

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.13 SUBJECT: Physical Hardware and Data Destruction / Re-Deployment		Page 34 of 59

## Physical Hardware and Data Destruction / Re-Deployment

### 1. Purpose

The purpose of this policy is to establish guidelines and standards to establish the **Organization's** obligations regarding to the proper destruction of **sensitive or confidential information** and the disposal, recycling, or reuse of any **information technology infrastructure** assets.


### 2. Scope

The scope of this policy applies to all **sensitive or confidential information** in all forms including, but not limited to, printed, typed, or handwritten and any **information technology infrastructure** assets that are no longer utilized by the **Organization**.

### 3. Requirements

- Upon expiration or request, all printed, typed, or handwritten material generated by, received, or stored by the **Organization** which contains **sensitive or confidential information** must be placed in a secured shredding containers for proper destruction or returned to the applicable party as deemed by any prior agreement.
- **Workforce members** are strictly prohibited from disposing of any printed, typed, or handwritten material, which contains **sensitive or confidential information**, in non-secured containers for disposal.
- **Information technology infrastructure** assets identified as "end of life" will be forwarded to the **Information Technology Department** for proper disposal.
- All storage mediums will be securely erased in accordance with industry best practices and analyzed for destruction or re-deployment.
- All electronic **information assets** will be removed from **computing equipment** using industry standard secure deletion methods prior to destruction or re-deployment.
- No **information technology infrastructure** assets will be disposed of via dumps, landfills, etc.
- All hard drives must be degaussed, overwritten with a commercially available disk cleaning program, or rendered unreadable by drilling, crushing or other demolition methods prior to destruction.
- **Information technology infrastructure** with non-functioning memory or storage technology will have the memory or storage device removed and will be rendered unreadable by drilling, crushing or other demolition methods prior to destruction.
- All destruction and redeployment activities will be authorized, properly documented and maintained by the **Information Technology Department**.

### 4. Responsibility

		Original Date: Revision Date: Approved By:
POLICY#: SOC-Policy.13 SUBJECT: Physical Hardware and Data Destruction / Re-Deployment		Page 35 of 59

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


- Secured shredding containers or shredding equipment will be placed in strategic locations throughout the building(s).
- The **Information Technology Department** will contract with a certified electronics recycler (SERI R2v3 Standard) and will oversee and certify all data destruction and asset management activities.
- The **Information Security Officer** will verify compliance with this policy through various methods, including but not limited to, internal and external audits of asset management activities.

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

- Shredding/Recycling Vendor Service Agreement
- Physical Hardware and Data Destruction Authorization

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Form.05 SUBJECT: Physical Hardware and Data Destruction / Re-Deployment Acknowledgment		Page 36 of 59

## Physical Hardware and Data Destruction Authorization

	<h3>Hardware For Secure Destruction</h3>				
Customer: _____			Date: _____		
Device Name	Last Logged in User	Location	Serial Number	Reason for Destruction	Certificate *
					<input type="checkbox"/> Yes
					<input type="checkbox"/> Yes
					<input type="checkbox"/> Yes
					<input type="checkbox"/> Yes
I have reviewed the above list of items and approve the secure destruction of all hardware listed.					
Signature: _____			Date: _____		

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.15 SUBJECT: Business Continuity Planning		Page 37 of 59

## Business Continuity Planning

### 1. Purpose

The purpose of this policy is to establish guidelines and standards for the development, testing, and annual maintenance of a business continuity plan.


### 2. Scope

The scope of this policy applies to **workforce members** who are accountable to ensure that a Business Continuity Plan is developed, tested, and maintained.

### 3. Requirements

Business continuity planning is critical to the recovery of the **Organization** should an internal or external event occur.

- The **Organization's** Business Continuity Plan is designed to quickly recover, and resume business operations should an internal or external event occur. The business continuity plan will provide guidelines to safeguard and protect the **Organization's workforce members** and property, financial and operational assessments, **information assets**, and records and to minimize disruption to business activities.
- The **Organization** will establish a business continuity team and organizational chart that identifies **workforce members**, and their roles and responsibilities should an internal or external event occur.
- The **Organization** will conduct a periodic, or at least annual, business impact assessment to identify risks and vulnerabilities utilizing the Failure Mode Effect Analysis methodology.
- The Business Continuity Plan will include:
  - Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
  - Succession Plan: A description of the flow of responsibility when normal staff are unavailable to perform their duties.
  - Data Study: A detailed list of the data stored on the systems, its criticality, and its confidentiality.
  - Criticality of Service List: A list of all the services the **Organization** provides and their order of importance, including recovery time objectives in the order of recovery for both short-term and long-term timeframes.
  - Data Backup and Restoration Plan: A detailed list of what data is backed up, the devices used to store data, storage location, back up cycle and the process for restoring and recovering data.

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.15 SUBJECT: Business Continuity Planning		Page 38 of 59

- Equipment Replacement Plan: An equipment list with description, model numbers, usage, suppliers/contact information and importance of equipment for continuance of operations.
- Communication Management: An outline of responsibilities associated with internal and external communication, designated personnel and guidelines for appropriate communications and responses.
- The **Organization** will assemble an Emergency Response Team (ERT) dedicated to safeguarding **workforce members** and facilities in times of emergency. The ERT will be trained to assess casualties and stabilize **workforce members** to the best of their abilities. First Aid Responders, who are part of the ERT will receive professional training in CPR and first aid, no less than every two years and will be responsible for accessing and stabilizing casualties in the event of an accident.
- The business continuity plan will be tested periodically, or at least on an annual basis. Results will be documented, and failures will be assessed and corrected.
- The business continuity plan will be furnished to clients upon request to ensure the **Organization's** compliance with contractual obligations. As deemed necessary, the **Organization** will promptly update its business continuity plan to include potential threat scenarios.


