



# City of Elkins

## Rules and Ordinances Committee Meeting

---

October 14, 2024

3:30 PM

Phil Gainer Community Center  
142 Robert E Lee Ave. Ext.

**Charter Authority of the Rules & Ordinances Committee:** Consider and propose to Council new and amended ordinances, rules, and policies.

### AGENDA

1. **Call to order and roll call**
2. **Public comment**
3. **Minutes**
  - a. Proposed minutes for the meeting of July 1, 2024
4. **New business**
  - a. Admin Officers ordinance
  - b. Cybersecurity policy
  - c. Consideration of changes to the floodplain ordinance
5. **Announcements**
6. **Adjournment**



## CITY OF ELKINS AGENDA ITEM REPORT

<b>Meeting Date:</b>	October 14, 2024
<b>Section:</b>	Minutes
<b>Category:</b>	Action Item
<b>Agenda Item Name:</b>	Proposed minutes for the meeting of July 1, 2024
<b>Recommended By:</b>	City Clerk
<b>Summary:</b>	Minutes proposed for the meeting of July 1
<b>Fiscal Impact:</b>	n/a
<b>Recommendation:</b>	Consider for approval
<b>Attachments:</b>	1. Rules and Ordinances Committee - 2024_07_01 - minutes_proposed

**RULES AND ORDINANCES COMMITTEE  
REGULAR MEETING  
MINUTES**

*401 Davis Avenue  
City Hall, Council Chambers  
July 1, 2024  
3:30 p.m.*

Present were members: C. Lowther (chair), A. Carroll, and L. Severino.

Also present were: Steve Himes (fire chief), Travis Bennett (police chief), and Sutton Stokes (city clerk).

**PUBLIC COMMENT**

There was no public comment.

**MINUTES**

Carroll **MOVED APPROVAL OF THE MINUTES OF THE MEETING OF JUNE 3, 2024.** The motion carried.

**NEW BUSINESS**

Severino **MOVED RECOMMENDING COUNCIL APPROVAL OF AMENDING THE CHARTER TO CORRECT INCONSISTENT DATES GIVEN FOR MUNICIPAL ELECTIONS.** The motion carried.

The meeting adjourned at 4:05 p.m.

\_\_\_\_\_  
Name & Title

\_\_\_\_\_  
Signature



## CITY OF ELKINS AGENDA ITEM REPORT

<b>Meeting Date:</b>	October 14, 2024
<b>Section:</b>	New business
<b>Category:</b>	Action Item
<b>Agenda Item Name:</b>	Admin Officers ordinance
<b>Recommended By:</b>	Administrative Officers, City Attorney
<b>Summary:</b>	As directed by Resolution 1791, the city's Administrative Officers and City Attorney have prepared draft language to amend Code confirming the longstanding practice of delegation of various authorities to the Administrative Officers. See attached memo for a detailed explanation.
<b>Fiscal Impact:</b>	n/a
<b>Recommendation:</b>	Consider for recommendation to Council
<b>Attachments:</b>	<ol style="list-style-type: none"> <li>1. code change re admin officers - 2024_10_11</li> <li>2. authority of admin officers - 2024_10_10 - after city attorney review</li> </ol>

# Memo

To: Rules & Ordinances Committee

From: Sutton Stokes, City Clerk

Date: October 11, 2024

Re: Proposed Code change concerning Administrative Officers

---

City staff have identified some sections of the Elkins City Charter and Elkins City Code that could be clarified to enable the city government to finetune and strengthen its administration and operations. The most extensive clarifications concern the roles and authority of the city’s Administrative Officers, as described in this memo.

## Background

The need for these clarifications is primarily the result of certain actions not taken after the 2021 election. In that election, voters were asked to decide for or against a proposal to change the form, or “plan,” of the Elkins city government.

West Virginia Code (8-3-2) allows municipalities to choose from one of five “plans” for the shape of a city government. Since at least 1901, Elkins has been chartered under the Mayor-Council Plan (“Plan I”). In 2021, voters were asked to weigh in on amending the charter to adopt a new plan, the Manager-Mayor Plan (“Plan V” in 8-3-2). Voters rejected this amendment, preferring instead to remain with the Mayor-Council Plan.

