INVOICE#	LINE	DUE DATE	INVOICE DATE	REFERENCE		PAYMENT AMOUNT	DIST GL ACCOUNT		CK SQ
				BLOOMSDALE BANK (GEN GOVT)					
			109	ALLIANCE WATER RESOURCES, INC.					
105127	1	7/03/24	7/01/24	PARK		8,137.44	20	20-20-8750	1
	2			STREET		29,526.56	21	21-21-8750	1
	3			WATER		52,513.02	30	30-30-8750	1
	4			SEWER		35,659.98	31	31-31-8750	1
					INVOICE TOTAL	125,837.00			
					VENDOR TOTAL	125,837.00			
			101642	AUDACY OPERATIONS					
2539327.6	1	7/03/24	6/30/24	WLC CTR		2,000.00	10	10-18-7163	1
					INVOICE TOTAL	2,000.00			
2700958-3	1	7/03/24	6/30/24	WLC CTR		1,589.80	10	10-18-7163	1
					INVOICE TOTAL	1,589.80			
2700959-3	1	7/03/24	6/30/24	WLC CTR		1,592.20	10	10-18-7163	1
					INVOICE TOTAL	1,592.20			
					VENDOR TOTAL	5,182.00			
			101104	COTTON'S ACE HARDWARE					
JULY 2024	1	7/03/24	7/03/24	POLICE		6.59	10	10-16-6200	1
	2			FIRE		75.92	10	10-17-6810	1
					INVOICE TOTAL	82.51			
					VENDOR TOTAL	82.51			
			101601	FORWARD SLASH TECHNOLOGY					
16806	1	7/03/24	7/01/24	CAPITAL PROJECTS		45.06	70	70-70-8219	1
					INVOICE TOTAL	45.06			
16818	1	7/03/24	7/01/24	ARPA CAPITAL PROJECTS		7,047.59	70	70-70-8219	1
					INVOICE TOTAL	7,047.59			
16835	1	7/03/24	7/01/24	CAPITAL PROJECTS		665.00	70	70-70-8055	1
	2			ADMIN		546.25	10	10-13-6805	1
	3			WATER		2,353.62	30	30-30-7059	1
	4			ADMIN		2,353.62	10	10-13-7059	1
	5			SEWER		2,353.63	31	31-31-7059	1
					INVOICE TOTAL	8,272.12			
					VENDOR TOTAL	15,364.77			
			100890	GFI DIGITAL					
2895035	1	7/03/24	6/26/24	ADMIN		176.01	10	10-13-6550	1
					INVOICE TOTAL	176.01			
					VENDOR TOTAL	176.01			
			101286	JEREMY BRAUER					
JULY 2024	1	7/03/24	7/03/24	JUDICAL		1,500.00	10	10-12-7030	1
	2			JUDICAL		137.50	10	10-12-7030	1

INVOICE#	LINE	DUE DATE	INVOICE DATE	REFERENCE		PAYMENT AMOUNT	DIST	GL ACCOUNT	CK SQ
					INVOICE TOTAL	1,637.50			
					VENDOR TOTAL	1,637.50			
			2590	MISSISSIPPI LIME CO					
1733214	1	7/03/24	6/25/24	WATER		3,652.37	30	30-30-6501	1
					INVOICE TOTAL	3,652.37			
1733737	1	7/03/24	6/27/24	WATER		3,970.54	30	30-30-6501	1
					INVOICE TOTAL	3,970.54			
1734819	1	7/03/24	7/03/24	WATER		3,894.67	30	30-30-6501	1
					INVOICE TOTAL	3,894.67			
					VENDOR TOTAL	11,517.58			
			101881	O'NEALL'S SEPTIC SERVICE, LLC					
12861	1	7/03/24	6/14/24	FRENCH HERITAGE - WLC CTR		160.00	10	10-18-7170	1
					INVOICE TOTAL	160.00			
					VENDOR TOTAL	160.00			
			101355	RHODES 101					
000429804	1	7/03/24	7/01/24	POLICE		1,843.66	10	10-16-6200	1
					INVOICE TOTAL	1,843.66			
					VENDOR TOTAL	1,843.66			
			101471	RMC, LLC					
130930	1	7/03/24	6/25/24	STREET		270.00	21	21-21-6105	1
					INVOICE TOTAL	270.00			
					VENDOR TOTAL	270.00			
			3790	SIDENER ENVIRONMENTAL SERVICES					
532788	1	7/03/24	3/24/24	WATER		1,307.90	30	30-30-6805	1
					INVOICE TOTAL	1,307.90			
95687	1	7/03/24	3/20/24	WATER		2,516.79	30	30-30-6805	1
					INVOICE TOTAL	2,516.79			
					VENDOR TOTAL	3,824.69			
			3740	STE GENEVIEVE HERALD					
JUNE 26 24 RENTAL	1	7/03/24	6/26/24	BLDG		15.40	10	10-14-6022	1
					INVOICE TOTAL	15.40			
					VENDOR TOTAL	15.40			
			3725	STE. GENEVIEVE CHAMBER					
8226	1	7/03/24	7/02/24	LEGIS		500.00	10	10-11-7156	1
					INVOICE TOTAL	500.00			
					VENDOR TOTAL	500.00			

INVOICE#	LINE	DUE DATE	INVOICE DATE	REFERENCE	PAYMENT AMOUNT	DIST GL ACCOUNT	CK SQ
			101882	VANDALIA LEADER UNION			
1040990	1	7/03/24	6/26/24	HORIZON GRANT - WLC CTR	1,100.50	10 10-18-7170	1
				INVOICE TOTAL	1,100.50		
				VENDOR TOTAL	1,100.50		
				BLOOMSDALE BANK (GEN GOV TOTAL	167,511.62		
				TOTAL MANUAL CHECKS	.00		
				TOTAL E-PAYMENTS	.00		
				TOTAL PURCH CARDS	.00		
				TOTAL ACH PAYMENTS	.00		
				TOTAL OPEN PAYMENTS	167,511.62		
				GRAND TOTALS	167,511.62		

BANK# / CHECK#	DATE	ACCOUNT#	NAME	CHECK AMOUNT	CLEARED	MANUAL	VOID	REASON FOR VOID
1 BLOOMSDALE BANK (GEN GOVT)								
12259168	7/01/2024	100937	AT & T	632.60		E-PAY		
12259169	7/01/2024	575	CITIZENS ELECTRIC CORP.	19,877.16		E-PAY		

* See Check Summary below for detail on gaps and checks from other modules.

