required to use their badges for access. In addition, the employee must have a physical key to get access. The Seminole County Sheriff's Office ("Sheriff") maintains a log of those employees that gain access, and the log is available for review by the Clerk on an as-needed basis. A third-party (Sheriff) maintaining the electronic access system, in addition to the Clerk maintaining the physical key system, is an additional level of access control security.

B. Data Transmission and Storage

1. Control objectives: The control objective is to ensure that the Clerk has a system in place to provide that all data is secure and that the server and network infrastructure is hardened against internal and external unauthorized access.

2. Control Techniques:

   a. It is policy that all Clerk records must be stored on Clerk computer hardware.

   b. It is policy that employees are not allowed to store records on personal computers including laptops.

   c. It is policy that all Clerk records must be saved and stored on the Clerk's secure systems.

d. It is policy that all Clerk records must be transmitted over a secure network.

e. It is policy that all Clerk storage devices must be fully erased or physically destroyed before disposal.

3. Procedures:

a. Employees who have access to DHSMV license information are informed that the records they are viewing are confidential, and they are not allowed to store records on personal computers, including laptops.

b. Employees are informed that they are required to only save records on the Clerk’s secured provided network locations.

C. Logical Security Control

1. Control Objective: The objective of logical security controls is to ensure that the operating system, database management system, and applications are designed to restrict user access.

2. Control Techniques:

a. To ensure secured access, user authentication credentials are assigned to each individual user;

b. Clerk policy requires that authentication credentials are not shared;

c. Clerk policy requires that Administrator-level authentication credentials require multi-factor authentication;

d. Clerk policy prohibits Administrator accounts from having access to the Internet;

e. Clerk policy prohibits Administrator accounts from direct access to email;

f. Firewall appliances are implemented at network ingress/egress;

g. Firewalls are implemented on all computer endpoints;

h. Firewalls are kept under active maintenance;

i. Firewalls are patched and up-to-date;

j. All servers are kept under active maintenance, patched and up-to-date;

k. Malware prevention software resides on all computer endpoints, kept under active maintenance, patched, and up-to-date;

l. The DHSMV data is not retained after viewed by the Judge;

m. All access to DHSMV data is logged, and every request log is maintained and reviewed.

Clerk’s Information Technology Policies:

Policy	Page
#23-0001, Acceptable Use	13 - 14
#24-0002, Firewall	15 - 16
#24-0003, Multi-Factor Authentication	17 - 19
#24-0004, Multi-Factor Authentication Token Device	20 - 21
#24-0005, Passwords	22 - 24
#24-0006, Server	25 - 26
#24-0007, Email	27 - 28
#24-0008, Endpoint Protection	29 – 30

Policy #23-0001, Acceptable Use

I. OVERVIEW

Seminole County Clerk of the Circuit Court and Comptroller (Clerk's Office) provides access to and use of its technology resources to its staff, vendors, contractors, and public to support its mission. Access and use of Clerk's Office resources is a privilege and requires that users of such technology resources act responsibly. Users shall only access and / or make use of Clerk's Office technology resources in a manner that is consistent with applicable federal, state, and local laws and Clerk's Office policies and procedures. Users accessing the Clerk's Office technology resources have no expectation of privacy with respect to such uses. Please note that applicable laws and policies are not limited to those specifically addressing access to and use of computers and networks; they may also include, but are not limited to, laws and policies related to personal conduct.

II. PURPOSE

The purpose of this policy is to establish a standard for acceptable use of Clerk's Office technology resources; demonstrating due diligence with regards to the security of Clerk's Office Information Technology network and data.

III. SCOPE

The scope of this policy applies to all users of the Clerk's Office technology resources whether or not formally affiliated with the Clerk's Office or accessing and using technology resources from remote locations.