#### 4. Responsibility

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

- The Business Continuity Team will be responsible for conducting the periodic, or at least annual, business impact assessment to identify risks and vulnerabilities.
- The Business Continuity Team will be responsible for the periodic, or at least annual, testing of the business continuity plan.
- The **Organization's Information Security Officer** will serve as the ERT Leader and be responsible for the periodic, or at least annual review and maintenance of safety procedures.
- 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**.

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.15 SUBJECT: Cybersecurity		Page 39 of 59

## Cybersecurity

### 1. Purpose

The purpose of this policy is to establish guidelines and standards regarding cybersecurity for the **information technology infrastructure**.

### 2. Scope

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

### 3. Requirements

- The **Organization** is committed to preventing cyber security attacks through the establishment of strong policies
- The **Organization** will establish and/or engage with a Security Operations Center (SOC) to provide 24x7x365 monitoring and response to cybersecurity incidents. EDR agents will be deployed on all workstations, servers and firewalls in accordance with the EDR Policy.
- The SOC will be responsible for continuous improvement of the security posture and effectiveness of the **Information Technology Department's** tools and strategies, real-time trending and expanded data analytics, event log and activity tracking, as well as security incident and notification records.


### 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 enforcement of the requirements outlined herein.
- The **Information Security Officer** will be responsible for configuring monitoring systems.
- 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**.

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.16 SUBJECT: Information Technology Security		Page 40 of 59

## Information Technology Security Policies

### 1. Purpose

The purpose of this policy is to establish guidelines and standards regarding the **Information Technology Department's** security policies designed to protect the **Organization's information technology infrastructure**.

### 2. Scope

The scope of this policy applies to the **information technology infrastructure** owned, leased, or managed by the **Organization**.

### 3. Requirements

The **Organization** is committed to preventing cyber security attacks and system vulnerabilities through the establishment of strong policies and procedures. This is the policy regarding the monitoring and improvement of policies.

- All IT security policies will be routinely reviewed and updated as new systems, technologies, and abilities are integrated into the **information technology infrastructure**.
- At a minimum, all policies will be reviewed on an annual basis.


### 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** or their designee, will be responsible for maintaining all IT Security Policies.
- 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**.

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.17 SUBJECT: Email Protection		Page 41 of 59

## Email Protection

### 1. Purpose

The purpose of this policy is to establish guidelines and standards regarding the protection of the email system.

### 2. Scope

The scope of this policy applies to the **Organization's** Microsoft 365 email system.

### 3. Requirements

The **Organization** is committed to preventing cyber security attacks through the establishment of strong policies. Email is defined as messages distributed by electronic means from one computer user to one or more recipients via a network. Email protection services and the deployment of security tools are essential to protecting email systems and allow the **Information Technology Department** to monitor emails for unwanted or malicious activity.

The following security protocols must be enforced:

- 2FA/multifactor authentication
- Email security (spam and malware protection)
- Advanced threat detection
- Data loss prevention
- Tamper proof email archive
- Cloud-to-cloud backup and recovery
- Phishing and impersonation protection
- Account takeover protection
- Forensics and incident response

### 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.
- All **workforce members** of the **Information Technology Department** are responsible for the identification and remediation of all detected threats and attacks.
- The **Information Technology Department** will monitor the completion of daily backups and archiving activities and documents as part of the daily checklist activities.
- The **Information Security Officer**, or their designee, will be responsible for the selection and configuration of monitoring systems.



		Origined Date: Revision Date: Approved By:
POLICY#: SOC-Policy.17 SUBJECT: Email Protection		Page 42 of 59

- 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**.

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.18 SUBJECT: Two Factor Authentication (2FA)		Page 43 of 59

## Two Factor Authentication (2FA)

### 1. Purpose

The purpose of this policy is to establish guidelines and standards for the use of two factor authentication (2FA) to ensure security and reliability of the **information technology infrastructure**.

### 2. Scope

The scope of this policy applies to all **workforce members** who have an active email address or remotely access the **Organization's information technology infrastructure**.

### 3. Requirements

- All **workforce members** who have access to the **Organization's** email system or remotely access the **information technology infrastructure** must use Two Factor Authentication (2FA) to enhance the security posture and prevent unauthorized use of their email or the **information technology infrastructure**.
- All **workforce members** will have five days from the date of hire to contact the **Information Technology Department** to set up 2FA via an approved authenticator. After which the 2FA will be enforced and the **workforce member** will be unable to access email or connect remotely until the **workforce member** contacts the **Information Technology Department**.
- Two Factor (2FA) Authentication is required for all remote access via Cisco Duo in accordance with the Acceptable Use - Remote Access Policy where applicable.

### 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

Acceptable Use – Remote Access

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.19 SUBJECT: BitLocker Encryption		Page 44 of 59

## BitLocker Encryption

### 1. Purpose

The purpose of this policy is to establish guidelines and standards for the use of BitLocker encryption to ensure security and reliability of the **Information technology infrastructure**.

### 2. Scope

The scope of this policy applies to all **workforce members** who have or are responsible for any **computing equipment** that contains **sensitive or confidential information** within the **Organization's Information technology infrastructure**.

### 3. Requirements

- All **computing equipment** that contains **sensitive or confidential information** will be required to have BitLocker encryption enabled.

### 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**.

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.20 SUBJECT: Endpoint Detection and Response (EDR)		Page 45 of 59

## Endpoint Detection and Response (EDR)

### 1. Purpose

The purpose of this policy is to establish guidelines and standards regarding the security 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 policies and procedures. EDR services monitor specific endpoints (workstations and servers) for unwanted or nefarious activity.

- EDR monitoring agents will be deployed on all identified **computing equipment**, prior to deployment in the production environment in accordance with the Hardening Policy.
- The Security Operations Center will report compromised endpoints to the **Information Technology Department**.
- Actions to mitigate threats such as isolation from the **information technology infrastructure** will be taken in accordance with the Incident Response Policy.
- After analysis, the alerts that are generated, various options ranging from isolating the machine to removing suspicious files will be taken.