BANK TOTALS:	
OUTSTANDING	20,509.76
CLEARED	.00
BANK 1 TOTAL	20,509.76
VOIDED	.00

FUND		TOTAL	OUTSTANDING	CLEARED	VOIDED
10	GENERAL	1,859.62	1,859.62	.00	.00
20	PARK	430.75	430.75	.00	.00
21	TRANSPORTATION TAX	2,475.48	2,475.48	.00	.00
27	CEMETERY	34.88	34.88	.00	.00
30	WATER	9,331.55	9,331.55	.00	.00
31	SEWER	6,377.48	6,377.48	.00	.00

Ste. Geneviève Missouri

Street Closure Request

Date 8-13-24

Name Amanda Hutchings Organization Downtown Ste. Genevieve Non-Profit

Address P.O. Box 13 City Ste. Genevieve State MO Zip 63670

Phone Number and/or email information dwntwnstegen@gmail.com

Reason for closure Pecanapalooza Street Festival

Street(s) to be closed Market St. (Dubourg Pl. to 3rd St.) + 3rd St. (Market to Merchant St.) + Merchant St. (3rd St. to Dubourg Pl.) Island of Flags

Date of event for closure Saturday, Nov 2nd

Time(s) for closure 10am - 6pm

Office Use Only

Council Approval	Yes __	No __	Date _____
Police Dept. Approval	Yes __	No __	Date _____
Street Dept. Approval	Yes __	No __	Date _____

Special Conditions _____

3D
ANT ST
DUBOURG PL
S THIRD ST
MARKET ST
Allow traffic

RESOLUTION 2024 - 39

A RESOLUTION OF THE BOARD OF ALDERMEN OF THE CITY OF STE. GENEVIEVE, MISSOURI ADOPTING THE INFORMATION TECHNOLOGY SECURITY POLICIES MANUAL.

WHEREAS, Forward Slash Technologies is recommending the adoption of new Information Technology Security Policies ("IT Security Policies") for the City of Ste. Genevieve that will replace the current Technology and Computer Policy that was adopted in 2020 by Resolution 2021-07; and

WHEREAS, the Board of Aldermen have reviewed the proposed policy, made recommendations and the need to establish said policy; and

WHEREAS, the Board of Aldermen wish to accept and approve the new IT Security Policies manual attached to and made part of this resolution.

NOW, THEREFORE, BE IT RESOLVED BY THE BOARD OF ALDERMEN OF THE CITY OF STE. GENEVIEVE, MISSOURI, AS FOLLOWS:

Section 1: The Board of Aldermen hereby adopts the Information Technology Security Policies (IT Security Policies) manual attached as Exhibit "A".

Section 2: That this resolution shall become effective immediately for the City of Ste. Genevieve.

PASSED AND APPROVED BY THE BOARD OF ALDERMEN OF THE CITY OF STE. GENEVIEVE, MISSOURI THIS 22nd DAY OF AUGUST, 2024.

Approved as to form:

_____
Brian Keim, Mayor

_____
Mark Bishop, City Attorney

SEAL

Reviewed by:

_____
Pam Meyer, City Clerk

_____
Happy Welch, City Administrator

Exhibit "A"

IT Security Policies

Original Date: April 16, 2024

Revision Date: July 15, 2024

Approved by:

Table of Contents

IT Policy Definitions 4
Acceptable Use – Computing Equipment 7
Acceptable Use – Removable Media 11
Removable Media Request Form 13
Acceptable Use – Remote Access 14
Access Control 16
Unique User ID 19
Password 21
Account Lock-out 23
Principle of Least Privilege 24
Data Backup 26
Change Management 28
Security Awareness Training 30
Hardening 32
Physical Hardware and Data Destruction / Re-Deployment 34
Physical Hardware and Data Destruction Authorization 36
Business Continuity Planning 37
Cybersecurity 39
Information Technology Security Policies 40
Email Protection 41
Two Factor Authentication (2FA) 43
BitLocker Encryption 44
Endpoint Detection and Response (EDR) 45
Email Phishing 47
Dark Web Monitoring 48
Vulnerability Scanning 50
Vulnerability Management 52
Penetration Testing 54

Incident Response 56
IT Security Policy Acknowledgment 58

IT Policy Definitions

Application Software – shall include all hosted and/or premise-based software and/or databases specifically authorized by **management** for use within the **information technology infrastructure**, whether purchased, leased, developed, or managed by the **Organization**.

Computing Equipment – shall include, but not be limited to desktop computers, laptops, notebooks, smartphones, smartwatches, servers, tablets, or any general-purpose device that can accept software.

Information Assets – shall mean any piece of information or data, stored in any manner which has any of the following characteristics, has value to the **Organization**, is not easily replaceable without cost, skills, time, or resources, or is part of the **Organization's** identity.

Information Security – shall mean the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of **sensitive or confidential information**, or the **information technology infrastructure** from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.

Information Security Officer (ISO) – is a member of **Information Technology Department** who is responsible for establishing and maintaining the **Organization's** vision, strategy, and program to ensure the **information technology infrastructure** is adequately protected. The **ISO**, or their designee, directs **workforce members** in identifying, developing, implementing, and maintaining processes across the **Organization** to reduce risks. The **ISO** responds to incidents, establishes appropriate standards and controls, manages security technologies, and directs the establishment and implementation of policies and procedures. The **ISO** is also responsible for compliance with all federal, state, local, and contractual obligations as it relates to the privacy and security of **sensitive or confidential information** and the **information technology infrastructure.**

Information Technology Department – shall mean the department(s) within or contracted with the **Organization** responsible for the configuration, support, and maintenance of the **information technology infrastructure**. Includes but is not limited to helpdesk, engineering, **network infrastructure, telecommunications**, and the Security Operations Center (SOC).

