2022 AUDIT OF CLERK'S DRIVER'S LICENSE AND/OR MOTOR VEHICLE EXCHANGE

REPORT NO. 041522

DISTRIBUTION LIST

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

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

April 15, 2022

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

We have conducted an audit of the Clerk's Office Driver License Transcript Data Exchange for 2022. The audit is to ensure continued compliance with the Memorandum of Understanding (MOU) between the Seminole County Clerk of the Circuit Court and Comptroller (Clerk) and the Florida Department of Highway and Motor Vehicles (DHSMV). This is our 2022 annual audit.

We greatly appreciate the cooperation and support received from Mr. Tony Landry and the IT Division.

Respectfully submitted,

Bill Carroll, CPA, CFE, CIG, CIGA
Inspector General

Approved by:

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

2022 Annual Audit
Clerk's Office Driver License and/or Motor Vehicle Exchange Audit
Report No. 041522

GRANT MALOY
CLERK OF THE CIRCUIT COURT AND COMPTROLLER

Bill Carroll, CPA, CFE, CIG, CIGA
Inspector General

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

Table of Contents

Executive Summary

This 2022 audit was requested by the Seminole County Clerk of the Circuit Court and Comptroller (Clerk) and the Clerk's Chief Information Services Officer.

The request for the audit was to ensure compliance with the Memorandum of Understanding (MOU) No. HSMV – 0303-20 signed on June 11th, 2020.

The objectives of the audit were to determine:

- Compliance with the security requirements of the MOU and applicable statutes and Clerk policies;
- If there is adequate security over the access of the Clerk's Information Services to the DHSMV data through the motor vehicle transcript process; and,
- If there is adequate security over the distribution, uses, modification, and disclosure of DHSMV data.

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 DHSMV 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 DHSMV 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 Mr. Tony Landry, Chief Information Systems Officer and his entire staff for their assistance in the performance of this audit. Their commitment to exceptional service to the Clerk's Office is commendable.

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

Background

On June 11th, 2020, a Memorandum of Understanding (MOU) was entered into between the Seminole County Clerk of Court (Clerk) and the Florida Department of Highway Safety and Motor Vehicles (DHSMV). The referenced MOU contract number is HSMV-0303-20.

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

The MOU requires the Clerk 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.