IV. POLICY

Non-compliance with this policy may result, depending upon the nature of the non-compliance, in the user's account or access to the Clerk's Office technology resources being suspended, or disabled, or permanently terminated. In the case of suspension, the Clerk's Office may require implementation of certain remedial measures prior to reinstatement of the user's account or access. Additionally, the user may be referred for sanctions to the appropriate disciplinary body and may be subject to civil and criminal penalties. The Clerk's Office may take any actions it deems necessary to protect and manage the security and integrity of its technology resources, including but not limited to, suspending or disabling user accounts or limiting the available resources through traffic shaping, data caps, or other measures.

V. PROCEDURES

A. The Clerk's Office provides access to and use of its technology resources to its employees and others, to support its mission. Access and use of the Clerk's Office technology resources is a privilege and requires that users of such technology resources act responsibly. Users shall only access and/or make use of the Clerk's Office technology resources in a manner that is consistent with applicable federal, state, and local laws and the Clerk’s Office policies and procedures. Users accessing the Clerk’s Office technology resources have no expectation of privacy with respect to such uses. Please note that applicable laws and policies are not limited to those specifically addressing access to and use of computers and networks; they may also include, but are not limited to, laws and policies related to personal conduct.

B. Users of the Clerk’s Office technology resources must:

1. Follow all applicable federal, state, and local laws;
2. Follow all Clerk’s Office policies and procedures and IT standards;
3. Follow all Florida Department of Law Enforcement Criminal Justice Information Services policies and procedures and IT standards when accessing CJIS technology resources per FBI CJIS Security Policy;
4. Actively maintain the security of all devices accessing Clerk’s Office technology resources or being used to access, store, or process Clerk’s Office maintained data;
5. Actively maintain the security and privacy of data or Clerk’s Office maintained third-party data and store such data only in authorized locations, consistent with Clerk’s Office policies and standards;
6. Report privacy, security, or technology policy violations to the Clerk’s Office IT Security Manager.

Policy #24-0002, Firewall

I. OVERVIEW

The firewall policy defines how the Seminole County Clerk of the Circuit Court and Comptroller ("Clerk" or "Clerk's Office") primary network firewalls should handle inbound and outbound network traffic for specific IP addresses, address ranges, protocols, applications, and content types.

II. PURPOSE

In accordance with industry 'best practices' and to comply with numerous compliance regulations, the Clerk's Office has prepared various Information Technology Security policies and procedures which are intended to protect the confidentiality, integrity and availability of our critical client data and our technology resources. This document describes network firewall policy at the Clerk's Office in defining and administering these policy and procedures.

III. SCOPE

The scope of this policy applies to all employee, vendors, contractors, technology resources, and public users using the Clerk's network for access to and from the Internet. All network traffic passes through the Clerk's primary network firewall, providing a layer of security.

IV. POLICY

Non-compliance with this policy shall be considered a violation of the Clerk's Acceptable Use Policy and will be addressed and remediated accordingly.

A. Ownership and Responsibility: All equipment and applications within this scope will be administered by the IT Networking Team. Administrative Access to the Clerk's Office firewalls will be governed by the Security Manager.

B. Firewall Patches / Maintenance: All equipment and applications within this scope are under a 24/7 technical support & firmware / software support contracts directly with the vendor. The network firewalls will be regularly monitored for firmware, security, and database updates:

a. Firmware updates will be one version removed from latest release and checked monthly. This allows the firmware to be up to date and in vendor's TAC "Preferred" version of use.

b. Security updates will be current version release and checked weekly.

c. Database updates will be current version release and checked on the following schedule:

i. Antivirus database: Checked and updated every hour at five minutes past the hour.

ii. Application and Threat databases: Checked and updated every 30 minutes.

iii. Wildfire databases (Vendor specific): Checked and updated every 15 minutes.

C. Network Connections: All external and wireless connection to the Clerk's Office networks must pass through the primary network firewalls. In addition, all network connections entering a high security network must pass through a network firewall. Any change to an external connection or in the configuration of the firewall must be adequately tested and documented according to the Change Management Policy.

D. Network Firewall Physical Security: All Clerk's Office network firewalls must be in a physically secure data center where access is controlled by the Clerk's Office's Information Technology department.