Information Technology Infrastructure – shall mean, but not limited to **computing equipment, network devices, network infrastructure,** and **telecommunications** technology owned, leased, or managed by the **Organization**.

Organization – shall mean a unit of people that is structured and managed to meet a need or to pursue a collective goal (i.e., City of Ste. Genevieve).

Management – shall mean the person or persons controlling and directing functions which coordinates the efforts of **workforce members** to accomplish goals and objectives efficiently and

effectively. **Management** shall include, but not be limited to planning, organizing, staffing, leading, directing and controlling the **Organization.**

Minimum Necessary Standard – shall mean that the **Organization** will take reasonable steps to limit unnecessary use, inappropriate access to and disclosure of **sensitive or confidential information** and all other **information assets** to the extent needed to perform assigned jobs duties.

Network Devices – shall mean components used to connect computers or other electronic devices. **Network devices** shall include, but not be limited to firewalls, switches, web filters, spam filters, wireless access points, backup devices, IP security cameras, security gateways, routers, bridges, hubs, and repeaters, as well as hybrid **network devices** such as multilayer switches, protocol converters, bridge routers, proxy servers, network address translators, multiplexers, network interface controllers, wireless network interface controllers, ISDN terminal adapters, line drivers, and various related hardware.

Network Infrastructure – shall include, but not be limited to all connections between the MDFs and IDF's, network/data racks, UPS, generators, patch panels, patch cables, ethernet cables, raceways, trays, and network door access controls.

Principle of Least Privilege – shall mean the practice of limiting access to the minimal level that will allow normal functioning. Applied to **workforce members,** the **Principle of Least Privilege** translates to giving **workforce members** the lowest level of privilege to perform job duties.

Removable Media – shall include, but not be limited to flash drives, external hard drives, memory sticks, SD cards, audio/video devices (tablets, iPods, MP3, or similar hybrid devices) smartphones, cell phones, smartwatches, micro drives, non-standard PDAs, optical discs, Blu-ray discs, DVDs, CDs, floppy disks, and magnetic tapes.

Sensitive or Confidential Information – shall mean all individual identifiable **information assets**, created, or maintained by the **Organization,** in all form (e.g., electronic, paper, verbal, etc.) whether at rest or in transit, which contain any of the following identifiers:

- Names
- All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census:
    - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people
    - The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
- All elements of dates (except year) for dates directly related to an individual, including birth date, date of death; and all ages over 89 and all elements of dates (including year) indicative

of such age, except that such ages and elements may be aggregated into a single category of age 90 or older

- Phone numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health plan member ID's
- Employee numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code
- Any medical or health data

Telecommunications – shall mean internet carrier services, internet modem, demarc, telephone systems, telephone handsets, voicemails, and any portable, mobile or desktop radios.

Workforce Members – shall include, but not limited to full and part-time employees, students and/or interns, contractors, vendors, service providers, volunteers and all other persons who conduct business on behalf of the **Organization**, regardless of whether they are paid by the **Organization**.

Acceptable Use – Computing Equipment

1. Purpose

   The purpose of this policy is to establish guidelines and standards regarding the acceptable use of **computing equipment** in accordance with the **Organization's** obligations to safeguard **sensitive or confidential information** and the **information technology infrastructure**.

2. Scope

   The scope of this policy applies to all **workforce members** who access any **computing equipment** owned, leased, managed and/or approved by the **Organization** to conduct business and services. All **workforce members** are responsible for exercising good judgement regarding the appropriate use of **information assets**, **computing equipment**, and **network devices** in accordance with the **Organization's** policies and standards, as well as local, state, and/or federal laws and regulations and contractual obligations. This policy will provide minimum standards for acceptable use for **computing equipment**.

   In relation to this policy, **computing equipment** shall include, but not be limited to; desktop, laptop, notebook, tablet, smartphone, servers, or any general-purpose device that can accept software.

3. Requirements

   The **Organization** is committed to preventing the loss or unauthorized access to **sensitive or confidential information** and hereby imposes the following mandatory restrictions on the use of **computing equipment**:

   - **Sensitive or confidential information** owned, leased, or managed by the **Organization** is strictly prohibited from being stored on any local **computing equipment** without management and the **Information Technology Department's** approval. All **sensitive or confidential information** should always be stored on secured file shares on the **Organization's** file servers or an approved **removable media** device in accordance with the Removable Media Device Policy.
   - **Workforce members** are responsible to promptly report the theft, loss, or unauthorized access of any **computing equipment** used to conduct business or services.
   - All **computing equipment** whether owned, leased, or managed by the **Organization** or approved BYOD (Bring Your Own Device) must always be password protected.
   - **Workforce members** are strictly prohibited from sharing unique user IDs and passwords with anyone. All unique user IDs and passwords must be treated as **sensitive or confidential information**. **Workforce members** may be asked for their password as part of a help desk support call in which they initiated. In that case, **workforce members** must change their passwords at the first opportunity in accordance with the Password Policy.
   - **Workforce members** must lock their screen or log off when their **computing equipment** is unattended.

- All **computing equipment** used by **workforce members** to conduct business and services that is connected to the **Organization's information technology infrastructure**, shall be continually executing approved virus-scanning software with a current virus database in accordance with the Vulnerability Management Policy.
- Under no circumstances is a **workforce member** authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the **Organization's computing equipment** or an approved BYOD. The lists below are by no means exhaustive but an attempt to provide a framework for activities which fall into the category of unacceptable use. The following activities are strictly prohibited, with no exceptions:

  - Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other application software that are not appropriately licensed for use by the **Organization**.
    Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the **Organization** or the **workforce member** does not have an active license is strictly prohibited.
    Accessing **information assets**, **computing equipment**, or an account for any purpose other than conducting the **Organization's** business, even if you have authorized access, is prohibited.
    Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate **management** should be consulted prior to the export of any material that is in question.
    Introduction of malicious programs onto any **computing equipment** (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
    Using the **Organization's computing equipment** to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
    Disruptions of the **information technology infrastructure** and/or causing security breach which includes, but is not limited to, accessing data of which the **workforce member** is not an intended recipient or logging into **computing equipment** that the **workforce member** is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
    Port scanning or security scanning is expressly prohibited without the **Information Technology Department's** prior authorization.
  - Executing any form of network monitoring which will intercept **information assets** not intended for the **workforce member's computing equipment** unless this activity is a part of the **workforce member's** normal job/duty.