### 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 be responsible for configuring, deploying, and monitoring systems.
- 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**.




Originated Date:  
Revision Date:  
Approved By:

POLICY#: SOC-Policy.20  
SUBJECT: Endpoint Detection and Response (EDR)

Page  
46 of 59

6. Associated Documents
  - Incident Response Policy
  - Hardening Policy

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.22 SUBJECT: Email Phishing		Page 47 of 59

## Email Phishing

### 1. Purpose

The purpose of this policy is to establish guidelines and standards regarding the **Organization's** obligations relating to **workforce member's** email phishing awareness. **Workforce members** are the first line of defense and must be made aware of such security risks.

### 2. Scope

The scope of this policy applies to all **workforce members**. Phishing is the fraudulent practice of sending emails or other messages purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers.

### 3. Requirements

- All **workforce members** accessing the **Organization's information technology infrastructure** must understand how to protect **sensitive or confidential information** and the **information technology infrastructure**.
- The **Organization** will provide email phishing campaigns on at least a quarterly basis.


### 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 for understanding and following all security-related policies and procedures and asking **management** or the **Information Technology Department** for clarification when needed.
- The **Information Security Officer** is responsible for the selection and delivery of industry standard security phishing materials necessary to carry out required phishing activities within the **Organization**.
- The **Information Technology Department** will provide quarterly phishing reports to **management**.

### 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**.

		Originated Date: Revision Date: Approved by:
POLICY#: SOC-Policy.22 SUBJECT: Dark Web Monitoring		Page 48 of 59

## Dark Web Monitoring

### 1. Purpose

The purpose of this policy is to establish guidelines and standards for Dark Web monitoring to ensure the security and reliability of the **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 policies and procedures. Dark web is defined as the part of the world wide web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable. Dark web monitoring is a process of searching for and monitoring information on the dark web. It is designed to find stolen or leaked information, such as compromised passwords, credentials, intellectual property, and other **sensitive or confidential information** being shared and sold among criminals operating on the dark web. To comply with this policy,

- The **Organization** will use industry standard dark web monitoring tools.
- The **Information Technology Department** will review and analyze compromises daily as part of the SOC daily checklist.
- Mitigations will be based on the information that is found.
- Information that is publicly available will not necessitate any remediation.
- The **Information Technology Department** will contact **workforce members** directly for any password hits. Reuse of compromised passwords 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** of the **Information Technology Department** will be responsible for the enforcement of the requirements outlined herein.
- The **Information Security Officer** will be responsible for the selection and configuration of monitoring systems.
- 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

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.22 SUBJECT: Dark Web Monitoring		Page 49 of 59

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



		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.23 SUBJECT: Vulnerability Scanning		Page 50 of 59

## Vulnerability Scanning

### 1. Purpose

The purpose of this policy is to establish guidelines and standards to assist in maintaining a secure and reliable **information technology infrastructure**.

### 2. Scope

The scope of this policy applies to the **information technology infrastructure**. Vulnerability Scanning includes, but is not limited to, scanning for patch levels, scanning for functions, ports, protocols, and services that should not be accessible and scanning for improperly configured or incorrectly operating information flow control mechanisms.

### 3. Requirements

Vulnerability Scanning is an information gathering process which identifies weaknesses in the **information technology infrastructure** that could compromise the infrastructure. Bi-monthly Vulnerability Scans will be conducted as part of the **Organization's** continual evaluation process of risk and vulnerability management.

- The **Organization** will use industry standard security vulnerability scanning software to carry out all vulnerability scanning and audit reporting within the **information technology infrastructure**. Several tools may be used for security vulnerability scanning and the tool set will be reviewed periodically, or at least annually by the **Information Security Officer**.
- Vulnerability Scanning tools must be capable of performing the following tasks:
  - Host Discovery – Identifying **computing equipment** listed in the **Organization's information technology infrastructure**
  - Operating System Detection
  - Scanning for patch levels, functions, ports, protocols, and services
  - Software Version Detection
  - Network-based vulnerability scanning
  - Operating systems security patch auditing
  - Database vulnerability auditing
  - Anti-virus auditing
- Any new **information technology infrastructure** must undergo vulnerability scanning prior to deployment to the production network.
- Vulnerability Scanning may cause network performance or availability issues. The **Organization's Information Technology Department** will make reasonable efforts to minimize such issues.

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.23 SUBJECT: Vulnerability Scanning		Page 51 of 58

- All devices owned, leased, or managed by the **Organization** within the **information technology infrastructure** are subject to security Vulnerability Scanning.
- At the conclusion of each scan, all discovered vulnerabilities will be documented. The reports produced by the vulnerability scanning tool may be used as the above documentation. Reports will be provided to **management** upon request from the **Information Technology Department**.

#### 4. Responsibility

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


- The **Information Security Officer** is responsible for the selection and deployment of industry standard security vulnerability scanning software to carry out all vulnerability scanning and audit reporting within the **Organization's information technology infrastructure**.
- The **Information Security Officer** ensures bi-monthly vulnerability scans are performed and the evaluation and mitigation of the results of the vulnerability scans are completed in accordance with the Vulnerability Management Policy.
- The **Information Security Officer** will maintain scan reports to track scanning activities. Additionally, he/she will provide access to authorized **workforce members** in accordance with regulatory and contractual obligations.

#### 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

Vulnerability Management Policy

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.25 SUBJECT: Vulnerability Management		Page 52 of 59

## Vulnerability Management

### 1. Purpose

The purpose of this policy is to establish guidelines and standards to address the **Organization's** obligations relating to the management of security vulnerabilities.

### 2. Scope

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

### 3. Requirements

Vulnerability Management is a security practice designed to mitigate exploitations of vulnerabilities through a systematic and documented process for managing the timely identification and deployment of patches and other threat remediation practices.