V. DEFINITIONS

A. Change Management - The process of requesting, developing, approving, and implementing a planned or unplanned change within the Clerk's Office's Information Technology infrastructure.

B. Network Firewall – A single-purpose hardware device designed to control the flow of traffic between points. Often, these are implemented to increase security between the outside world (Internet) and an origination's network connections. The Clerk's Office Information Technology department has implemented Network Firewalls between internal networks and any external network (example: Internet, Seminole County, Court Administration, FDLE, DHSMV, and other networks).

Policy #24-0003, Multi-Factor Authentication

I. OVERVIEW

The use of Multi-Factor Authentication (MFA) in addition to an account password is an important aspect of computer security. By adding an MFA in addition to an account password, the security level is greatly improved. All employees, including contractors and vendors with access to Seminole County Clerk of the Circuit Court and Comptroller ("Clerk" or "Clerk's Office") technology resources are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. In addition, all employees who have elevated accounts (i.e., Administrators) are required by the Clerk's Cybersecurity Insurance Agency to also have MFA applied to such accounts.

II. PURPOSE

The purpose of this policy is to establish a standard for the addition of MFA for accounts which have elevated privileges.

III. SCOPE

The scope of this policy applies to all account holders regardless of affiliation with the Clerk's offices, networks, data stores, or any other technology resources containing any information.

IV. POLICY

Compliance: Non-compliance with this policy shall be considered a violation of the Clerk's Office's Acceptable Use Policy and will be addressed and remediated accordingly.

A. Responsibility of Users

1. Users are responsible for adhering to the Standards, Policies, and Processes as written in the IT Password Policy and Acceptable Use documents. The following Standards, Policies, and Processes do not replace or supersede any other Standards, Policies, or Processes, they are provided to specifically address MFA procedures.

2. Users are responsible for keeping MFA applications and any other types of authentication secure and confidential, including not sharing or storing this information in an insecure manner. Passwords, passcodes, or MFA devices (i.e., cell phone with mobile app) should not be written down or left in an easily accessible location.

3. Passwords, passcodes, or MFA information must not be shared, even with IT support staff. If anyone asks you for this information, please report the incident to IT ext. 4040.

4. Always log out of applications or lock your workstation when leaving a computer to prevent unauthorized use. <Window> - <L> keys pressed together will lock your workstation.

B. MFA Devices:

1. Silverfort Mobile application: Push notification for MFA from Silverfort installed on mobile device.

2. Silverfort or other One-Time Password (OTP) application: Time based six-digit passcode used for MFA; installed on mobile device.

3. Tokenized One-Time Password (OTP): OTP token device displays six-digit passcode used for MFA and is self-contained; no ancillary device required.

C. Account Configurations:

1. Administrator Accounts – all logon attempts

2. VDI Accounts – all logon attempts

3. General User Accounts – Once per 15 hours per ‘source’ device

D. Administrator Accounts:

1. Administrator accounts will have external email accounts; only required during mobile application configuration or pairing.

2. Administrator accounts will require Multi-Factor Authentication (MFA) for all logon attempts to all workstations and servers.

V. DEFINITIONS

A. Technology Resources

1. All Clerk’s Office owned, operated, leased, or contracted computing, networking, telecommunications, and information resources;

2. All information maintained within the Clerk’s Office computing resources;

3. All voice and data networks, telecommunications and communication systems and infrastructure;

4. All technology resources including all hardware, software, applications, databases, and storage media.

B. Types of Authentication

1. Password – A combination of letters, numbers, symbols, and special characters that can be used to authenticate a person to an account accessing a technology resource. Long forms of passwords are sometimes called a passphrase.

2. Biometric – Unique physical or behavioral characteristics of a person that can be analyzed to uniquely identify and authenticate a person to an account for access to a technology resource.

3. Token – A hardware or software device that can be cryptographically verified as unique.

4. Geolocation – For purpose of this policy, geolocation refers to the process of identifying the location of a user based upon the known location of their IP (Internet Protocol) address or from data collected from their authenticated devices with built-in location detection.