Under the Mayor-Council Plan (the city’s longstanding and current plan, as endorsed by voters in the 2021 election), the mayor and council—acting *together*—are both the *governing* (i.e., lawmaking) and *administrative* (i.e., managerial and operating) authorities of the city.

If voters had endorsed the new Manager form of government, the Charter would *instead* have identified *Council* as the *governing* authority and the *Manager* as the *administrative* authority.

There would also have been a Manager section of the Charter, enumerating the administrative authorities assigned by council to the Manager, such as the hiring, termination, and supervision of staff; the supervision of the city’s departments and agencies; and so forth.

## **Who Holds Administrative Authority Now?**

After voters rejected the Manager form of government, the Charter section describing the Manager’s authorities was simply deleted. No later action was taken to reassign administrative authority to anyone else.

This oversight essentially left administrative authority with council and the mayor—but again, under the rules of the Mayor-Council Plan, acting only *as a body*, on a majority vote held at public meetings. Clearly, it is not possible for a group of 11 elected officials to be directly responsible for the numerous daily administrative decisions required for the effective functioning of a modern city. Instead, administrative authority must be delegated.

## **Role of Council’s Five Administrative Officers**

In practice, Council has long relied on its five appointed Administrative Officers (the City Clerk, the City Treasurer, the Fire Chief, the Operations Manager, and the Police Chief) to exercise administrative authority over their respective departments and the various personnel assigned thereto by council action.

However, neither this category of employee nor any of the related practices are explicitly described anywhere in the Charter or Code. Because of a range of problems that can arise when these authorities are not clearly delineated, it is important that Council take action to ensure that the above practice is clearly reflected in city law.

The best way to formalize the above practice would be by adding the attached “Powers and Duties of Administrative Officers” to Code.

This new language would fill in the above blanks by explicitly stipulating who the City’s Administrative Officers are; clarifying that administrative authority is delegated to them; and confirming that they are empowered to exercise this authority over their respective departments. The section’s preamble also assigns “mutual responsibility” for managing the affairs of the City on Council’s behalf, underlining the crucial element of teamwork and collaboration that will always be vital to the success of a government structured in this way.

In addition to granting these powers, this section also imposes obligations and duties on these Officers, such as ensuring Council’s laws and rules are faithfully executed, collaborating to prepare and submit a budget, advising Council on the condition and needs of the City, goal setting, and so forth. Further, the section clarifies the nature of the City’s chain of command, to further strengthen communication and efficiency.

This language is proposed to be adopted as an ordinance amending Code, not the Charter, as the best means of clarifying the questions described earlier in this memo while still respecting the form of government selected by the voters in 2021.

##

## **POWERS AND DUTIES OF ADMINISTRATIVE OFFICERS**

There shall be five Administrative Officers of the City (the City Clerk, the City Treasurer, the Fire Chief, the Operations Manager, and the Police Chief), nominated and appointed as described in Charter Section 3.01, sworn to uphold the Constitution of the United States and the Constitution of this State, and mutually responsible for the conduct and management of the affairs of the City in accordance with the Charter, this Code, general law, and the ordinances, resolutions, and orders of Council.

In addition to specific provisions concerning these officers elsewhere in the Charter and in this Code, these Officers shall hold administrative authority over their respective departments and shall competently and fairly exercise the power and duties described in this section over the personnel assigned to their departments by Council. These Officers shall:

- (a) Exercise sole responsibility for the appointment, delegation of authority, supervision, performance evaluation, and discipline, including removal, of all City employees assigned by Council to their respective departments, except as otherwise provided by law, or by rules adopted by Council.
- (b) Exercise sole responsibility for the direction, supervision, and administration of all departments, offices, and agencies of the City falling within their respective departments, except as otherwise provided by law, or by rules adopted by Council.
- (c) Serve as the point of contact between elected officials, when they are acting in their capacity as elected officials, and the personnel assigned to these Officers' departments. Individual elected officials shall not attempt to influence or direct the work or actions of any employee, except as otherwise specifically allowed by law, or by rules adopted by Council.
- (d) Attend all meetings of Council, with the right to take part in any discussion or deliberation. The Administrative Officers may not vote on issues before Council.
- (e) Ensure that all laws, ordinances, and provisions of the Charter, Code, and acts of the Council are faithfully executed and enforced.
- (f) Collaborate to prepare and submit to the Finance Committee and Council the annual budget and capital program.
- (g) Propose to the Council official acts of the City, including ordinances, policies, and rules, which Council may by ordinance or other action adopt with or without amendment.
- (h) Make such reports as the Council may require concerning the operations of City departments, offices, and agencies.
- (i) Keep the Council fully advised as to the condition and future needs of the City and make recommendations to the Council concerning the affairs of the City.