- All **information technology infrastructure** owned, leased, or managed by the **Organization** will be monitored for vulnerabilities.
- All identified vulnerabilities will be documented, analyzed, and a remediation plan will be developed to mitigate all risks to the **information technology infrastructure**.
- All applicable fixes, patches and updates will be tested and applied as necessary.
- The **Organization** will deploy automated patch management solutions whenever possible.
- Where technically feasible, all **application software** used, furnished, and/or supported by the **Organization** will be reviewed to identify and remediate security vulnerabilities during initial implementation and upon modifications and updates.
- End Point Detection software will be installed on all computing devices and configured for real-time monitoring in accordance with the EDR Policy.
- Anti-Virus protection will be installed on all **computing equipment** and configured for real-time protection. Virus definitions shall be routinely updated. No one shall be permitted to stop anti-virus definition updates and scans except the **Information Security Officer** in accordance with the Hardening Policy.
- Vendor sites, bulletins, notifications, and industry publications will be routinely reviewed.
- An inventory of all **information technology infrastructure** assets will be audited, periodically or at least annually in accordance with the **Information Technology Department's** Annual Review.
- Vulnerabilities are considered remediated when the risk of exploitation has been fully removed and subsequent scans of the device show the vulnerability no longer exists.

### 4. Responsibility

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

- The **Information Security Officer** ensures the review, evaluation, and mitigation of the results of the vulnerability scans.



Originated Date:  
Revision Date:  
Approved By:

POLICY#: SOC-Policy.25  
SUBJECT: Vulnerability Management

Page  
53 of 59

- The **Information Security Officer** reserves the right to independently audit each unit at will or at **management** request. These audits will review existing scanning data and verify that vulnerabilities were remediated.
- The **Information Security Officer** ensures all fixes, patches and updates are tested and installed in a timely manner.
- The **Information Security Officer** is responsible for the selection and deployment of Anti-Virus and End Point Detection software.

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

Vulnerability Scanning Policy  
EDR Policy  
Hardening Policy

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.25 SUBJECT: Penetration Testing		Page 54 of 59

## Penetration Testing

### 1. Purpose

The purpose of this policy is to establish guidelines and standards to address the **Organization's** obligations relating to Penetration Testing.

### 2. Scope

The scope of this policy applies to the **information technology infrastructure**. Penetration Testing includes, but is not limited to, scanning for patch levels, scanning for functions, ports, protocols, and services that should not be accessible to **workforce members or computing equipment**.

### 3. Requirements

Penetration Testing is an information gathering process which identifies weaknesses in the **information technology infrastructure** that could compromise the infrastructure. Periodic Penetration Testing, following a specific schedule is part of the **Organization's** continual evaluation process of risk and vulnerability management.

- The **Organization** will use industry standard penetration testing to carry out all testing and audit reporting for the externally facing **information technology infrastructure**. Several tools may be used for penetration testing and the tool set will be reviewed periodically, or at least annually.
- The scope of an external penetration test is the exposed external perimeter of the **information technology infrastructure** accessible to public networks. It shall assess any unique access to the scope from the public networks, including services that have access restricted to individual external IP addresses. Testing must include both application-layer and network-layer assessments. External penetration tests also include remote access vectors such as VPN connections.
- Penetration Testing may cause network performance or availability issues. The **Organization's Information Technology Department** will make reasonable efforts to minimize such issues.
- At the conclusion of each test, all discovered vulnerabilities will be documented. The reports produced by penetration testing may be used as the above documentation. Documentation shall be available upon request.

### 4. Responsibility

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

- The **Information Security Officer** ensures the selection and deployment of industry standard penetration tests to carry out all penetration testing and audit reporting within the **Organization's information technology infrastructure**.

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.25 SUBJECT: Penetration Testing		Page 55 of 59


- The **Information Security Officer** ensures monthly penetration tests are performed and the evaluation and mitigation of the results of the penetration tests are completed in accordance with the Vulnerability Management Policy.
- The **Information Security Officer** will maintain scanning report files to track testing activities. Additionally, he/she will provide access to authorized **workforce members** in accordance with regulatory and client contractual obligations.

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

Vulnerability Management Policy

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.25 SUBJECT: Incident Response		Page 56 of 62

## Incident Response

### 1. Purpose

The purpose of this policy is to establish guidelines and standards regarding incident response to cyber security breaches of the **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 policies and procedures. Despite all efforts, there is the possibility of a breach occurring, and having a set procedure in place is considered best practice.

- Initial Categorization: What has occurred, who/how was it detected, who is managing the response.
- Determine Scope: More technical breakdown expected extent of incident. Assess impact.
- Collect Evidence: Log of collector, evidence, time, and date.
- Analysis: Technical understanding of incident, update scope, determine what the desired end state.
- Containment: What has been done to keep the incident from spreading.
- Resolution: How was the issue resolved.
- Future Recommendations: What changes need to be made to the **information technology infrastructure**.

### 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 be responsible for all communication with **management**.
- The **Information Security Officer** will be responsible for managing documentation of the incident response steps.
- 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

		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.25 SUBJECT: Incident Response		Page 57 of 62

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



		Originated Date: Revision Date: Approved By:
POLICY#: SOC-Policy.25 SUBJECT: Acknowledgment		Page 58 of 62

## IT Security Policy Acknowledgment

I \_\_\_\_\_ acknowledge that I have received a copy of the IT Security Policies, which establishes guidelines and standards for the **Organization**.

I understand that I should consult **Management**, or the **Information Technology Department** should I have questions or need clarification regarding the requirements and my responsibilities outlined in this policy.

I further acknowledge that Violations of this policy, including failure to report Violations of this policy will be subject to the **Organization's** Personnel Policy.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

This page was intentionally left blank.