5. PIN – A Personal Identification Number is a short number or password used locally on a device as a convenient authentication alternative to typing a full password.

6. MFA – Multi Factor Authentication uses two or more authentication factors. Typically, passwords, biometrics, or tokens are used in two steps to achieve authentication.

Policy #24-0004, Multi-Factor Authentication Token Device

I. OVERVIEW

The use of Multi-Factor Authentication ("MFA") in addition to an account password is an important aspect of computer security. This document is an addendum to the Policy 24-0003, for use when assigning an MFA Token or other One Time Password ("OTP") device to an employee for use in lieu of the Silverfort MFA Application.

II. PURPOSE

The purpose of this document is for establishing a standard, assignment, and responsibility for the use of an MFA Token.

III. POLICY

Non-compliance with this policy shall be considered a violation of the Clerk's Office's Acceptable Use Policy and will be addressed and remediated accordingly.

A. Responsibility of Users: Users are responsible for adhering to the Standards, Policies, and Processes as written in the IT Password Policy and Acceptable Use documents. The following Standards, Policies, and Processes do not replace or supersede any other Standards, Policies, or Processes, they are provided to specifically address MFA Token assignment and use.

1. Users are responsible for keeping MFA tokens (Tokenized One-Time Password (OTP): OTP token device displays six-digit passcode used for MFA and are self-contained; no ancillary device required.) secure and confidential, including not sharing or storing this information in an insecure manner.

2. Passwords, passcodes, or MFA information must not be shared, even with IT support staff. If anyone asks you for this information, please report the incident to IT ext. 4040.

3. When not in use, an MFA token must be put away or not in plain sight.

4. Always log out of applications or lock your workstation when leaving a computer to prevent unauthorized use. <Window> - <L> keys pressed together will lock your workstation.

B. Loss of MFA Token: Employees who wish to use an MFA Token in lieu of the Silverfort MFA Application will be given an MFA Token to use. If this device is lost, stolen, or missing, the employee may purchase a replacement for $40.

IV. DEFINITIONS

A. Technology Resources

1. All Clerk’s Office owned, operated, leased, or contracted computing, networking, telecommunications, and information resources;

2. All information maintained within the Clerk’s Office computing resources;

3. All voice and data networks, telecommunications and communication systems and infrastructure;

4. All technology resources including all hardware, software, applications, databases, and storage media.

B. Types of Authentication

1. Password: A combination of letters, numbers, symbols, and special characters that can be used to authenticate a person to an account accessing a technology resource. Long forms of passwords are sometimes called a passphrase.

2. Token: A hardware or software device that can be cryptographically verified as unique.

3. MFA: Multi Factor Authentication uses two or more authentication factors. Typically, passwords, biometrics, or tokens are used in two steps to achieve authentication.

Policy #24-0005, Passwords

I. OVERVIEW

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and / or exploitation of our systems or services. All employees, including contractors and vendors with access to Seminole County Clerk of the Circuit Court and Comptroller ("Clerk" or "Clerk's Office") technology resources are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

II. PURPOSE

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

III. SCOPE

The scope of this policy applies to all account holders regardless of affiliation with the Clerk's offices, networks, data stores, or any other technology resources containing any information.

IV. POLICY

Non-compliance with this policy shall be considered a violation of the Clerk's Office's Acceptable Use Policy and will be addressed and remediated accordingly.

A. Responsibility of Users:

1. Users are responsible for keeping passwords and all other types of authentication secure and confidential, including not sharing or storing passwords in an insecure manner. Passwords should not be written down or left in an easily accessible location.

2. Passwords are confidential and should not be stored electronically without strong encryption.

3. Passwords must not be shared, even with IT support staff. If anyone asks you for your password, please report the incident to IT Security at (407) 665-4548.

4. Create unique passwords for each of your user accounts. You will likely have access to several systems requiring usernames and passwords, remember to use different passwords for different systems.

5. Always log out of applications or lock your workstation when leaving a computer to prevent unauthorized use. <Window> - <L> keys pressed together will lock your workstation.