- (j) Devote all assigned working time to the performance of the duties of their offices, and while occupying such offices are not to engage, directly or indirectly, or be actively interested in any private business which would conflict with the performance of duties concerning the affairs of the City.
- (k) Propose annually to Council short- and long-term goals and objectives to be accomplished in the performance of their duties.
- (l) Perform such other duties as are specified in the Charter, this Code, or other acts of Council.



## CITY OF ELKINS AGENDA ITEM REPORT

<b>Meeting Date:</b>	October 14, 2024
<b>Section:</b>	New business
<b>Category:</b>	Action Item
<b>Agenda Item Name:</b>	Cybersecurity policy
<b>Recommended By:</b>	Dewaine Corley, IT consultant to the city
<b>Summary:</b>	The city lacks a comprehensive, modern cybersecurity policy. The attached is proposed for adoption.
<b>Fiscal Impact:</b>	n/a
<b>Recommendation:</b>	Consider for recommendation to council
<b>Attachments:</b>	1. CYBERSECURITY POLICY AND PROCEDURES Draft 2



## CYBERSECURITY POLICY AND PROCEDURES

### 1. Purpose:

The purpose of this policy is to establish the City of Elkins guidelines for computer security and protection of an organization's networks and its content or knowledge base, and to minimize the risk of internal and external cyber threats.

### 2. Scope:

This policy applies to all City elected officials, **appointed officials**, employees, contractors, consultants, and others specifically authorized to access information and associated assets owned, operated, controlled, or managed by the City of Elkins.

### 3. Policy:

The City of Elkins is committed to building a strong cybersecurity program to support, maintain, and secure critical infrastructure and data systems. In order to achieve this, the City will identify, evaluate, and take steps to avoid or mitigate risk to the City's information assets and prevent unauthorized digital or physical access, damage, theft, compromise, or interference to the City's information systems and facilities. These steps include implementing and operating controls to manage the City's information security risks and ensuring that all users of information assets are aware of their responsibilities in protecting those assets while complying with all applicable federal, state, or other regulations

#### 4. Responsibilities

Roles and responsibilities must be separated so that a single individual, account, or function cannot intentionally or unintentionally subvert a critical process. Controls must also be put in place so that no single person can access, modify, or use assets without authorization or detection. Achieving and maintaining cybersecurity is a shared responsibility. **Information Technology Manager, once appointed, will ensure that a written Cybersecurity Policy is implemented,** reviewed and updated on a periodic basis; including providing training and updates to City staff; confirm identification, acquisition, and implementation of information system software and hardware; identify locations where Personally Identifiable Information (PII) is stored and accessible; provide input for who should have access to PII and with what types of privileges or access rights, performing periodic classification assessments and ensuring regular reviews to update and manage changes to risk; assess system vulnerabilities and implement security tools and safeguards for protecting PII; ensure implementation, enforcement, and effectiveness of IT Security policies and procedures; plan, execute, and lead security audits across the City; facilitate an understanding and awareness that security requires participation and support at all organizational levels; and oversee daily activities and use of information systems to ensure employees, business partners, and contractors adhere to these policies and procedures. **Under the direction of the IT Manager, once appointed, the Information Technology Administrator will help implement and enforce the items outlined in this policy.** They will manage logs and events of all systems, and conducting periodic reviews to ensure our cybersecurity. All users, including employees, elected officials, **appointed officials, contractors, must comply with all aspects of this policy.** Users are responsible for the acceptable use and security of infrastructure and data.

#### 5. Standards:

##### 5.1 Asset Management

An inventory of all approved hardware and software on the City's network and systems will be maintained that documents the following:

- The employee in possession of the hardware or software
- Date of purchase
- Serial number
- Type of device and description ( OS, Processor type, RAM, Manufacture, etc.)
- For licensed software: # of licenses, license renewal date(s), other restrictions, etc.

## 5.2 Personally Identifiable Information (PII)

An inventory of all current PII information by type and location will be maintained. The following table will be used to inventory PII.