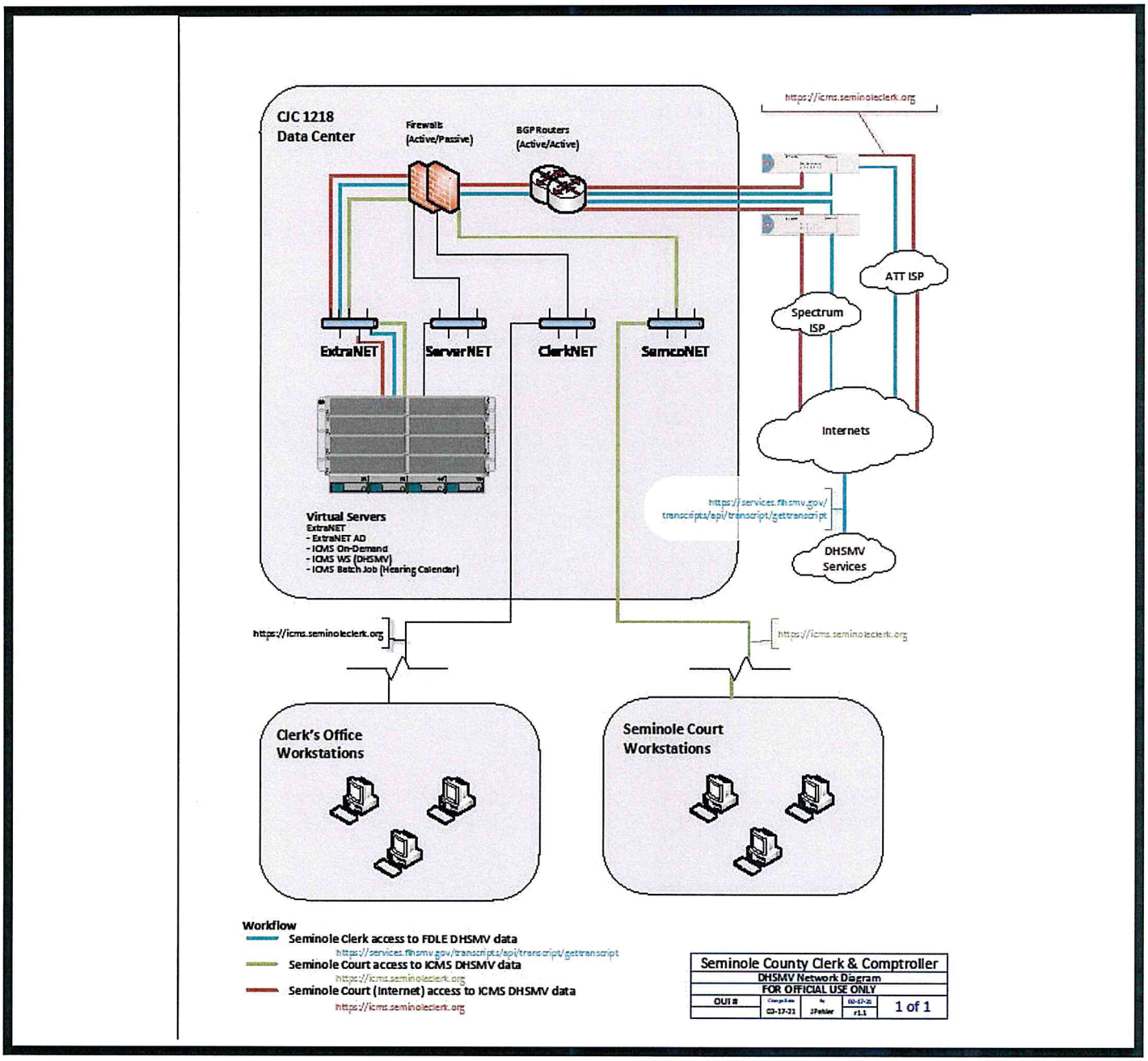
The DHSMV as the custodian of the state's driver and vehicle records, is required to provide access to records permitted to be disclosed by law. More specifically a provision of

Section III of the MOU states:

> "Under this MOU, the [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 [Clerk's Office] agrees to maintain the confidential and exempt status of any and all information provided by the DHSMV 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 DHSMV. For example, below is a network diagram of the network and the workflow for access to the ICMS DHSMV data.

EXHIBIT A NETWORK DIAGRAM - DHSMV



The IT Division has established physical security controls as illustrated below.

EXHIBIT B – CAMERA SECURITY TO MONITOR THE CLERK'S ENTERPRISE COMPUTER SYSTEM. DIGITAL TAPE RECORDING IS MAINTAINED FOR CONTINUOUS MONITORING. SEMINOLE COUNTY SHERRIF'S OFFICE MONITORS THE PERIMITERS OF THE CLERK'S OFFICE WITH VIDEO AND DEPUTY'S 24 HOURS A DAY 7 DAYS A WEEK.