Circumventing a **workforce member** authentication or security of any **computer equipment** or account.

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a **workforce member's information technology infrastructure's** connection, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, the **Organization's workforce members** to parties outside the **Organization**.
- Commercial use of the **information technology infrastructure** for non-**Organization** purposes.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email or telephone, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within the **Organization's information technology infrastructure** of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the **Organization** or connected via the **Organization's information technology infrastructure**.

For security and network maintenance purposes, the **Information Technology Department** will monitor the **information technology infrastructure**, and network traffic, per the Vulnerability Management Policy. The **Organization** reserves the right to audit the **information technology infrastructure** on a periodic basis to ensure compliance with this policy.

4. Responsibility

The following responsibilities have been implemented to ensure that this policy is enforced effectively across all parts of the **Organization**:

- All **workforce members** who require the use of **computing equipment** will be issued such devices by the **information technology infrastructure**. The **Organization** recognizes that **workforce member's** personally owned equipment (BYOD) can play a valuable role in convenience, efficiency, and productivity of its **workforce members**. All BYOD devices must be examined and approved by the **Information Security Officer** or their designee, prior to use or connectivity to the **Organization's** secured **information technology infrastructure**. The **Information Technology Department** reserves the right to determine the level of access for each BYOD device. The **workforce members** could be granted full, limited, or guest access.

- The **Information Technology Department** reserves the right to block or limit the use of certain third-party applications, such as those that probe the network or share files illegally, that may harm the **information technology infrastructure**. As the number of approved **application software** continually evolves, the **workforce member** must check with **Information Technology Department** to verify third-party applications and get the **Information Technology Department's** approval before downloading any new **application software** on an active, approved BYOD device.
- **Workforce members** must acknowledge that the use of BYOD devices in connection with business carries specific risks for which the **workforce members** will assume full liability. In the case of litigation, the **Organization** may take and/or confiscate a **workforce member's** personally owned device at any time.
- Reasonable precautions need to be made to protect **computing equipment** and should be to return it in good operating condition, including all accessories originally provided with the product, such as chargers, batteries, etc., at the **Organization's** request, or at the conclusion of employment with the **Organization**.
- The **computing equipment** shall not be used for nonwork-related tasks.
- The **computing equipment** shall only be used by approved **workforce members**.
- Lost or damaged **computing equipment** must be reported in a timely manner. In the event of a loss of, or damage to **computing equipment**, other than reasonable wear and tear, an incident report will be completed and reviewed to determine the cause of the incident. If negligence is the determined cause, the employee may be financially responsible for the replacement or repair of the **computing equipment** and may be subject to the **Organization's** Personnel Policy.

5. Violations / Enforcement

   Any known Violations of this policy shall be immediately reported to the **Organization's Information Security Officer**. Violations of this policy, including failure to report violations of this policy, may result in immediate termination and/or other disciplinary actions in accordance with the **Organization's** Personnel Policy.

6. Associated Documents

   Password Policy
   Acceptable Use - Removable Media Device Policy
   Vulnerability Management Policy

Acceptable Use – Removable Media

1. Purpose

   The purpose of this policy is to establish guidelines and standards regarding the Acceptable Use of Removable Media in accordance with the **Organization's** obligations to safeguard **sensitive or confidential information** and the **information technology infrastructure**.

2. Scope

   The scope of this policy applies to all **workforce members** and will provide the minimum standards for acceptable use of **removable media**.

   Removable media shall include, but not be limited to flash drives, external hard drives, memory sticks, SD cards, audio/video devices (tablets, iPods, MP3, or similar hybrid devices, smartphones, cell phones, smartwatches, micro drives, non-standard PDAs, optical discs, Blu-ray discs, DVDs, CDs, floppy disks, and magnetic tapes.

3. Requirements

   The **Organization** is committed to preventing the loss or unauthorized access to **sensitive or confidential information** and hereby imposes the following mandatory restrictions on the use of **removable media** devices:

   - **Workforce members** are strictly prohibited from using unauthorized **removable media** on any **computing equipment**.
   - All **removable media** must be issued and approved by the **Information Security Officer** or their designee.
   - All approved **removable media** shall only be used by authorized **workforce members** when other secure means are not available.
   - Authorized **workforce members** shall only use **removable media** for the purposes of storing or transporting data for work-related functions.
   - All **removable media** shall always be stored in a safe manner and all authorized **workforce members** shall take all necessary precautions to secure any **removable media** in their possession.
   - Use of any connection for unapproved access, transfer or storage of data owned, leased, or managed by the **Organization** is strictly prohibited.

4. Responsibility

The following responsibilities have been implemented to ensure that this policy is enforced effectively across all parts of the **Organization**:

- All **workforce members** who require use of **removable media** must submit the Removable Media Request Form to the **Information Security Officer** for review and approval prior to transferring any **information assets** onto **removable media**.
- The **Information Security Officer** will review requests ensuring that they are in compliance with all federal, state, local, and contractual obligations related to **sensitive or confidential information**. The **Information Security Officer** will recommend secure alternatives, where available.
- The **Information Security Officer** will provide **workforce members** with approved **removable media**. Additionally, he/or she will obtain the **workforce member's** acknowledgment of the **acceptable use of removable media**.

5. Violations / Enforcement

Any known Violations of this policy shall be immediately reported to the **Organization's Information Security Officer**. Violations of this policy, including failure to report violations of this policy, may result in immediate termination and/or other disciplinary actions in accordance with the **Organization's** Personnel Policy.

6. Associated Documents

Removable Media Request Form
Removable Media Acknowledgement

Removable Media Request Form

Workforce Member Name: _____

Reason for Request

Information Assets to be Transferred (be specific)

X _____ X _____

Date: _____ Date: _____

The following should be filled out by the IT Department

☐ Approved ☐ Not Approved

Decision Notes

Media Provided

X _____ X _____

Date: _____ Date: _____

Acceptable Use – Remote Access

1. Purpose

   The purpose of this policy is to establish guidelines and standards regarding the acceptable use of remote access in accordance with the **Organization's** obligations to safeguard **sensitive or confidential information** and the **information technology infrastructure**.