<u>Location</u>	<u>PII by type</u>	<u>Essential</u>	<u>Location</u>	<u>Owner</u>
Website				
Contractors				
File in a staff office				
File in building				
File offsite				
Desktop				
HR System				
Financial System				
Laptop				
Flash drive				
Cell phones				
Tablets				
Other				

With the exception of the Police Department who have their own records retention policy, each manager will determine if PII being collected by their department is essential. If PII is not essential, it will either not be collected, or (if collected) will be destroyed per West Virginia's records retention schedule and as per City policy and procedures. The City will not collect sensitive information, such as Social Security numbers if there is no legitimate business need.

The West Virginia Identity Theft Protection Act, **West Virginia Code Section 61-3-54** prohibits anyone (individual, private or public corporation, or business) who maintains Social Security numbers from:

- Printing a consumer's SSN on any mailed materials not requested by the consumer unless redacted
- Printing a consumer's SSN on a card used by the consumer that is required to access products or services
- Publicly posting or displaying a consumer's SSN, such as on a website

Exceptions include requirements by state or federal laws, including statute records (such as W2s, W4s, 1099s, etc.) that are required by law to be made available to the public for use for internal verification or administrative processes, or for enforcing a judgment or court order

### 5.3 Identity Management, Authentication and Access Control

Information Technology Manager, once appointed, is responsible for ensuring that access to the City's systems and data is appropriately controlled. All systems housing City data (including laptops, desktops, tablets, and cell phones) are required to be protected with a password or other form of authentication. Except for the instances noted in this policy, users with access to the City systems and data shall not share passwords with anyone.

The City has established the following password configuration requirements for all systems and applications (where applicable):

- Minimum password length: minimum 10 characters using number, sign, upper and lower case letters.
- Password complexity: use a passphrase rather than a password
- Prohibited reuse for six (6) iterations
- PIN'S no less than 6 characters.
- Changed periodically (every 180 days)
- Invalid login attempts set to lock after three Employees are encouraged to follow further safeguards such as:
  - Not allowing PII on mobile storage media
  - Utilizing Locking file cabinets
  - Not allowing PII left on desktops
  - Encrypting sensitive files on computers
  - Requiring password protection
  - Enabling multi-factor authentication
- Following the record retention plan and destroying records no longer required Where possible, multi-factor authentication will be used when users authenticate to the City's systems.
- Users are granted access only to the system data and functionality necessary for their job responsibilities.
- Privileged and administrative access is limited to authorized users who require escalated access for their job responsibilities and where possible will have two accounts: one for administrator functions and a standard account for day-to-day activities.
- Once appointed, all user access requests must be approved by the Information Technology Manager.

- Once appointed, the Information Technology Manager shall make sure all system access is removed of all users who separate from the City within 48 hours.

On an annual basis, a review of user access will be conducted by the departments **under the direction of the Information Technology Manager, once appointed**, to confirm compliance with the access control policies outlined above.

#### 5.4 Awareness and Training

City staff are required to complete City assigned security training:

1. Upon hire and within 30 days of receiving login credentials
2. Annually

**On an annual basis, the IT Manager, once appointed, will conduct** email phishing exercises of its users. The purpose of these tests is to help educate users on common phishing scenarios. It will assess the level of awareness and comprehension of phishing, understanding, and compliance with policy around safe handling of emails containing links and/or attachments, and the ability to recognize a questionable or fraudulent message.

#### 5.5 Data Security

##### 5.5.1 Data Classification

Users must adhere to the Records Retention Policy regarding the storage and destruction of data. Data residing on City's systems must be continually evaluated and classified into the following categories:

- Users' Personal Use: Includes individual user's personal data, emails, documents, etc. This policy does not apply to a user's personal information.
- Marketing or Informational Material: Includes already-released marketing material, commonly known information, data freely available to the public, etc. and this policy does not apply
- Operational: Includes data for basic organizational operations, communications with vendors, employees, etc. (non-confidential). The majority of data will fall into this category.
- Confidential: Any information deemed confidential. The following list provides guidelines on what type of information is typically considered confidential. Confidential data may include:
  - Employee or customer Social Security numbers or personally identifiable information (PII)

- Personnel files o Protected Health Information (PHI)
- Network diagrams and security configurations
- Privileged communications regarding legal matters.
- Passwords/passphrases o Bank account information and routing numbers
- Payroll information o Credit card information
- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