EXHIBIT C

CLERK ENTERPRISE SYSTEM IS LOCKED IN A PHYSICALLY SECURED LOCATION

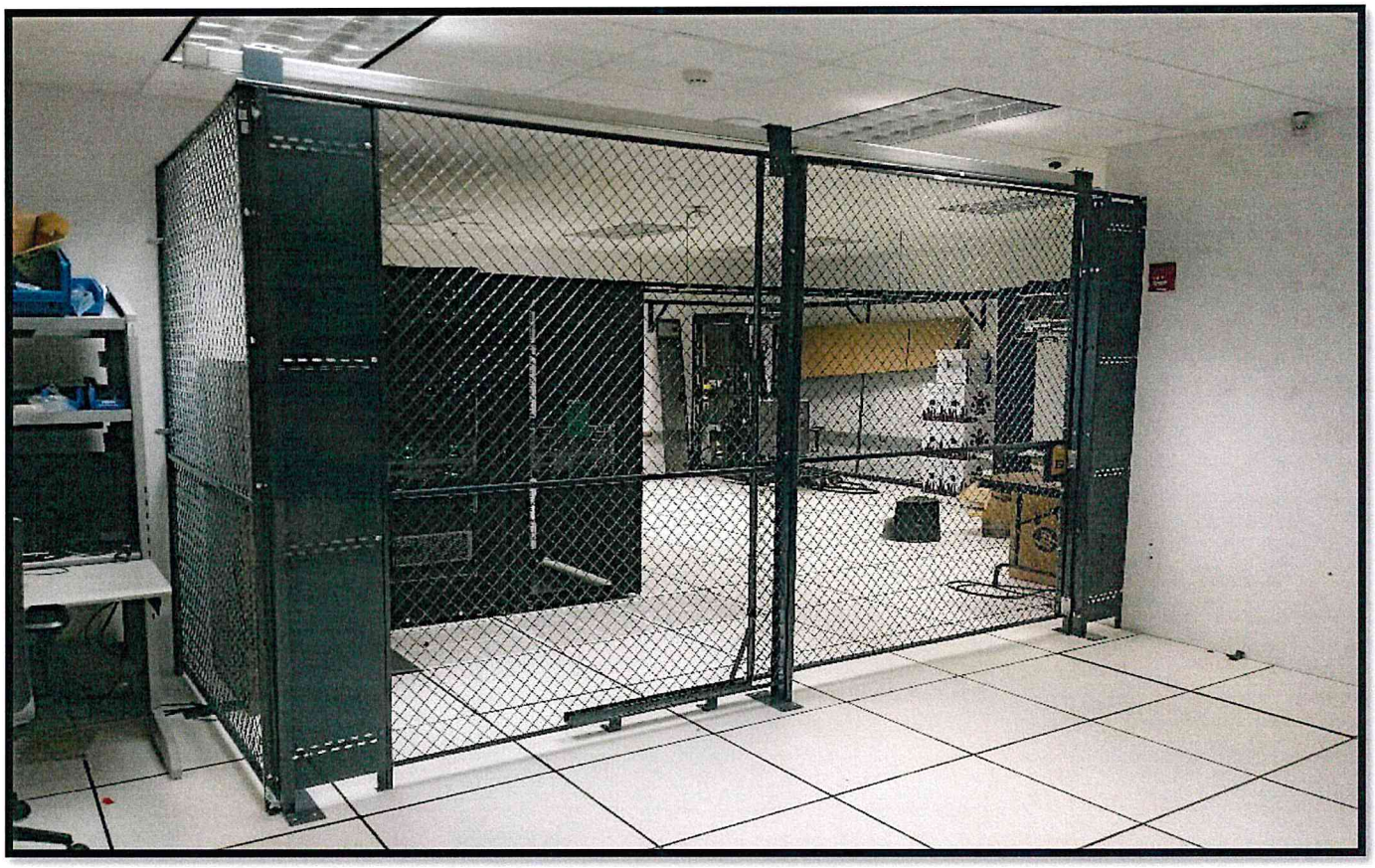
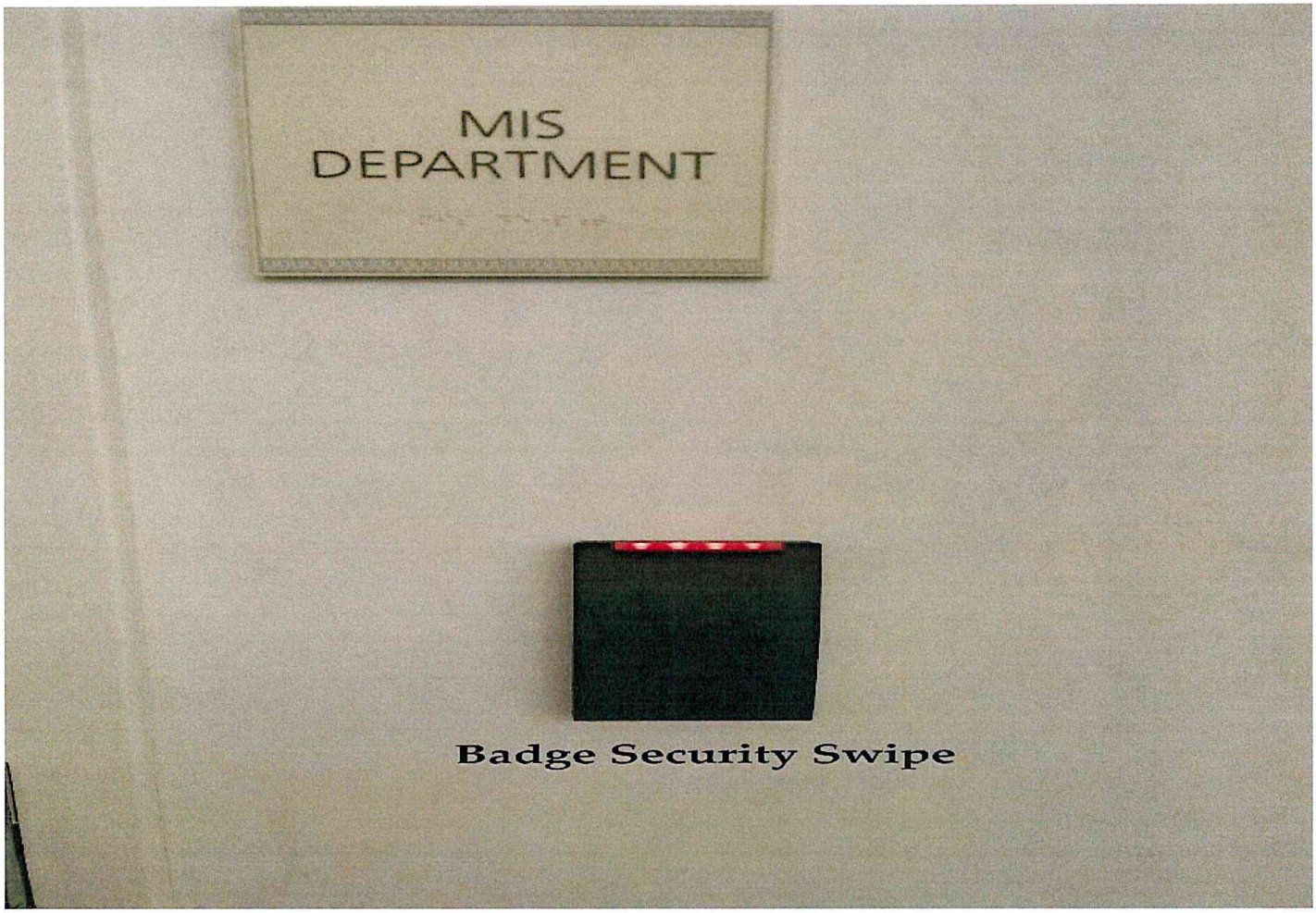