2. Scope

   The scope of this policy applies to all **workforce members** and all remote access connections used to remotely connect to the **information technology infrastructure** to do work on behalf of the **Organization**.

3. Requirements

   - Only authorized **workforce members** are permitted remote access to the **Organization's information technology infrastructure** and must adhere to all the **Organization's** policies and contractual obligations.
   - Remote access is only provided though the **Organization's** Virtual Private Network (VPN).
   - VPN access is limited to only **computing equipment** owned, leased, or managed by the **Organization**. **Workforce members** are strictly prohibited from accessing the **Organization's** network with any personal **computing equipment** unless it is an approved BYOD, in accordance with the Acceptable Use - Computing Equipment Policy.
   - VPN users are required to log-off and disconnect from the **Organization's information technology infrastructure** when access is no longer needed to perform job responsibilities.
   - VPN users must lock workstations when unattended to prevent unauthorized access to **sensitive or confidential information** or the **information technology infrastructure**.
   - VPN users will be automatically disconnected from the **Organization's information technology infrastructure** after a designated period of inactivity.
   - VPN users are strictly prohibited from viewing or accessing any **sensitive or confidential information** from any unsecure location.
   - VPN users are strictly prohibited from sharing their VPN unique user ID or password with anyone or configuring their VPN to remember or automatically enter their unique user ID and password. All VPN passwords must comply with the **Organization's** Password Policy.
   - Printing or copying **sensitive or confidential information** from a remote location is strictly prohibited.

4. Responsibility

   The following responsibilities have been implemented to ensure that this policy is enforced effectively across the **Organization**:

- **Workforce members** who require remote access must submit the User Access Form to the **Information Technology Department** for review and approval.
- Authorized **workforce members** will be issued approved **computing equipment** by the **Information Technology Department**.
- The **Information Technology Department** will install the approved VPN client on the approved **computing equipment.**
- The **Information Technology Department** will work with the **workforce members** to set up Cisco Duo in accordance with the Two Factor (2FA) Authentication Policy if applicable.
- The **Information Security Officer** will verify compliance with this policy through various methods, including but not limited to internal and external audits.

5. Violations / Enforcement

Any known Violations of this policy shall be immediately reported to the **Organization's Information Security Officer**. Violations of this policy, including failure to report violations of this policy, may result in immediate termination and/or other disciplinary actions in accordance with the **Organization's** Personnel Policy.

6. Associated Documents

Password Policy
User Access Form
Two Factor Authentication Policy
Acceptable Use - Computing Equipment

Access Control

1. Purpose

   The purpose of this policy is to establish guidelines and standards to prevent unauthorized access to **computing equipment**, **network devices**, and **sensitive or confidential information** within the **Organization's information technology infrastructure**.

2. Scope

   The scope of this policy applies to all **workforce members**, all file storage locations including all **computing equipment** and **network devices** within the **Organization's information technology infrastructure**.

3. Requirements

   Access control policies and procedures are required to regulate who can access the **Organization's sensitive or confidential information** and the **information technology infrastructure**.

   - Physical access to printed **sensitive or confidential information** must always be stored in a locked and /or secured location. Only **workforce members** with a specific "need to know" will be granted access to such **information assets** and access will be limited to the **minimum necessary standard** needed to complete the assigned task.
   - Access to the **information technology infrastructure** is controlled by a secure login process. The access controls defined in the Unique User ID, Password, Principal of Least Privilege and Account Lockout Policies must always be applied. The Login process must also be protected by Password characters hidden by symbols.
   - Access within **application software** which contains **sensitive or confidential information** must be restricted using the security features built into the **application software** in consideration of the **minimum necessary standard**. The access must also:
     - Be compliant with the **Organization's** Unique User ID, Password, Principal of Least Privilege and Account Lockout Policies.
     - Be separated into clearly defined roles.
     - Give the appropriate level of access required for the role of the **workforce member** to ensure that unauthorized **workforce members** do not have privileged access to **information technology infrastructure** and that authorization levels to administer and manage **information technology infrastructure** are appropriate.
     - Be unable to be overridden (with admin settings removed or hidden from the **workforce members**).

- Be free from altercation by rights inherited from the operating system that could allow unauthorized higher levels of access.
- Be logged and auditable. Additionally, access to all security logs and audit reports will be restricted to only authorized **workforce members**.

- The use of and controls for all the **Organization's information technology infrastructure** will be reviewed periodically, or at least annually to ensure access levels meet security requirements.
- Access to or use of **sensitive or confidential information** is strictly prohibited on mobile or portable devices, where deemed applicable by contractual obligations.
- All **workforce members** who require access to **sensitive or confidential information and the information technology infrastructure** will be identified. All level(s) of access and/or any conditions appropriate to such access will be maintained through the periodic, or at least annual review of job descriptions and access levels, in accordance with the Principal of Least Privilege Policy.
- Reasonable efforts will be made to limit a **workforce member's** access, in accordance with the **minimum necessary standard**, to only **sensitive or confidential information** and the **information technology infrastructure** needed to carry out his/her duties.
- For situations where access to or disclosure of **sensitive or confidential information** occurs on a routine and recurring basis, the access to or disclosure of **sensitive or confidential information** will be limited to the amount of information reasonably necessary to achieve the purpose of the access or disclosure.
- Vendor agreements will be reviewed periodically, or at least annually to ensure access to **sensitive or confidential information** being released meets the **Organization's minimum necessary standard**.
- Exceptions to the **minimum necessary standard** include:

  - Disclosures to the applicable client who provided the information; and
  - Disclosures otherwise required by law.

4. Responsibility

   The following responsibilities have been implemented to ensure that this policy is enforced effectively across all parts of the **Organization**:

   - The **Information Technology Department** will be responsible for the configuration of systems to enforce the requirements outlined herein.
   - The **Information Security Officer** will verify compliance with this policy through various methods, including but not limited to internal and external audits.

5. Violations / Enforcement

   Any known Violations of this policy shall be immediately reported to the **Organization's Information Security Officer**. Violations of this policy, including failure to report violations of this policy, may

result in immediate termination and/or other disciplinary actions in accordance with the **Organization's** Personnel Policy.