### 5.5.2 Data Storage

The following guidelines apply to storage of the different types of organizational data

- Operational: Operational data should be stored on a server that gets the most frequent backups. Some type of system- or disk-level redundancy is encouraged.
- Confidential: Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard or code secured. **No thumb drive, external hard drives will be left in unsecured areas where the ability for others to have access or ability to transport data.**

### 5.5.3 Data Transmission

The following guidelines apply to the transmission of the different types of organizational data. •

**Confidential:** Confidential data shall not be 1) Transmitted outside the City's network without the use of strong encryption 2) Left on voicemail systems, either inside or outside the organization's network. 3) Transmitted via email, outside of the organization's network. **4) Placed on external storage devices for the purpose of transmission outside our network.**

Data while transmitted, includes any data sent across the City's network or any data sent to or from a City-owned or City-provided system. Types of transmitted data that shall be encrypted include:

- VPN tunnels
- Remote access sessions
- Web applications • Email and email attachments
- Remote desktop access
- Communications with applications/databases

#### 5.5.4 Data Destruction

Employees must follow State's and City's records retention policy and procedures before destroying any data.

- Confidential: Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply to data located on City-owned or City-provided systems, devices, media, etc.:

- Storage media (CD's, DVD's, storage devices): Physical destruction is required, some shredders may be able to perform this function.
- Hard drives/systems/mobile storage media: At a minimum, DoD three (3) pass data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the City shall use the most secure commercially available methods for data wiping. Alternatively, the City may physically destroy the storage media.

#### 5.5.5 Data Storage

Stored Data includes any data located on City-owned or City-provided systems, devices, media, etc.

Examples of encryption options for stored data include:

- Whole disk encryption • Encryption of partitions/files
- Encryption of disk drives
- Encryption of personal storage media/USB drives

- Encryption of backups
- Encryption of data generated by applications

## **6. Information Protection Processes and Procedures:**

### 6.1 Secure Software Development

Where applicable, all software development activities performed by City or by vendors on behalf of the organization shall employ secure coding practices including those outlined below.

A minimum of 2 software environments for the development of software systems should be available – development/training and a production environment. Software developers or programmers are required to develop in the development/training environment and promote objects into the production environments. The development/training environment is used for assurance testing by the end-user and the developer. The production environment should be used solely by the end-user for production data and applications. Compiling objects and the source code is not allowed in the production environment.

### 6.2 Contingency Planning

The City's business contingency capability is based upon cloud and local backups of all critical business data. This critical data is defined as "the data that is critical to successful organization operation". Full data backups will be performed on a daily basis. Confirmation that backups were performed successfully will be conducted daily. Testing of cloud backups and restoration capability will be performed on a monthly basis.

During a contingency event, all IT decisions and activities will be coordinated through and under the direction of the Information Technology Manager.

The following are some examples of possible business contingency scenario procedures:

- In the event that one or more of City 's systems or applications are deemed corrupted or inaccessible, **the Information Technology Manager, once appointed**, will work with the respective vendor(s) to restore data from the most recent cloud and local backup and, if necessary, acquire replacement hardware.
- In the event that the location housing the City systems are no longer accessible, **the Information Technology Manager, once appointed**, will work with the respective vendor(s) to acquire any necessary

replacement hardware and software, implement these at one of the City's other sites, and restore data from the most recent cloud, off-site, or local backup.

### **6.3 Network Infrastructure**

The City will protect its electronic communications network from the Internet by utilizing a firewall. For maximum protection, the network devices shall meet the following configuration standards:

- Vendor recommended, and industry standard configurations will be used.
- Changes to firewall and router configuration will be approved by Information Technology Manager
- Both router and firewall passwords shall be secured and difficult to guess.
- The default policy for the firewall for handling inbound traffic shall be to block all packets and connections unless the traffic type and connections have been specifically permitted.
- Inbound traffic containing ICMP (Internet Control Message Protocol) traffic shall not be passed in from the Internet, or from any un-trusted external network.
- All web services running on routers shall be disabled.
- Simple Network Management Protocol (SNMP) Community Strings shall be made (changed from the default "public") "private".

### **6.4 Network Servers**

Servers typically accept connections from several sources, both internal and external. As a general rule, the more sources that connect to a system, the more risk associated with that system, so it is particularly important to secure network servers.