EXHIBIT D

ACCESS TO THE MIS DEPARTMENT IS SECURED BY ELECTONIC BADGE ENTRY



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 VIA of the MOU states the following:

> "Internal Control and Data Security Audit – This MOU is contingent upon the [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 [Clerk's Office] must submit an Internal Control and Data Security Audit from a currently licensed Certified Public Accountant, on or before the risk anniversary of the execution date of the is MOU or within one hundred twenty (120) days form receipt of a request from the DHSMV. 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."

The audit was conducted in accordance with the International Standards for the Professional Practices of Internal Auditing and the Principles and Standards for the Offices of Inspector General.

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's Office and DHSMV 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 May 2021 to April 2022.

We reviewed the following:

- The MOU and the applicable statutes, codes, and Clerk of Court 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 DHSMV, Clerk of Court Office, and the Courts;
- The IT Internal Control objectives and techniques;
- The internal controls that ensure DHSMV 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 DHSMV.

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;
- Make certain that the Clerk's Office has adequate policies and procedures in place to protect personal data provided by the DHSMV through the driver license transcript process;
- Determine if there is adequate security over the access of the Clerk's Office and DHMVS data; and,
- Confirm that there is appropriate security over the distribution, use, modification, and disclosure of DHSMV 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 DHSMV for the driver's license transcript process. There are sufficient safekeeping controls over the distribution, use, modification, and disclosure of DHSMV 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.

The audit was conducted in accordance with the International Standard for the Professional Practice of Internal Auditing and the Principles and Standards for Offices of Inspector General. It included tests of records and other auditing procedures, as we considered necessary in the circumstances.

EXHIBIT E

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

Background Information

On June 11th, 2020, a Memorandum of Understanding (MOU) was made and entered into between the Clerk and DHSMV.

The purpose of the MOU was to establish the conditions and limitations under which the DHSMV Vehicles agreed to provide electronic access to Driver's License and Motor Vehicle information to the Clerk.

IT Department Policy Statement

This policy which is established by the Information Systems 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 MOU. The IT Department of the Clerk has developed security requirements and standards consistent with Florida Statutes, Florida Administrative Code and the Florida Department of Motor Vehicles.

Included within this policy are the following sections to address all of the Internal Control requirements. The section includes: I. Definitions of Internal Control Objectives and Techniques; and II. IT Policies and Procedures.

I. DEFINITION OF INTERNAL CONTROL OBJECTIVES AND TECHNIQUES

There are three sections of Internal Control Objectives that ensure compliance with the terms and conditions of the MOU (HSMV-0303-20) between the Clerk 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.

INTERNAL CONTROL OBJECTIVES/TECHNIQUES AND PROCEDURES

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:

- To ensure the Control Objective noted above is addressed, the Clerk installed a camera system that monitors servers and network hardware; and,
- 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 the secured area.

3. Procedures:

- Clerk operates a digital video camera system that provides 24-hour video coverage, with 30-day retention of the videos of the secured areas. Clerk of Court management reviews the videotapes on an as-needed basis.
- Seminole County Sherriff's Office monitors the perimeters of the Clerk's Office with video and Deputy's 24 hours a day 7 days a week.
- 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 key to get access. The Seminole County Sheriff maintains a log of those employees that gain access, and the log is available for review by 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:

- It is policy that all Clerk records must be stored on Clerk computer hardware
- It is policy that employees are not allowed to store records on personal computers including laptops
- It is policy that all Clerk records must be saved and stored on the Clerk's secure systems
- It is policy that all Clerk records must be transmitted over a secure network
- It is policy that all clerk storage devices must be fully erased or physically destroyed before leaving a secured device.

3. Procedures:

- Employees who have access to Motor Vehicle and Driver's 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.
- 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 Objectives:

- 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:

- To ensure secured access, user authentication credentials are assigned to each user;
- Clerk policy requires that authentication credentials are not shared;
- Clerk policy requires that Administrator-level authentication credentials require multi-factor authentication;
- Clerk policy prohibits Administrator accounts from having access to the Internet;
- Clerk policy prohibits Administrator accounts from direct access to email;
- Firewall appliances are implemented at network ingress/egress;
- Firewalls are implemented on all computer endpoints;
- Firewalls are kept under active maintenance;
- Firewalls are patched and up to date;
- All servers are kept under active maintenance, patched and up to date;
- MFA being added as an additional layer of security to existing authentication and authorization controls;
- Malware prevention software resides on all computer endpoints, kept under active maintenance, patched, and up to date;
- The DHSMV data is not retained after viewed by the Judge; and,
- All access to the department of motor vehicle data is logged, and every request log is maintained and reviewed.