# NOTICE OF PUBLIC HEARING

A public hearing will be held at Ste. Genevieve City Hall on Thursday, August 22, 2024 at 6:00 p.m. At this hearing, citizens may comment on the property tax rates proposed to be set by the City of Ste. Genevieve a political subdivision. The tax rates shall be set to produce revenues which the budget for the fiscal year 2025 shows to be required from the property tax.

ASSESSED VALUATION (By Categories)	PRIOR YEAR TAXES 2023	CURRENT YEAR TAXES 2024
Real Estate	\$ 63,651,421	\$ 64,357,658
Personal Property	\$ 16,014,158	\$ 15,784,521
<b>TOTAL:</b>	<b>\$ 79,665,579</b>	<b>\$ 80,142,179</b>

FUND	TAX RATE FOR 2023 PER \$100	PROPOSED TAX RATE FOR 2024 PER \$100
General Revenue	0.4812	0.4823
Cemetery	0.0480	0.0481
Band	0.0773	0.0775
Park & Recreation	0.1251	0.1254
Public Safety	0.2684	0.2690
	<b>\$ 1.0000</b>	<b>\$ 1.0023</b>

**CITY OF STE. GENEVIEVE**  
**Pam Meyer, City Clerk**

*Posted :*     **Ste. Genevieve County Library**  
                   **Ste. Genevieve County Court House**  
                   **Ste. Genevieve City Hall**

**August 6, 2024**

SUE WOLK, COUNTY CLERK  
COUNTY OF STE GENEVIEVE  
STATE OF MISSOURI

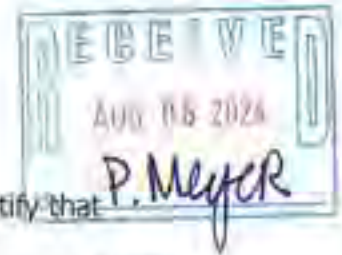
55 South Third Street, Room 2  
Ste. Genevieve, MO 63670  
Phone: 573-883-5389, ext. 2  
Fax: 573-883-7202

Nancy Baker  
Deputy County Clerk

Michelle Garzenmeyer  
Deputy County Clerk

Kim MacMillan  
Deputy County Clerk

NOTICE OF 2024 AGGREGATE ASSESSED VALUATION  
AFTER THE B.O.E. FOR  
CITY OF STE. GENEVIEVE  
COUNTY OF STE. GENEVIEVE, STATE OF MISSOURI



I, Sue Wolk, County Clerk of Ste. Genevieve County, State of Missouri, do hereby certify that the following is the aggregate assessed valuation of City of Ste. Genevieve, a political subdivision in Ste. Genevieve County, for the year 2024 as shown on the assessment lists on August 1, 2024.

	TOTAL BEFORE TIF		TOTAL AFTER
REAL ESTATE	DEDUCTION	LESS TIF	TIF DEDUCTION
Residential	40,407,880	732,370	39,675,510
Agricultural	24,260	-	24,260
Commercial	24,769,954	112,066	24,657,888
PERSONAL PROPERTY	15,784,521	-	15,784,521
<b>TOTAL</b>	<b>80,986,615</b>	<b>844,436</b>	<b>80,142,179</b>

**NEW CONSTRUCTION: \$ 699,840**

This information is transmitted to assist you in complying with Section 67.110 RSMo, which requires that notice be given and public hearings held before tax rates are set.

IN WITNESS WHEREOF, I have hereunto set my hand and affixed the seal of the County Commission of Ste. Genevieve County at my office in Ste. Genevieve, this 2nd of August, 2024.

  
\_\_\_\_\_  
County Clerk

(If applicable, locally assessed railroad and utility property and state assessed railroad and utility property are included).

SPECIAL NOTE: STATE ASSESSED RAIL CARS ARE NOT INCLUDED IN THE ABOVE FIGURES. TAX IS TO BE FIGURED, BILLED, AND COLLECTED BY STATE.

**BILL NO. 4627**

**ORDINANCE NO.**

**AN ORDINANCE AUTHORIZING THE MAYOR TO ENTER INTO A MISSOURI HIGHWAYS AND TRANSPORTATION COMMISSION TRANSPORTATION ENHANCEMENTS FUNDS PROGRAM AGREEMENT FOR PUBLIC IMPROVEMENTS ALONG SOUTH FOURTH STREET (HWY 32) TAP -- 9901(879)**

**WHEREAS**, the City of Ste. Genevieve seeks to improve sidewalk accessibility in the city limits utilizing a TAP Grant from the Missouri Department of Transportation (MoDOT) along South Fourth Street (HWY 32); and

**WHEREAS**, these improvements will improve pedestrian facilities in the city from just north of St. Joseph Street and extending approximately 1294 linear feet to the intersection of Rozier and Hwy 32; and

**WHEREAS**, the improvements will become the responsibility of the City to maintain after construction; and

**WHEREAS**, the Ste. Genevieve Sidewalk and Trail Analysis report from June 2022 highlights this area within the city limits as a connecting trail from downtown to Progress Parkway and the Community Center; and

**WHEREAS**, the Board of Aldermen believe it to be in the best interests of its residents to approve the agreement for the improvements with MoDOT.

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

**SECTION 1.** The Board of Aldermen of the City of Ste. Genevieve, Missouri, hereby approves the execution of an agreement with Missouri Highways and Transportation Commission for improvements along Hwy 32 inside the City Limits that will consist of improving pedestrian facilities.

**SECTION 2.** The improvements located in the City are on the East side of Fourth Street (MO 32) from 125 feet North of St. Joseph Street to Rozier Street. The length of the improvement is 1,294 linear feet.

**SECTION 3.** The Mayor is hereby authorized to execute such agreement (Attached as exhibit "A") and the City Clerk to attest to such execution and to affix the official seal of the City of Ste. Genevieve.

**SECTION 4:** The City Administrator of the City of Ste. Genevieve is hereby authorized to execute all other documents necessary for this project on behalf of the City of Ste. Genevieve.

