Network and Cyber Security Policy

I. Policy Background

The City of Crossville is committed to safeguarding the confidentiality of all access and application assets of the City, and to comply with current laws, regulations, guidelines and best practices to protect all city assets and departments from the dangers of cybercrimes.

II. Purpose

This policy was written to provide a security framework to all employees, stakeholders and contractors of the City of Crossville to protect from unauthorized access, loss or damage while utilizing technology or information systems.

Failure to act in accordance with this policy may result in disciplinary action, up to termination.

III. Scope

This policy applies to all employees, third-party vendors and contractors who have, or need access to the City's information systems and data.

IV. Security Training and Awareness

The City of Crossville will periodically provide training for employees to help them understand their roles and responsibilities that involve computers, networks and the use of the Internet.

V. Personnel Responsibilities

All employees, stakeholders and contractors or third-party vendors must be cyber security aware, and are required to follow the procedures listed hereinafter.

1. All devices provided by the City of Crossville are strictly for city business. Devices are provided for the sole purpose of the performance of assigned roles and duties.
2. Properly sign out of systems and devices, or lock when not in use and after shift hours.
3. Immediately and directly notify the IT Department of any suspicious activity.
4. Keep areas that do not require public access secure.
5. Third-party vendors or contractors must be approved by the IT Department.
6. Employees should not share passwords or access credentials unless approved by the department head and the IT Department.
7. End users, third-party vendors nor contractors shall install software, change settings or circumvent security measures without prior authorization from the IT Department.
8. Any person or entity that requires direct access to a city owned device or a city secured network must read, sign and agree to the *Computer, Electronic Equipment, Internet and Email Usage* acknowledgement listed in the City of Crossville Personnel.

VI. Policy Implementation and Review

The City of Crossville IT Department shall be in charge of implementation and execution of cyber security processes and policies. The department is to be included in matters relating to networks, hardware and software security, as well as hardware and software purchases or leases. This policy may be reviewed and revised as technology and best practice guidelines evolve.

VII. Incident Response

1. Employees, third-party vendors and contractors must contact the IT Department by phone to report suspected compromises, breaches or threats. Lee Lawson – 931-787-3166; Kyle Sherrill – 931-200-4480. Do not use email or internal messaging. This could alert hackers and result in lost evidence.
2. The IT Department will make an assessment to determine the type of incident and report to the City Manager. The report to the City Manager should be made as soon as possible, however, priority is given to securing the network and data.
3. The City Manager or Risk Manager will notify the proper insuring agency for the City for potential claims and public notification. No external forensic teams shall be hired without insurance carrier approval.
4. During the assessment, the IT Department will remove access to computers, networks, and Internet, and if necessary, throughout any investigation. Access will not be reinstated until such time that the threat is mitigated and\or further safeguards or training is in place.
5. Depending on the type of threat, IT may reset user passwords, limit future access or monitor a user's activity, including but not limited to, email, instant messaging, and browsing history. The IT Department may work with forensic experts to identify attack vectors.
6. The City Manager will notify appropriate department heads, administrative personnel, council members and\or law enforcement.
7. If Police Department systems are directly affected, such as iSoms, RMS Systems or court records, access will be terminated and the Chief of Police must notify the Tennessee Bureau of Investigation.
8. If SCADA systems are directly affected, water production and distribution facilities must implement manual override protocols. Local, state and federal law enforcement should be notified.
9. Updates and findings shall be reported to the City Manager as they become available. The City Manager or City Attorney will oversee the dissemination any reports or findings from any investigation.
10. Any discoveries, results or conclusions shall not be discussed outside of the IT Department or the investigating agency, unless approved by the City Manager or City Attorney.
11. Clean up procedures will vary by type of threat or breach, however, in the event of a ransomware attack, the IT Department will verify that backups are not affected. Attack vectors will be hardened before AD, DNS servers are rebuilt. Workstations will remain offline until reimaged with a new installation of the OS and applications.
12. IT shall conduct a post incident assessment to determine if further policies or procedures are necessary.

VIII. Risk Assessment

1. The IT Department shall verify compliance of policies and procedures through various methods, including but not limited to, reports, internal and external audits.
2. The IT Department may inspect email, messages or devices and computers as necessary to ensure compliance and secure operations.
3. This policy shall be reviewed annually and updated as necessary.