- Unnecessary files, services, and ports shall be removed or blocked. If possible, a server hardening guide, which is available from the leading operating system manufacturers, shall be followed.
- Network servers, even those meant to accept public connections, shall be protected by a firewall or access control list.
- When possible, a standard installation process shall be developed for the City's network servers. A standard process will provide consistency across servers no matter which employee or contractor handles the installation.
- Clocks on network servers shall be synchronized with the City's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

## 6.5 Network Segmentation

Network segmentation is used to limit access to data within the City network based upon data sensitivity. The City maintains two wireless networks. The guest/public wireless network will grant the user internet access only. Access to the secure wireless network is limited to the City staff and devices, and provides the user access to the intranet.

Under the direction of the Information Technology Manager, a third-party network administrator manages the network, monitors firewall logs, and operating system event logs. The Information Technology Manager authorizes vendor access to the system components as required for maintenance.

## 7. Protective Technology:

### 7.1 Email Filtering

The City shall filter email, at a minimum of, the Internet gateway and/or the mail server. This filtering will help reduce spam, viruses, or other messages that may be deemed either contrary to this policy or a potential risk to the City's IT security.

Additionally, email or anti-malware programs may be implemented to identify and quarantine emails that are deemed suspicious.

### 7.2 Internet Filtering

The IT Department, once established, shall block access to internet websites and protocols that are deemed inappropriate or pose a security risk. Some examples of blocked categories are adult/sexually explicit material, advertisements, hacking, violence and hate content.

### 7.3 Network Vulnerability Assessments

On a quarterly basis, the IT Department, once established, will perform both internal and external network vulnerability assessments. The purpose of these assessments is to establish a comprehensive view of the organization's network as it appears internally and externally. These evaluations will be conducted under the direction of Information Technology Manager to identify weaknesses with the

network configuration that could allow unauthorized and/or unsuspected access to the organization's data and systems.

In addition, annual penetration testing will be run to identify weaknesses or vulnerabilities that will need to be addressed.

## **8. Anomalies and Events:**

The following logging activities are conducted by IT System Administrator/ Information Technology Manager, once appointed:

- Domain Controllers - Active Directory event logs will be configured to log the following security events: account creation, escalation of privileges, login failures, and excessive repeated login attempts.
- Application Servers - Logs from application servers (e.g., web, email, database servers) will be configured to log the following events: errors, faults, login failures, and excessive repeated login attempts.
- Network Devices - Logs from network devices (e.g., firewalls, network switches, routers) will be configured to log the following events: errors, faults, login failures, and excessive repeated login attempts.

Passwords should not be contained in logs. Passwords displayed on posted notes or that are visible to other individuals is strictly prohibited.

Logs of the above events will be reviewed by the IT System Administrator, utilizing a SIEM (Security Information and Event Management), at least once per month. Event logs will be configured to maintain record of the above events for at least three months.

## **9. Security Continuous Monitoring:**

### 9.1 Anti-Malware Tools

All City servers and workstations shall utilize endpoint protection software to protect systems from malware and viruses. Real-time scanning will be enabled on all systems and weekly malware scans will be performed. A monthly review of the endpoint protection software dashboard will be conducted by IT System Manager, once appointed to confirm the status of virus definition updates and scans.

## 9.2 Patch management

All software updates and patches will be distributed to all City systems as follows:

- Workstations shall be configured to install software updates every night automatically.
- Server software updates shall be manually installed at least quarterly
- Any exceptions shall be documented.

## **10. Response Planning**

The City's annual security awareness training shall include direction and guidance for the types of security incidents users could encounter, what actions to take when an incident is suspected, and who is responsible for responding to an incident. A security incident, as it relates to the City's information assets, can be defined as either an Electronic or Physical Incident.

**Information Technology Manager, once appointed, is responsible for** coordinating all activities during a significant incident, including notification and communication activities and the chain of escalation and deciding if/when outside agencies, need to be contacted.

### **10. Electronic Incidents:**

10.1 This type of incident can range from an attacker or user accessing the network for unauthorized/malicious purposes to a virus outbreak or a suspected Trojan or malware infection. When an electronic incident is suspected, the steps below should be taken in order.

1. Remove the compromised device from the network by unplugging or disabling network connection. Do not power down the machine.