**SECTION 5.** All ordinances and parts of ordinances which are in conflict with the provisions of this Ordinance are hereby repealed.

**SECTION 6.** This ordinance shall be in full force and effect from and after its passage and approval as provided by law.

**DATE OF FIRST READING:** August 8, 2024.

**DATE OF SECOND READING:** \_\_\_\_\_.

**PASSED AND APPROVED THIS \_\_\_\_\_ DAY OF \_\_\_\_\_, 2024 BY A ROLL CALL VOTE AS FOLLOWS:**

**VOTE**

**ALDERWOMAN AMIE DOBBS  
ALDERMAN ROBERT DONOVAN  
ALDERMAN ERIC BENNETT  
ALDERMAN JEFF EYDMANN  
ALDERMAN MIKE RANEY  
ALDERMAN JOE PRINCE  
ALDERMAN JOE STEIGER  
ALDERMAN PATRICK FAHEY**

**\_\_\_ Yes \_\_\_ No \_\_\_ Absent**

**Signatures on next page**

Approved as to form:

\_\_\_\_\_  
Brian Keim, Mayor

\_\_\_\_\_  
Mark Bishop, City Attorney

SEAL

Reviewed by:

\_\_\_\_\_  
Pam Meyer, City Clerk

\_\_\_\_\_  
Happy Welch, City Administrator

CCO Form: FS25  
Approved: 04/95 (MGB)  
Revised: 03/24 (TLP)  
Modified:

CFDA Number: 20.205  
CFDA Title: Highway Planning and Construction  
Award name/number: TAP – 9901(879)  
Award Year: 2024  
Federal Agency: Federal Highway Administration, Department of Transportation

**MISSOURI HIGHWAYS AND TRANSPORTATION COMMISSION  
TRANSPORTATION ENHANCEMENTS FUNDS  
PROGRAM AGREEMENT**

THIS AGREEMENT is entered into by the Missouri Highways and Transportation Commission (hereinafter, "Commission") and City of Ste. Genevieve (hereinafter, "City").

**WITNESSETH:**

NOW, THEREFORE, in consideration of the mutual covenants, promises and representations in this Agreement, the parties agree as follows:

(1) PURPOSE: The United States Congress has authorized, in Infrastructure Investment and Jobs Act (IIJA); 23 U.S.C. §101, §106 §133; and §208 funds to be used for transportation enhancements activities. The purpose of this Agreement is to grant the use of such transportation enhancement funds to the City.

(2) LOCATION: The transportation enhancements funds which are the subject of this Agreement are for the project at the following location: The East side of 4<sup>th</sup> street (MO 32) from 125 ft. North of St. Joesph Street to Rozler Street

The general location of the project is shown on attachment marked "Exhibit A" and incorporated herein by reference.

(3) REASONABLE PROGRESS POLICY: The project as described in this agreement is subject to the reasonable progress policy set forth in the Local Public Agency (LPA) Manual and the final deadline specified in Exhibit B attached hereto and incorporated herein by reference. In the event, the LPA Manual and the final deadline within Exhibit B conflict, the final deadline within Exhibit B controls. If the project is within a Transportation Management Area that has a reasonable progress policy in place, the project is subject to that policy. If the project is withdrawn for not meeting reasonable progress, the City agrees to repay the Commission for any progress payments made to the City for the project and agrees that the Commission may deduct progress payments



made to the City from future payments to the City. The City may not be eligible for future Transportation Enhancements Funds if the City does not meet the reasonable progress policy.

(4) INDEMNIFICATION: To the extent allowed or imposed by law, the City shall defend, indemnify and hold harmless the Commission, including its members and department employees, from any claim or liability whether based on a claim for damages to real or personal property or to a person for any matter relating to or arising out of the City's wrongful or negligent performance of its obligations under this Agreement.

(5) INSURANCE:

(A) The City is required or will require any contractor procured by the City to work under this Agreement:

(1) To obtain a no cost permit from the Commission's district engineer prior to working on the Commission's right-of-way, which shall be signed by an authorized contractor representative (a permit from the Commission's district engineer will not be required for work outside of the Commission's right-of-way); and

(2) To carry commercial general liability insurance and commercial automobile liability insurance from a company authorized to issue insurance in Missouri, and to name the Commission, and the Missouri Department of Transportation and its employees, as additional insureds in amounts sufficient to cover the sovereign immunity limits for Missouri public entities (\$600,000 per claimant and \$4,000,000 per occurrence) as calculated by the Missouri Department of Insurance, Financial Institutions and Professional Registration, and published annually in the Missouri Register pursuant to Section 537.610, RSMo.

(B) In no event shall the language of this Agreement constitute or be construed as a waiver or limitation for either party's rights or defenses with regard to each party's applicable sovereign, governmental, or official immunities and protections as provided by federal and state constitution or law.

(6) AMENDMENTS: Any change in this Agreement, whether by modification or supplementation, must be accomplished by a formal contract amendment signed and approved by the duly authorized representatives of the City and the Commission.

(7) COMMISSION REPRESENTATIVE: The Commission's District Engineer is designated as the Commission's representative for the purpose of administering the provisions of this Agreement. The Commission's representative may designate by written notice other persons having the authority to act on behalf of the Commission in furtherance of the performance of this Agreement.

(8) NONDISCRIMINATION ASSURANCE: With regard to work under this Agreement, the City agrees as follows:

(A) Civil Rights Statutes: The City shall comply with all state and federal statutes relating to nondiscrimination, including but not limited to Title VI and Title VII of the Civil Rights Act of 1964, as amended (42 U.S.C. §2000d and §2000e, *et seq.*), as well as any applicable titles of the "Americans with Disabilities Act" (42 U.S.C. §12101, *et seq.*). In addition, if the City is providing services or operating programs on behalf of the Department or the Commission, it shall comply with all applicable provisions of Title II of the "Americans with Disabilities Act".

