RESOLUTION NO. _______

A RESOLUTION APPROVING A CYBER SECURITY PLAN FOR
THE CITY OF KINGSPORT

WHEREAS, Public Chapter No. 1111 amended various sections in Chapter 51 of Title 7 as well as sections in Chapter 4 of Title 65 of the Tennessee Code Annotated requiring utilities to adopt and implement a cyber security plan; and

WHEREAS, the plan is to provide for the protection of the utility's facilities from unauthorized use, alteration, ransom, or destruction of electronic data; and

WHEREAS, in or around April, 2023 utilities division working in conjunction with the information technology department promulgated and implemented a cyber security plan in accordance with Public Chapter No. 1111; and

WHEREAS, it is now deemed advisable for the board to formally adopt the cyber security plan in light of its application to multiple city departments.

Now therefore,

BE IT RESOLVED BY THE BOARD OF MAYOR AND ALDERMEN AS FOLLOWS:

SECTION I. That the board hereby formally adopts the cyber security plan as more fully set forth herein:

City of Kingsport, Tennessee

Issue Date		Submitted by:
April 3, 2023	**Cyber Security Plan**	**Floyd Bailey, CIO**

Supersedes
All Previous

Purpose
The City of Kingsport, Tennessee Cyber Security Plan outlines the guidelines and provisions for preserving the security of the cities data and technological infrastructure for all departments. Specifically, to include:

1) Water Services Department
2) Wastewater Services Department
3) Stormwater Department
4) Sanitation Department
5) Streets Department
6) Leisure Services
7) Finance Department
8) Information Technology Department
9) Fire Department
10) Police Department
11) Legal/Risk Department
12) Kingsport Area Transit Department
13) Purchasing Department
14) Building and Planning Department

Scope
The Plan applies to all employees, contractors and anyone who has permanent or temporary access to the City of Kingsport Assets, systems and software or hardware whether cloud based or on premise.

Plan Elements

I. Kingsport Cybersecurity Framework

The Cities IT network will be designed using the National Institute of Standards and Technology's (NIST) five recommended functional areas as specified below:

A. **Identify:** Installation of hardware/software to identify abnormalities in the flow of information into, exiting and/or within the municipal network

B. **Protect:** Installation of hardware/software and/or business practices to deter the infiltration and proliferation of malicious activity within the municipalities network

C. **Detect:** Installation of hardware/software to identify malicious and/or abnormal network activity.

D. **Respond:** Implement procedures and infrastructure to isolate network penetration when necessary and eliminate additional associated risks

E. **Recover:** Installation of hardware/software and procedures to maintain "clean" versions of the cities digital infrastructure to facilitate quick recovery when needed.

II. Protection of personal and municipal devices and network access

Any digital device or access point used as an entrance to the municipalities technological infrastructure is to be vetted by IT and secured in a manner approved by the IT department. The following is a list of acceptable methods of providing this security:

A. Multifactor authentication

B. Frequent password change

C. Municipal data access through secure/private networks approved and provided by the IT department only

III. Additional measures

A. To further reduce the likelihood of security breaches, employees should:

1. Report stolen, lost or damaged equipment to the IT department as soon as possible.

2. Use complex passwords and change account passwords as required.

3. Report a perceived security threat to the IT department or city management.

4. Refrain from downloading suspicious, unauthorized or illegal software on municipal equipment.

5. Avoid accessing suspicious websites.

6. The City of Kingsport's Information Technology Cyber Security personnel and/or Network Manager will, among other related activities:

B. Implement network security and access authentication systems.

1. Ensure the current state of security mitigation updates for software applications and equipment by

i. updating

ii. patch application

iii. firmware

iv. any other solution recommendations

2. Arrange for security training for all employees on an ongoing basis

3. Inform employees regularly about new scam emails or viruses and ways to combat them.

4. Investigate security breaches thoroughly.

IV. The Notification, administration and oversight of this Plan is the responsibility of the IT department.

V. Department Managers are responsible implementing this Plan within their respective departments.

VI. Disciplinary action related to violations of this Plan shall be consistent with the standard procedures outlined in the Employee Handbook.

SECTION II. That the board finds that the actions authorized by this resolution are for a public purpose and will promote the health, comfort and prosperity of the citizens of the city.

SECTION III. That this resolution shall take effect from and after its adoption, the public welfare requiring it.

ADOPTED this the 19th day of December, 2023.

____
PATRICK W. SHULL, MAYOR

ATTEST:

____
ANGELA MARSHALL, DEPUTY CITY RECORDER

APPROVED AS TO FORM:

____
RODNEY B. ROWLETT, III, CITY ATTORNEY