6. Associated Documents

Unique User ID Policy
Password Policy
Principal of Least Privilege Policy
Account Lockout Policy

Unique User ID

1. Purpose
   The purpose of this policy is to establish guidelines and standards for unique user identification and to ensure accountability of all **workforce members** that access the **Organization's information technology infrastructure.**

2. Scope
   The scope of this policy is to define the creation of a unique identifier for **workforce members** that access the **Organization's information technology infrastructure** that processes, stores, and/or transmits **sensitive or confidential information** that is owned, leased, or managed by the **Organization**. Use of a unique identifier provides a means to verify the identity of the **workforce member** accessing the **information technology infrastructure**. An effective unique user identification practice ensures that system activity can be traced to a specific **workforce member**.

3. Requirements

   - The **Organization** requires that each **workforce member** with access to the **Organization's information technology infrastructure** should be identified by a unique user ID.
   - A separate unique identifier is required for all **workforce members** who administer and maintain the **information technology infrastructure** in accordance with the Principle of Least Privileged Policy.
   - Wherever possible, built-in accounts, such as root and administrator accounts will be disabled.
   - The **Organization** requires **workforce members** to identify themselves uniquely before the **workforce members** are allowed to perform any action in the **information technology infrastructure.**
   - **Workforce members** are strictly prohibited from sharing their unique user IDs with other **workforce members** including **management**, or anyone at any time, unless authorized by the **Information Technology Department.**
   - The unique identification will be defined at the system level.

4. Responsibility

   - The **Information Technology Department** will be responsible for creating unique users IDs for access to the **information technology infrastructure**.
   - The **Information Technology Department** will perform ongoing maintenance of user IDs. User IDs that are not associated with an active **workforce member** present an increased risk for abuse. User IDs provided to **workforce members** will be disabled at the time of termination.

- The **Information Technology Department** may temporarily disable accounts for **workforce members** leaving for extended periods with no need to access the system, such as medical/family leave or vacations.
- **The Information Security Officer** will verify compliance with this policy through various methods, including but not limited to internal and external audits.

5. Exceptions
   Exceptions to the requirements outlined herein may be granted by the **Information Security Officer**, where deemed reasonable and necessary. The **Information Security Officer** will identify and mitigate risks to the **Organization's information technology infrastructure** in accordance with the Vulnerability Management Policy.

6. Violations / Enforcement
   Any known Violations of this policy shall be immediately reported to the **Organization's Information Security Officer**. Violations of this policy, including failure to report violations of this policy may result in immediate termination and/or other disciplinary actions in accordance with the **Organization's** Personnel Policy.

7. Associated Documents
   Vulnerability Management Policy
   Principle of Least Privileged Policy

Password

1. Purpose

   The purpose of this policy is to establish guidelines and standards for the creation of strong passwords, the protection of those passwords, and the frequency of change to ensure a secure and reliable **information technology infrastructure.**

2. Scope

   The scope of this policy applies to all **workforce members** who have or are responsible for an account or any form of access that supports a password on any **information technology infrastructure.**

3. Requirements

   - All passwords must meet industry standard complexity requirements.
   - Passwords must be a minimum of 8 characters in length. If a particular system will not support 8-character passwords, then the maximum number of characters allowed by that system shall be used.
   - Passwords must contain characters from at least 3 or the 4 ASCI character sets which include uppercase, lowercase, numeric, and special characters.
   - Passwords shall not:
     - Be composed of one or more dictionary words in any language or words with substitutions of numbers for letters such as p@ssw0rd.
     - Contain the same unique user ID which with they are associated.
     - Contain patterns or repeating combinations such as aaabbb, qwerty, zyxwvuts or 123321.
   - **Workforce members** are strictly prohibited from using the same password for multiple access needs, including, but not limited to, those accounts outside of the **Organization's information technology infrastructure.**
   - Passwords must not be shared with anyone unless authorized by the **Organization**. All passwords must be treated as **sensitive or confidential information**. **Workforce members** may be asked for their password as part of a help desk support call, which they initiated with the **Information Technology Department**. In that case, **workforce members** will be required to change their passwords as part of the support call.
   - **Workforce members** shall not write passwords down and store them anywhere in their office. Passwords stored in a file on **computing equipment** must be encrypted.
   - **Workforce members** are strictly prohibited from using the "Remember Password" feature of **application software** (for example, web browsers).

- Passwords must be changed from their default setting prior to deployment into the **Organization's information technology infrastructure.**
- All passwords including system-level and user-level passwords must be changed periodically, not to exceed 90 days.
- Passwords must have a minimum lifetime of at least 1 day.
- Applications and systems must remember (and not allow the use of) the last (at least) 12 passwords.
- **Workforce members** shall apply the above password requirements to any system or software application that does not enforce these requirements.

4. Responsibility

The following responsibilities have been implemented to ensure that this policy is enforced effectively across all parts of the **Organization**:

- The **Information Technology Department** will be responsible for the configuration of systems to enforce the requirements outlined herein.
- The **Information Security Officer** will verify compliance with this policy through various methods, including but not limited to internal and external audits.
- The **Information Technology Department** may deploy authentication mechanisms that are stronger than passwords, as necessary.

5. Violations / Enforcement

Any known Violations of this policy shall be immediately reported to the **Organization's Information Security Officer**. Violations of this policy, including failure to report violations of this policy, may result in immediate termination and/or other disciplinary actions in accordance with the **Organization's** Personnel Policy.

Account Lock-out

1. Purpose

   The purpose of this policy is to establish guidelines and standards to prevent unauthorized access to the **Organization's information technology infrastructure**.

2. Scope

   The scope of this policy applies to all **workforce members** who have or are responsible for accessing any **information technology infrastructure**.

3. Requirements

   - All **information technology infrastructure** must be manually locked when unattended to prevent unauthorized access.
   - The Account Lockout Policy in Active Directory is configured to limit user login attempts to no more than six (6) successive attempts. Upon lockout, **workforce members** must contact the helpdesk and verify their identity to have their accounts unlocked.
   - **Workforce members** are strictly prohibited to contact the Help Desk on behalf of another **workforce member** in the event of an account lockout.