3. IT Internal Control Policies and Procedures:

Acceptable Use Policy

Overview

Clerk 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 resources is a privilege and requires that users of such technology resources act responsibly. Users shall only access and / or make use of Clerk technology resources in a manner that is consistent with applicable federal, state, and local laws and Clerk policies and procedures. Users accessing Clerk 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 not limited to, laws and policies related to personal conduct.

Purpose

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

Scope

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

Policy Compliance

Non-compliance with this policy may result, depending upon the nature of the non-compliance, in the user's account or access to Clerk technology resources being suspended, or disabled, or permanently terminated. In the case of suspension, Clerk 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 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.

Related Standards, Policies, and Processes

Clerk provides access to and use of its technology resources to its employees and others, to support its mission. Access and use of Clerk technology resources is a privilege and requires that users of such technology resources act responsibly. Users shall only access and/or make use of Clerk technology resources in a manner that is consistent with applicable federal, state, and local laws and Clerk policies and procedures. Users accessing Clerk 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.

Users of Clerk technology resources must:

1. Follow all applicable federal, state, and local laws;
2. Follow all Clerk policies and procedures and IT standards;
3. Actively maintain the security of all devices accessing Clerk technology resources or being used to access, store, or process Clerk maintained data.
4. Actively maintain the security and privacy of data or Clerk maintained third-party data and store such data only in authorized locations, consistent with Clerk policies and standards.
5. Report privacy, security, or technology policy violations to the Clerk IT Security Manager.

Related Standards, Policies, and Processes (Continued)

User actions, such as those described below, of Clerk technology resources shall be considered misuse of its technology resources:

1. Utilizing any identity or account not specifically assigned by Clerk IT to the user;
2. Hindering, monitoring, or intercepting another user's network traffic;
3. Attempting to access, disclose, destroy, use, or modify Clerk technology systems or data without authorization of data owners;
4. Using technology resources for partisan political or campaign activities, such as making technology resources available to a candidate, campaign, political party, or political actions committee;
5. Using technology resources for commercial purposes (including but not limited to personal financial gain);
6. Using technology resources for personal or commercial purposes, excluding uses such as personal email or access to the internet, when such activities do not interfere with an individual's employment responsibilities at Clerk's Office;
7. Using technology resources for unlawful communications or activity, including threats of violence, obscenity, pornography, defamation, harassing communications (as defined by law), such as cyberstalking or other similar activities in violation of laws;
8. Using technology resources for the creation or transmission of materials which may put any person's personal safety at risk;
9. Using technology resources for unauthorized access to any system or network; and,
10. Engaging in the unauthorized copying, distributing, or transmitting of copyrighted materials such as software, music, or other media.

Contact Information

Information Technology Security (security@seminoleclerk.org) can assist with questions regarding this policy and related standards.

Definitions and Terms

Technology resources

All Clerk owned, operated, leased, or contracted computing, networking, telecommunications, and information resources;

All information maintained within Clerk computing resources;

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

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

Data owner

The unit administrator with direct responsibility for all access and use of designated types of data. Use of this term, in connection with this policy, shall not affect Clerk claims or rights of ownership of data or ownership of third-party data in possession of Clerk offices or technology resources.

Endpoint Protection Policy

The Endpoint Protection policy defines how the Clerk utilizes Endpoint Protection systems to assist in securing our technology resources from cybersecurity threats.

Purpose

In accordance with industry 'best practices' and to comply with numerous compliance regulations, Clerk 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 the endpoint protection policy at the Clerk's office.