B. Passwords:

1. Contain at least three of the following four-character types:

a. Numbers (0-9)

b. Lower case letters (a-z)

c. Upper case letters (A-Z)

d. Special Characters (example: !&%^@*#~)

2. Must be at least eight (8) characters in length.

3. Administrator Accounts:

a. Administrator accounts will not have external email accounts.

b. Administrator accounts will require Multi Factor Authentication (MFA).

V. DEFINITIONS

A. Technology Resources

1. All Clerk's Office owned, operated, leased, or contracted computing, networking, telecommunications, and information resources;

2. All information maintained within the Clerk's Office's computing resources;

3. All voice and data networks, telecommunications and communication systems and infrastructure;

4. All technology resources including all hardware, software, applications, databases, and storage media.

B. Types of Authentication

1. Password – A combination of letters, numbers, symbols, and special characters that can be used to authenticate a person to an account accessing a technology resource. Long forms of passwords are sometimes called a passphrase.

2. Biometric – Unique physical or behavioral characteristics of a person that can be analyzed to uniquely identify and authenticate a person to an account for accessing a technology resource.

3. Token – A hardware or software device that can be cryptographically verified as unique.

4. Geolocation – For purpose of this policy, geolocation refers to the process of identifying the location of a user based upon the known location of their IP (Internet Protocol) address or from data collected from their authenticated devices with built-in location detection.

5. API Token – An Application Program Interface token is a unique, long, token or key that may provide authentication for an application to access another service or application.

6. PIN – A Personal Identification Number is a short number or password used locally on a device as a convenient authentication alternative to typing a full password.

7. MFA – Multi Factor Authentication uses two or more authentication factors. Typically, passwords, biometrics, or tokens are used in two steps to achieve authentication.

Policy #24-0006, Server

I. OVERVIEW

The server policy defines how the Seminole County Clerk of the Circuit Court and Comptroller ("Clerk" or "Clerk's Office") servers should be used and maintained.

II. PURPOSE

In accordance with industry 'best practices' and to comply with numerous compliance regulations, the Clerk's Office has prepared various Information Technology Security policies and procedures which are intended to protect the confidentiality, integrity and availability of critical client data and technology resources. This document describes the server policy at the Clerk's Office in defining and administering these policy and procedures.

III. SCOPE

The scope of this policy applies to all employees, vendors, and contractors using the Clerk's Office servers. This scope should apply to all existing, new, and temporary server setups, installations, or decommissioning.

V. POLICY

Non-compliance with this policy shall be considered a violation of the Clerk's Office's Acceptable Use Policy and will be addressed and remediated accordingly.

A. Ownership and Responsibility

All equipment and applications within this scope will be administered by the IT System Administrator. Administrative Access to the Clerk's Office servers will be governed by the System Administrator and / or members of the Infrastructure Team.

B. Server Patches / Maintenance

All equipment and applications within this scope are regularly monitored for firmware, software, security, and database updates:

1. Firmware and Software updates will be one version removed from latest release and checked monthly. This allows the firmware / software to be up to date and in vendor's "Best-Practice" version of use.

2. Security updates will be current version release and checked monthly.

C. Network Connections

All server connections to the Clerk’s Office networks will be installed on the “Server” network (VLAN) to maintain isolation of server traffic and data flows from other networks. In addition, all network connections entering a high security network must pass through a network firewall (see Firewall Policy). Any change to a server’s network connection to the Internet must be adequately tested and documented according to the Change Management and Firewall Policies.

VI. DEFINITIONS

A. Change Management - The process of requesting, developing, approving, and implementing a planned or unplanned change within the Clerk’s Office’s Information Technology infrastructure.

B. Server –A server is a piece of computer hardware that provides functionality for other programs or devices, called "clients". This architecture is called the client–server model. Servers can provide various functionalities, often called "services", such as sharing data or resources among multiple clients, or performing computation for a client. A single server can serve multiple clients, and a single client can use multiple servers. A client process may run on the same device or may connect over a network to a server on a different device. Typical servers are database servers, file servers, mail servers, print servers, web servers, and application servers.