4. Responsibility

   The following responsibilities have been implemented to ensure that this policy is enforced effectively across all parts of the **Organization**:

   - The **Information Technology Department** will be responsible for the configuration of systems to enforce the requirements outlined herein.
   - The **Information Security Officer** will verify compliance with this policy through various methods, including but not limited to internal and external audits.

5. Violations / Enforcement

   Any known Violations of this policy shall be immediately reported to the **Organization's Information Security Officer**. Violations of this policy, including failure to report violations of this policy, may result in immediate termination and/or other disciplinary actions in accordance with the **Organization's** Personnel Policy.

Principle of Least Privilege

1. Purpose

   The purpose of this policy is to establish guidelines and standards to address the **Organization's** obligations relating to the **principle of least privilege**. **Workforce members** are only given the privileges necessary to accomplish the intended purpose or task.

2. Scope

   The scope of this policy applies to all **information technology infrastructure**. Privileged access enables a **workforce member** to take actions which may affect the **information technology infrastructure** and **information assets**, or accounts. Privileged access is only granted to those **workforce members** whose job duties require special privileges over the **information technology infrastructure**.

3. Requirements

   - All **workforce members** who require privileged access to the **information technology infrastructure** will be identified through the **Organization's** User Access Form.
   - Privileged access is only granted to those **workforce members** whose job duties require special privileges over the **information technology infrastructure**.
   - Reasonable efforts should be made to limit each privileged user's access to only the **information technology infrastructure** that is needed to carry out his/her duties.
   - If methods other than using privileged access will accomplish a task / action, those other methods must be used.
   - Vendor Agreements will be amended to ensure that privileged access is only granted to those vendors whose services require elevated privileges and that access is limited to the **information technology infrastructure** needed to carry out the specific services outlined in their Vendor Service Agreement.
   - Requests for privilege access from any **workforce member** must be approved by **management** and the **Information Security Officer** or his/her designee to ensure the least amount of privilege (which is reasonably necessary to accomplish the purpose) is granted in accordance with the **minimum necessary standard**.
   - Separate accounts will be created for privileged access. **Workforce members** are strictly prohibited from using such elevated privileges when it is not necessary to perform assigned duties.

4. Responsibility

   The following responsibilities have been implemented to ensure that this policy is enforced effectively across all parts of the **Organization**:

- All User Access Forms will be reviewed and approved by **management** and the **Information Technology Department** to ensure that access is granted in compliance with the Principle of Least Privilege Policy and **minimum necessary standard**.
- The **Organization** will evaluate job responsibilities periodically, or at least annually, and access privileges will be modified as necessary.
- Prior to receiving special privileged access, **workforce members** will be required to review and acknowledge the receipt and understanding of this policy.
- **Workforce members** with privileged access shall take necessary precautions to protect the **sensitive or confidential information** encountered in the performance of their duties.

5. Violations / Enforcement

Any known Violations of this policy shall be immediately reported to the **Organization's Information Security Officer**. Violations of this policy, including failure to report violations of this policy may result in immediate termination and/or other disciplinary actions in accordance with the **Organization's** Personnel Policy.

6. Associated Documents

User Access Form
Principle of Least Privilege Policy

Data Backup

1. Purpose

   The purpose of this policy is to establish guidelines and standards to address the need for performing periodic backups of the **Organization's information technology infrastructure.**

2. Scope

   The scope of this policy applies to **information assets** created, maintained, used, or stored within the **Organization's information technology infrastructure.**

3. Requirements

   - The **Organization** recognizes that **information assets** can be destroyed by a system malfunction, whether the incident is accidental or intentional. Maintaining adequate backups will ensure **information assets** are recoverable.
   - The ongoing availability of the **Organization's information technology infrastructure** is critical to the operation of the business. To minimize any potential loss or corruption of such **information assets**, the **Organization** will adequately backup **information assets** by establishing and following appropriate backup procedures.
   - All **information technology infrastructure** assets that create, update, or store mission critical **information assets** will be backed up daily to an approved backup system.
   - Logged information generated from each backup will be reviewed daily for the following purposes:

     - To check and correct errors.
     - To monitor the duration of the backup.
     - To optimize backup performance where possible.
     - To identify problems and take corrective action to reduce any risks associated with failed backups.

   - The **Information Technology Department** performs random tests periodically to verify integrity.
   - The **Information Technology Department** will maintain records demonstrating the review of backup logs and test restores to verify compliance with this policy for auditing purposes.

4. Responsibility

   The following responsibilities have been implemented to ensure that this policy is enforced effectively across all parts of the **Organization**:

- The **Information Technology Department** will be responsible for the selection of sources, scheduling of backups, and any necessary restores.
- The **Information Security Officer** will verify compliance with this policy through various methods, including but not limited to internal and external audits.

5. Violations / Enforcement

Any known Violations of this policy shall be immediately reported to the **Organization's Information Security Officer**. Violations of this policy, including failure to report violations of this policy, may result in immediate termination and/or other disciplinary actions in accordance with the **Organization's** Personnel Policy.

Change Management

1. Purpose

   The purpose of this policy is to establish guidelines and standards regarding change management in accordance with the **Organization's** obligations to safeguard **sensitive or confidential information** and the **information technology infrastructure**.

2. Scope

   The scope of this policy applies to the **Organization's information technology infrastructure**.

3. Requirements

   Change Management shall include the process of requesting, analyzing, approving, developing, implementing, and reviewing planned or unplanned changes within the **Organization's information technology infrastructure**. The Change Management process will include documentation and subsequent actions:

   - Changes must be formally requested; All requests for change will be documented.
   - Categorize, prioritize, analyze, and justify the change; the **Organization** will identify and document justification for the change which shall include, but not be limited to, assessing the urgency, researching, and classifying risks, and identifying the impact of the change on the **information technology infrastructure**, end user productivity, and budget.
   - Approval; Where necessary, change requests will require technical approvals, business / data owners' approvals and, in the event of a major or significant change, the **Information Security Officer's** approval.
   - Plan and complete the implementation of the change; This process shall include gathering the technical requirements, reviewing the specific implementation steps, and completing the change in a manner that will minimize the impact on the **information technology infrastructure**, end **workforce members**, and clients.