Scope

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

Policy Compliance

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

Related Standards, Policies, and Processes

Ownership and Responsibility

All equipment and applications within this scope will be administered by the IT Operations Team. Administrative access to the Clerk end point servers and software will be governed by the Clerk's Operations Team and / or the Clerk Security Manager.

Endpoint Patches / Maintenance

All equipment and applications are maintained under a 24-hour technical support & software support contract directly with the vendor. The endpoint server and client software will be regularly monitored for firmware, security, and database updates:

- Software updates will be current version release and checked monthly. This allows the software to be up to date and in vendor's "General Release" version of use;
- Security updates will be current version release and checked weekly; and,
- Database updates will be current version release and checked automatically daily.

Definitions and Terms

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.

Email Policy

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 Clerk's offices.

Purpose

This policy has been developed to define the requirements for proper function and retention of electronic mail (e-mail) messages at Clerk.

Scope

The scope of this policy applies to electronic mail messages and associated messaging systems owned by the Clerk.

Policy Compliance

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

Related Standards, Policies, and Processes

Employees should primarily use company email systems for business purposes the following uses of company email systems are prohibited:

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

Electronic Message Server Patches / Maintenance

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

- 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.

- 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.

- 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). Definitions and Terms 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 (e-mail), a text message, an instant message (i.e., Teams or Skype), or a command or request to access an internet site.

Firewall Policy

Overview

The firewall policy defines how the Clerk primary network firewalls should handle inbound and outbound network traffic for specific IP addresses, address ranges, protocols, applications, and content types.

Purpose

In accordance with industry 'best practices' and to comply with numerous compliance regulations, Clerk 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 Clerk in defining and administering these policy and procedures.

Scope

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

Policy Compliance

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

Related Standards, Policies, and Processes

Ownership and Responsibility

All equipment and applications within this scope will be administered by the IT Networking Team. Administrative access to the Clerk firewalls will be governed by the IT Security Manager.

Firewall Patches / Maintenance

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

- 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;
- Security updates will be current version release and checked weekly;
- Database updates will be current version release and checked on the following schedule; and,
- Application and Threat databases ▪ Checked and updated every 30 minutes at 15 minutes past half hour.

Network Connections

All external and wireless connection to Clerk 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.

Network Firewall Physical Security

All Clerk network firewalls must be in a physically secure data center where access is controlled by the Clerk's Information Technology department.

Definitions and Terms

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

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 Information Technology department has implemented Network Firewalls between our internal networks and any external network (example: Internet, Seminole County, Court Administration, FDLE, DHSMV, and other networks).

Password Policy

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 staff, including contractors and vendors with access to Clerk technology resources are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

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

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.

Policy Compliance

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

Related Standards, Policies, and Processes

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.

4. Create unique passwords for each of your user accounts. You will likely have access to several systems requiring username 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.

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.

Administrator Accounts:

1. Administrator accounts will not have external email accounts.
2. Administrator accounts will require Multi Factor Authentication (MFA).

Definitions and Terms

Technology Resources

All Clerk owned, operated, leased, or contracted computing, networking, telecommunications, and information resources;

- All information maintained within the Clerk computing resources;
- All voice and data networks, telecommunications and communication systems and infrastructure;
- All technology resources including all hardware, software, applications, databases, and storage media.

Types of Authentication

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.

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 a technology resource.

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

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.

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.

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.

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

Server Policy

Overview

The server policy defines how Clerk servers should be used and maintained.

Purpose

In accordance with industry 'best practices' and to comply with numerous compliance regulations, Clerk 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 the server policy at Clerk's office in defining and administering these policy and procedures.

Scope

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

Policy Compliance

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

Related Standards, Policies, and Processes

Ownership and Responsibility

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

Server Patches / Maintenance

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

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.

Network Connections

All server connections to the Clerk's 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.

Definitions and Terms

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