(B) Administrative Rules: The City shall comply with the administrative rules of the United States Department of Transportation relative to nondiscrimination in federally assisted programs of the United States Department of Transportation (49 C.F.R. Part 21) which are herein incorporated by reference and made part of this Agreement.

(C) Nondiscrimination: The City shall not discriminate on grounds of the race, color, religion, creed, sex, disability, national origin, age or ancestry of any individual in the selection and retention of subcontractors, including procurement of materials and leases of equipment. The City shall not participate either directly or indirectly in the discrimination prohibited by 49 C.F.R. §21.5, including employment practices.

(D) Solicitations for Subcontracts, Including Procurements of Material and Equipment: These assurances concerning nondiscrimination also apply to subcontractors and suppliers of the City. These apply to all solicitations either by competitive bidding or negotiation made by the City for work to be performed under a subcontract including procurement of materials or equipment. Each potential subcontractor or supplier shall be notified by the City of the requirements of this Agreement relative to nondiscrimination on grounds of the race, color, religion, creed, sex, disability or national origin, age or ancestry of any individual.

(E) Information and Reports: The City shall provide all information and reports required by this Agreement, or orders and instructions issued pursuant thereto, and will permit access to its books, records, accounts, other sources of information, and its facilities as may be determined by the Commission or the United States Department of Transportation to be necessary to ascertain compliance with other contracts, orders and instructions. Where any information required of the City is in the exclusive possession of another who fails or refuses to furnish this information, the City shall so certify to the Commission or the United States Department of Transportation as appropriate and shall set forth what efforts it has made to obtain the information.

(F) Sanctions for Noncompliance: In the event the City fails to comply with the nondiscrimination provisions of this Agreement, the Commission shall impose such contract sanctions as it or the United States Department of Transportation may determine to be appropriate, including but not limited to:

1. Withholding of payments under this Agreement until the City complies; and/or

2. Cancellation, termination or suspension of this Agreement, in whole or in part, or both.

(G) Incorporation of Provisions: The City shall include the provisions of paragraph (B) of this Agreement in every subcontract, including procurements of materials and leases of equipment, unless exempted by the statutes, executive order, administrative rules or instructions issued by the Commission or the United States Department of Transportation. The City will take such action with respect to any subcontract or procurement as the Commission or the United States Department of Transportation may direct as a means of enforcing such provisions, including sanctions for noncompliance; provided that in the event the City becomes involved or is threatened with litigation with a subcontractor or supplier as a result of such direction, the City may request the United States to enter into such litigation to protect the interests of the United States.

(9) ASSIGNMENT: The City shall not assign, transfer or delegate any interest in this Agreement without the prior written consent of the Commission.

(10) LAW OF MISSOURI TO GOVERN: This Agreement shall be construed according to the laws of the State of Missouri. The City shall comply with all local, state and federal laws and regulations relating to the performance of this Agreement.

(11) CANCELLATION: The Commission may cancel this Agreement at any time for a material breach of contractual obligations by providing the City with written notice of cancellation. Should the Commission exercise its right to cancel this Agreement for such reasons, cancellation will become effective upon the date specified in the notice of cancellation sent to the City.

(12) ACCESS TO RECORDS: The City and its contractors must maintain all records relating to this Agreement, including but not limited to invoices, payrolls, etc. These records must be available at no charge to the Federal Highway Administration (FHWA) and the Commission and/or their designees or representatives during the period of this Agreement and any extension, and for a period of three (3) years after the date on which the City receives reimbursement of their final invoice from the Commission.

(13) FEDERAL-AID PROVISIONS: Because responsibility for the performance of all functions or work contemplated as part of this project is assumed by the City, and the City may elect to construct part of the improvement contemplated by this Agreement with its own forces, a copy of Section II and Section III, as contained in the United States Department of Transportation Form Federal Highway Administration (FHWA) 1273 "Required Contract Provisions, Federal-Aid Construction Contracts," is attached and made a part of this Agreement as Exhibit C. Wherever the term "the contractor" or words of similar import appear in these sections, the term "the City" is to be substituted. The City agrees to abide by and carry out the condition and obligations of "the contractor" as stated in Section II, Equal Opportunity, and Section III, Nonsegregated Facilities, as set

out in Form FHWA 1273.

(14) ACQUISITION OF RIGHT OF WAY: With respect to the acquisition of right of way necessary for the completion of the project, City shall acquire any additional necessary right of way required for this project and in doing so agrees that it will comply with all applicable federal laws, rules and regulations, including 42 U.S.C. 4601-4655, the Uniform Relocation Assistance and Real Property Acquisition Act, as amended and any regulations promulgated in connection with the Act.

(15) MAINTENANCE OF DEVELOPMENT: The City shall maintain the herein contemplated improvements without any cost or expense to the Commission. All maintenance by the City shall be done for the safety of the general public and the esthetics of the area. In addition, if any sidewalk or bike trails are constructed on the Commission's right-of-way pursuant to this Agreement, the City shall inspect and maintain the sidewalk or bike trails constructed by this project in a condition reasonably safe to the public and, to the extent allowed by law, shall indemnify and hold the Commission harmless from any claims arising from the construction and maintenance of said sidewalk or bike trails. If the City fails to maintain the herein contemplated improvements, the Commission or its representatives, at the Commission's sole discretion shall notify the City in writing of the City's failure to maintain the improvement. If the City continues to fail in maintaining the improvement, the Commission may remove the herein contemplated Improvement whether or not the improvement is located on the Commission's right of way. Any removal by the Commission shall be at the sole cost and expense of the City. Maintenance includes but is not limited to mowing and trimming between shrubs and other plantings that are part of the improvement.

(16) PLANS: The City shall prepare preliminary and final plans and specifications for the herein improvements. The plans and specifications shall be submitted to the Commission for the Commission's review and approval. The Commission has the discretion to require changes to any plans and specification prior to any approval by the Commission.