Policy #24-0007, Email

I. OVERVIEW

Electronic messages (e-mail) often contains important and sometimes sensitive information. The access to and retention of such data is paramount. This document provides information on how to best access, retain, and secure electronic messages within the Seminole County Clerk of the Circuit Court and Comptroller ("Clerk" or "Clerk's Office") offices.

II. PURPOSE

This policy has been developed to define the requirements for proper function and retention of electronic mail ("email") messages at the Clerk's Office.

III. SCOPE

The scope of this policy applies to email messages and associated messaging systems owned and/or operated by the Clerk's Office.

IV. POLICY

Non-compliance with this policy shall be considered a violation of the Clerk's Office's Acceptable Use Policy and will be addressed and remediated accordingly.

A. Employees should primarily use company email systems for business purposes.

The following uses of company email systems are prohibited:

1. Excessive personal use of email;
2. Inappropriate or illegal content such as offensive jokes;
3. Engaging in illegal activities;
4. Encrypting personal emails and attachments;
5. Allowing other employees access to your email account.

B. Electronic Message Server Patches / Maintenance

All equipment and applications within this scope are regularly monitored for firmware, software, security, and database updates:

1. ESA Appliance firmware and software updates will be one version removed from latest release and checked monthly. This allows the firmware to be up to date and in vendor's TAC "General Release" version of use. Any security and database updates will be updated at the latest release version.

2. Exchange Server software updates will be one version removed from latest release and checked monthly. This allows the software to be up to date and in vendor's "Best Practices" version of use. Any security and database updates will be updated at the latest release version.

3. MS Teams software updates will be updated to the current release version determined by the IT Server Policy guidelines and / or determined by the vendor (Microsoft) as this application resides in the cloud (Office 365).

I. DEFINITIONS

A. Electronic Message – A self-contained piece of digital communication that is designed or intended to be transmitted between physical devices. Electronic Message includes, but is not limited to, electronic mail (email), a text message, an instant message (i.e., Teams or Skype), or a command or request to access an internet site.

Policy #24-0008, Endpoint Protection

I. OVERVIEW

The Endpoint Protection policy defines how the Seminole County Clerk of the Circuit Court and Comptroller ("Clerk" or "Clerk's Office") utilizes Endpoint Protection systems to assist in securing technology resources from cybersecurity threats.

II. PURPOSE

In accordance with industry 'best practices' and to comply with numerous compliance regulations, the Clerk's Office has prepared various Information Technology Security policies and procedures which are intended to protect the confidentiality, integrity and availability of critical client data and technology resources. This document describes the endpoint protection policy at the Clerk's Office in defining and administering these policy and procedures.

III. SCOPE

The scope of this policy applies to all employee, vendors, contractors, and technology resources users using the Clerk's Office workstations for access to the Internet. All workstations on our network are required to have an endpoint protection software installed as an additional layer of security when accessing the Internet.

IV. POLICY

Non-compliance with this policy shall be considered a violation of the Clerk's Office's Acceptable Use Policy and will be addressed and remediated accordingly.

A. Ownership and Responsibility: All equipment and applications within this scope will be administered by the IT Operations Team. Administrative Access to the Clerk's Office's endpoint servers and software will be governed by the Operations Team and / or the Security Manager, Jim Pehler.

C. Endpoint Patches / Maintenance: All equipment and applications within this scope are under 24/7/4 technical support & software support contracts directly with the vendor. The endpoint server and client software are regularly monitored for firmware, security, and database updates.

V. DEFINITIONS

Endpoint Protection – A single-purpose server designed to protect workstations from cybersecurity threats when accessing external information or systems on the Internet. An endpoint client is installed on the workstation and will attempt to prevent, detect, and respond to cybersecurity threats. Cybersecurity threats such as malware can be blocked by the endpoint client through prevention with use of vendor supplied list of known-threat applications, detection with program hash matching to known threats, and response to possible threats by centralized cataloging of applications and looking for abnormalities across vendor's client installs.