   The primary functional components covered herein include:

   - **Application Software** – Installation, patching, upgrade, or removal of **application software** products including operating systems, access methods, commercial off-the-shelf (COTS) packages, internally developed packages, and utilities. Application software changes being promoted to production as well as the integration of new application systems and the removal of obsolete elements.
   - Hardware – Installation, modification, removal, or relocation of **computing equipment**.

- Moves, Adds, Changes and Deletes – Changes to system configurations, including security groups and file permissions.
- Schedule Changes – Requests for creation, deletion, or revision to job schedules, back-up schedules or other regularly scheduled jobs managed by the **Information Technology Department**.
- Telephony – Installation, modification, de-installation, or relocation of equipment and services.
- Desktop – Any modification or relocation of **computing equipment** and services.
- Generic and Miscellaneous Changes – Any changes that are required to complete tasks associated with normal job requirements.

Tasks that require an operational process, but are outside the initial scope of this policy include:

- Business Contingency Planning
- Changes to non-production elements or resources
- Changes made within the daily administrative process which include, but are not limited to

  - Password resets
  - User adds/deletes
  - User modifications
  - Rebooting machines when there is no change to the configuration of the system

4. Responsibility

The following responsibilities have been implemented to ensure that this policy is enforced effectively across all parts of the **Organization**:

- The **Information Technology Department** will be responsible for properly documenting and following the change management process.
- The **Information Security Officer** will verify compliance with this policy through various methods, including but not limited to internal and external audits.

5. Violations / Enforcement

Any known Violations of this policy shall be immediately reported to the **Organization's Information Security Officer**. Violations of this policy, including failure to report violations of this policy, may result in immediate termination and/or other disciplinary actions in accordance with the **Organization's** Personnel Policy.

Security Awareness Training

1. Purpose

   The purpose of this policy is to establish guidelines and standards for **workforce member's** security awareness training. Security awareness training is an important aspect in protecting **sensitive or confidential information** and **information technology infrastructure**. **Workforce members** are the first line of defense and must be made aware of the security risks.

2. Scope

   The scope of this policy applies to all **workforce members**.

3. Requirements

   - All **workforce members** accessing the **Organization's information technology infrastructure** must understand how to protect **sensitive or confidential information**.
   - The **Organization** will ensure that all **workforce members** are given security awareness training on a quarterly basis. This training shall cover a variety of security topics selected by the **Information Security Officer**.
   - The **Organization** will also conduct refresher training for all **workforce members** anytime there are significant changes to the **Organization's** published IT security policies and procedures.

4. Responsibility

   The following responsibilities have been implemented to ensure that this policy is enforced effectively across all parts of the **Organization**:

   - **Workforce members** are responsible to review and acknowledge required IT Security Policies as well as complete all IT security awareness campaigns.
   - **Workforce members** should understand and follow all security related policies and procedures and ask **management** or the **Information Technology Department** for clarification when needed.
   - **Management** is responsible for ensuring all **workforce members** complete the required security awareness training at the required intervals.
   - The **Information Security Officer** is responsible for the selection and delivery of industry standard security training materials necessary to carry out required security awareness training activities within the **Organization**.

- **Management**, along with the **Information Technology Department** and the **Information Security Officer**, are responsible for ensuring all **workforce members** understand all security-related policies and procedures.
- The **Information Technology Department** is responsible for providing **management** with quarterly **workforce member** training reports.

5. Violations / Enforcement

   Any known Violations of this policy shall be immediately reported to the **Organization's Information Security Officer**. Violations of this policy, including failure to report violations of this policy, may result in immediate termination and/or other disciplinary actions in accordance with the **Organization's** Personnel Policy.

Hardening

1. Purpose

   The purpose of this policy is to establish guidelines and standards regarding the hardening of the **Organization's information technology infrastructure**.

2. Scope

   The scope of this policy applies to the **information technology infrastructure**.

3. Requirements

   The **Organization** is committed to preventing cyber security attacks through the establishment of strong hardening policies. Hardening is the process of securing a system by reducing its surface vulnerabilities. It is possible to reduce the number of possible vectors of attack by the removal of any software, access accounts and disabling of services that are not related to or required by known system functions. To comply with this policy:

   - Only **application software** that has been approved for use by **management** and the **Information Security Officer** may be installed on **computing equipment**.
   - Unessential **application software** and services will be uninstalled and/or disabled.
   - The boot order of **computing equipment** must be configured to prevent unauthorized booting from alternative media.
   - Access to local administrator accounts will be restricted to **workforce members** of the **Information Technology Department**, where possible.
   - Strong authentication will be required for all administrative and/or privileged access to all **information technology infrastructure** including, but not limited to, any access for the purpose of reviewing log files.
   - Default user IDs and passwords will be disabled or changed where possible, following installation and before use in the production environment.
   - All **computing equipment** will be protected by anti-virus software. The anti-virus software will be configured to automatically download the latest threat databases, and to perform weekly full scans in accordance with the Vulnerability Management Policy.
   - All **computing equipment** will be protected by EDR and cyber security agents in accordance with the Cyber Security Policy.
   - All **computing equipment** in the **Organization's information technology infrastructure** will be scanned for vulnerabilities bimonthly in accordance with the Vulnerability Scanning Policy.
   - All devices in the **Organization's information technology infrastructure** will be patched in accordance with the Vulnerability Management Policy.

4. Responsibility

The following responsibilities have been implemented to ensure that this policy is enforced effectively across all parts of the **Organization**:

- All **workforce members** of the **Information Technology Department** will be responsible for the enforcement of the requirements outlined herein.
- The **Information Security Officer** will verify compliance with this policy through various methods, including but not limited to internal and external audits.

5. Violations / Enforcement

Any known Violations of this policy shall be immediately reported to the **Organization's Information Security Officer**. Violations of this policy, including failure to report violations of this policy, may result in immediate termination and/or other disciplinary actions in accordance with the **Organization's** Personnel Policy.

6. Associated Documents

Cyber Security Policy
EDR Policy
Vulnerability Management Policy
Vulnerability Scanning Policy