(17) REIMBURSEMENT: The cost of the contemplated improvements will be borne by the United States Government and by the City as follows:

(A) Any federal funds for project activities shall only be available for reimbursement of eligible costs which have been incurred by City. Any costs incurred by City prior to authorization from FHWA and notification to proceed from the Commission are not reimbursable costs. The federal share for this project will be 80 percent not to exceed \$391,251.74. The calculated federal share for seeking federal reimbursement of participating costs for the herein improvements will be determined by dividing the total federal funds applied to the project by the total participating costs. Any costs for the herein improvements which exceed any federal reimbursement or are not eligible for federal reimbursement shall be the sole responsibility of City. The Commission shall not be responsible for any costs associated with the herein improvement unless specifically identified in this Agreement or subsequent written amendments.

(18) PROGRESS PAYMENTS: The City may request progress payments be made for the herein improvements as work progresses but not more than once every two weeks. Progress payments must be submitted monthly. The City shall repay any progress payments which involve ineligible costs.

(19) PROMPT PAYMENTS: Progress invoices submitted to MoDOT for reimbursement more than thirty (30) calendar days after the date of the vendor invoice shall also include documentation that the vendor was paid in full for the work identified in the progress invoice. Examples of proof of payment may include a letter or e-mail from the vendor, lien waiver or copies of cancelled checks. Reimbursement will not be made on these submittals until proof of payment is provided. Progress invoices submitted to MoDOT for reimbursement within thirty (30) calendar days of the date on the vendor invoice will be processed for reimbursement without proof of payment to the vendor. If the City has not paid the vendor prior to receiving reimbursement, the City must pay the vendor within two (2) business days of receipt of funds from MoDOT.

(20) PERMITS: The City shall secure any necessary approvals or permits from any federal or state agency as required for the completion of the herein improvements. If this improvement is on the right of way of the Commission, the City must secure a permit from the Commission prior to the start of any work on the right of way. The permits which may be required include, but are not limited to, environmental, architectural, historical or cultural requirements of federal or state law or regulation.

(21) INSPECTION OF IMPROVEMENTS AND RECORDS: The City shall assure that representatives of the Commission and FHWA shall have the privilege of inspecting and reviewing the work being done by the City's contractor and subcontractor on the herein project. The City shall also assure that its contractor, and all subcontractors, if any, maintain all books, documents, papers and other evidence pertaining to costs incurred in connection with the Transportation Enhancement Program Agreement, and make such materials available at such contractor's office at all reasonable times at no charge during this Agreement period, and for three (3) years from the date of final payment under this Agreement, for inspection by the Commission, FHWA or any authorized representatives of the Federal Government and the State of Missouri, and copies shall be furnished, upon request, to authorized representatives of the Commission, State, FHWA, or other Federal agencies.

(22) CREDIT FOR DONATIONS OF FUNDS, MATERIALS, OR SERVICES: A person may offer to donate funds, materials or services in connection with this project. Any donated funds, or the fair market value of any donated materials or services that are accepted and incorporated into this project shall be credited according to 23 U.S.C. §323.

(23) DISADVANTAGED BUSINESS ENTERPRISES (DBE): The Commission will advise the City of any required goals for participation by disadvantaged business enterprises (DBEs) to be included in the City's proposal for the work to be performed. The City shall submit for Commission approval a DBE goal or plan. The City shall comply

with the plan or goal that is approved by the Commission and all requirements of 49 C.F.R. Part 26, as amended.

(24) VENUE: It is agreed by the parties that any action at law, suit in equity, or other judicial proceeding to enforce or construe this Agreement, or regarding its alleged breach, shall be instituted only in the Circuit Court of Cole County, Missouri.

(25) NOTICE TO BIDDERS: The City shall notify the prospective bidders that disadvantaged business enterprises shall be afforded full and affirmative opportunity to submit bids in response to the invitation and will not be discriminated against on grounds of race, color, sex, or national origin in consideration for an award.

(26) FINAL AUDIT: The Commission may, in its sole discretion, perform a final audit of project costs. The United States Government shall reimburse the City, through the Commission, any monies due. The City shall refund any overpayments as determined by the final audit.

(27) AUDIT REQUIREMENTS: If the City expend(s) seven hundred fifty thousand dollars (\$750,000) or more in a year in federal financial assistance it is required to have an independent annual audit conducted in accordance with 2 CFR Part 200. A copy of the audit report shall be submitted to MoDOT within the earlier of thirty (30) days after receipt of the auditor's report(s), or nine (9) months after the end of the audit period. Subject to the requirements of 2 CFR Part 200, if the City expend(s) less than seven hundred fifty thousand dollars (\$750,000) a year, the City may be exempt from auditing requirements for that year but records must be available for review or audit by applicable state and federal authorities.

(28) FEDERAL FUNDING ACCOUNTABILITY AND TRANSPARENCY ACT OF 2006: The City shall comply with all reporting requirements of the Federal Funding Accountability and Transparency Act (FFATA) of 2006, as amended. This Agreement is subject to the award terms within 2 C.F.R. Part 170.

*[Remainder of Page Intentionally Left Blank]*

IN WITNESS WHEREOF, the parties have entered into this Agreement on the date last written below.

Executed by the City this \_\_\_\_\_ (date).

Executed by the Commission this \_\_\_\_\_ (date).

**MISSOURI HIGHWAYS AND  
TRANSPORTATION COMMISSION**

**CITY OF STE. GENEVIEVE**

By: \_\_\_\_\_

By: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

**ATTEST:**

**ATTEST:**

\_\_\_\_\_  
Secretary to the Commission

By: \_\_\_\_\_

Title: \_\_\_\_\_

Approved as to Form:

Approved as to Form:

\_\_\_\_\_  
Commission Counsel

By: \_\_\_\_\_

Title: \_\_\_\_\_

Ordinance No. \_\_\_\_\_