

REQUEST FOR COUNCIL ACTION

Meeting

Date: July 28.26

AGENDA SECTION: General Business	ORIGINATING DEPT: Administration
ITEM DESCRIPTION: Cybersecurity Policy & Disaster Recovery Plan	PREPARED BY: C.Roeder
As the City continues to rely on technology to provide essential services, protect sensitive information, and maintain public records, it is important to establish formal policies and procedures that reduce cybersecurity risks and ensure continuity of operations. The proposed Cybersecurity Policy establishes standards for the appropriate use and protection of the City's information technology systems. The proposed Computer & Records Disaster Recovery Plan provides a framework for restoring critical technology systems and records following a cyberattack, natural disaster, hardware failure, or other disruptive event. These documents establish best practices for safeguarding City information assets, minimizing service interruptions, and ensuring the City can continue essential operations during and after an emergency. <u>COUNCIL ACTION REQUESTED:</u> 1. Approve the Cybersecurity Policy as presented 2. Adopted Resolution 2026 – A Resolution 2026- A Resolution Adopting a Computer and Records Disaster Recovery Plan	



Cybersecurity Policy

Adopted by Stewartville City Council – July 28.2026

1. Purpose

The purpose of this policy is to protect the City of Stewartville's computer systems, networks, and data from unauthorized access, cyber threats, and security breaches.

2. Scope

This policy applies to all City employees, contractors, and elected officials who access City computer systems, email, or digital records.

3. Password Security

All City users must follow password security practices:

- Passwords must be at least 12 characters long.
 - Passwords should be protected.
 - Passwords should not be reused across multiple systems.
 - Passwords must be changed if a security compromise is suspected.
-

4. Email Security

City employees must use caution when handling email.

Employees should:

- Avoid opening suspicious attachments
- Avoid clicking unknown links
- Report suspicious emails to IT support

Phishing attempts should be immediately reported.

5. Software Updates

All City computers must maintain current software updates.

Updates include:

- Operating system updates
- Antivirus updates
- Security patches

Whenever possible, updates should be automated.

6. Antivirus and Malware Protection

All City computers must have active antivirus protection installed and maintained.

The City's IT provider will monitor and maintain security software.

7. Remote Access

Remote access to City systems must be secured through:

- VPN access or secure login systems
 - Strong authentication procedures
 - Authorization by the City Administrator or IT provider
-

8. Cybersecurity Incident Response

If a cybersecurity incident occurs:

1. Disconnect the affected device from the network.
 2. Notify the City Administrator and IT provider immediately.
 3. Do not attempt to fix the issue without IT guidance.
 4. Restore systems from secure backups if necessary.
-

9. User Responsibilities

City employees must:

- Protect confidential data
- Use City computers for official business
- Follow all IT security procedures
- Report suspicious activity immediately

Failure to comply with this policy may result in disciplinary action.

10. Policy Review

This policy should be reviewed periodically and updated as technology and security threats evolve.



Computer & Records Disaster Recovery Plan

Adopted by Stewartville City Council: July 28, 2026

Responsible Department: City Clerk

1. Purpose

The purpose of this Disaster Recovery Plan is to establish procedures to protect and restore the City of Stewartville's computer systems, electronic data, and essential documents following a disaster or major disruption.

This plan is intended to minimize downtime, protect critical information, and ensure the continuation of City services.

2. Scope

This plan applies to all City computer systems, servers, electronic data, software applications, and important paper records maintained by the City.

Departments covered include:

- Administration
 - Finance
 - Public Works
 - Utilities
 - Planning and Zoning
 - Any additional City technology systems
-

3. Potential Disaster Events

Disasters that could disrupt City operations include:

Natural Disasters

- Tornadoes/Severe Storms
- Flooding
- Fire

Technology Failures

- Server or hardware failure
- Network outages
- Power outages

Security Incidents

- Cyberattacks
- Ransomware
- Malware infections
- Unauthorized system access

Other Events

- Building damage
- Theft or vandalism
- Accidental deletion of data

4. Disaster Recovery Responsibilities

City Administrator

- Overall coordination of disaster recovery
- Determines operational priorities

Department Heads

- Identify critical systems and data
- Assist with restoring departmental operations

Finance Department

- Ensure restoration of financial and utility billing systems

IT Vendor / Technology Support

- Restore servers, networks, and software
- Assist with cybersecurity incidents

City Clerk

- Assist with recovery of official records and documents
-

5. Data Backup Procedures

The City will maintain regular backups of critical computer systems and files.

Backup procedures include:

- Daily backups of financial systems and shared files
- Weekly backups of workstations where applicable
- Secure off-site or cloud-based backup storage
- Periodic testing of backup restoration

Backups should follow the standard **3-2-1 backup rule**:

- 3 copies of important data
 - 2 different storage types
 - 1 copy stored off-site
-

6. System Recovery Priorities

Priority Level 1 – Critical Systems (restore within 24–48 hours)

- Financial software
- Utility billing system
- Email systems
- Network servers

Priority Level 2 – Important Systems (restore within 3–5 days)

- GIS or mapping systems
- Document management systems

Priority Level 3 – Routine Systems (restore within 7–10 days)

- Archived files
 - Historical documents
 - Non-essential software
-

7. Disaster Recovery Procedures

If a disaster occurs:

1. Notify the City Administrator and IT support provider.
2. Assess the extent of the system disruption.

3. Disconnect affected systems if a cybersecurity incident is suspected.
 4. Restore systems from the most recent secure backup.
 5. Verify system functionality and data integrity.
 6. Resume normal City operations.
-

8. Protection of Paper Records

Important City records should be protected through:

- Fire-resistant filing cabinets
- Secure document storage
- Digitization when possible
- Off-site storage of critical records

Examples of critical records include:

- Ordinances and resolutions
 - Financial records
 - Contracts and agreements
 - Property and utility records
 - Personnel files
-

9. Plan Testing and Review

This Disaster Recovery Plan should be reviewed periodically and updated as needed.

The City should periodically test backup restoration to ensure data can be successfully recovered.

10. Plan Maintenance

The City Administrator or designee is responsible for maintaining this plan and updating it when:

- New technology systems are implemented
 - Vendors change
 - A disaster or major incident occurs
-

CITY OF STEWARTVILLE
RESOLUTION 2026-_____

A RESOLUTION ADOPTING A COMPUTER AND RECORDS DISASTER RECOVERY PLAN

WHEREAS, the City of Stewartville relies on computer systems and electronic records to conduct essential municipal operations; and

WHEREAS, disruptions caused by natural disasters, cyber incidents, equipment failure, or other emergencies could impact the City's ability to provide services; and

WHEREAS, it is in the best interest of the City to establish procedures to restore computer systems and protect important municipal records in the event of a disaster;

NOW THEREFORE BE IT RESOLVED by the City Council of the City of Stewartville, Minnesota:

1. The City Council hereby adopts the City of Stewartville Computer and Records Disaster Recovery Plan.
2. City staff are authorized to implement and maintain the plan to ensure the protection and restoration of City technology systems and records.
3. The City Administrator or designee shall periodically review and update the plan as necessary.

Adopted by the City Council this 28th day of July, 2026.

Jimmie-John King, Mayor

ATTEST:

Cheryl Roeder, City Clerk