2. **Once appointed, report the incident to the IT System Administrator or Information Technology Manager.**

3. Contact the third-party service provider (and/or computer forensic specialist) as needed. The remaining steps should be conducted with the assistance of the third-party IT service provider and/or computer forensics specialist.

4. Disable the compromised account(s) as appropriate.

5. Backup all data and logs on the machine, or copy/image the machine to another system.
6. Determine exactly what happened and the scope of the incident.
7. Determine how the attacker gained access and disable it.
8. Rebuild the system, including a complete operating system reinstall.
9. Restore any needed data from the last known good backup and put the system back online.
10. Take actions, as possible, to ensure that the vulnerability will not reappear.
11. Conduct a post-incident evaluation. What can be learned? What could be done differently?

## 10.2 Physical Incidents

A physical IT security incident involves the loss or theft of a laptop, mobile device, PDA/Smartphone, portable storage device, or other digital apparatus that may contain City's information. All instances of a suspected physical security incident should be reported immediately to the IT System Administrator or **Information Technology Manager once appointed.**

## 10.3 Notification

If an electronic or physical security incident is suspected of having resulted in the loss of, or unauthorized access to employee PPI or third-party/customer data, notify the City Attorney's office for direction on procedures for notification of the public or affected entities as well as necessary government agencies.

## **11. Recovery & Restoration:**

Recovery processes and procedures shall be executed and maintained to ensure timely restoration of systems and/or assets affected by cybersecurity events.

**Information Technology Manager, once appointed, is responsible for managing and directing activities during an incident, including the recovery steps.**

Recovery planning and processes are improved by incorporating lessons learned into future activities.

Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet service providers, owners of the affected systems, victims, and vendors.

External communications should only be handled by designated individuals at the direction of the City Administrator. Recovery activities are communicated to internal stakeholders, executives, and management teams.

## 12. References:

West Virginia Administrative

West Virginia Revised Code Records, public reports and meetings West Virginia Identity Theft Protection Act

City of Elkins HR Rules City of Elkins Use of City Information Technology Policy & Procedures

City of Elkins Social Media Policy and Procedures

## 13. Review of Policy and Procedures:

This policy will be reviewed annually or as state and federal regulations are revised and necessitate a change in the policy or procedures.

Adopted: July 2024 Appendix B –

Confidentiality and Non-Disclosure Agreement This Confidentiality and Nondisclosure Agreement (the "Agreement") is entered into by and between City of Elkins ("Disclosing Party") and \_\_\_\_\_ ("Receiving Party") for the purpose of preventing the unauthorized disclosure of Confidential Information as defined below. The parties agree to enter into a confidential relationship with respect to the disclosure of certain proprietary and confidential information ("Confidential Information").

1. Definition of Confidential Information. For purposes of this Agreement, "Confidential Information" shall include all information or material that has or could have commercial value or other utility in the business in which Disclosing Party is engaged. Examples of Confidential Information include the following:
  - Employee or customer Social Security numbers or personal information
  - Customer data • Entity financial data
  - Product and/or service plans, details, and schematics,
  - Network diagrams and security configurations
  - Communications about entity legal matters
  - Password
  - Bank account information and routing numbers
  - Payroll information
  - Credit card information

- Any confidential data held for a third party

2. Exclusions from Confidential Information. Receiving Party's obligations under this Agreement do not extend to information that is:

- (a) publicly known at the time of disclosure or subsequently becomes publicly known through no fault of the Receiving Party;
- (b) discovered or created by the Receiving Party before disclosure by Disclosing Party;
- (c) learned by the Receiving Party through legitimate means other than from the Disclosing Party or Disclosing Party's representatives; or
- (d) is disclosed by Receiving Party with Disclosing Party's prior written approval.

3. Obligations of Receiving Party. Receiving Party shall hold and maintain the Confidential Information in strictest confidence for the sole and exclusive benefit of the Disclosing Party. Receiving Party shall carefully restrict access to Confidential Information to employees, contractors, and third parties as is reasonably required and shall require those persons to sign nondisclosure restrictions that are at least as protective as those in this Agreement. Receiving Party shall not, without the prior written approval of Disclosing Party, use for Receiving Party's own benefit, publish, copy, or otherwise disclose to others, or permit the use by others for their benefit or to the detriment of Disclosing Party, any Confidential Information. Receiving Party shall return to Disclosing Party any and all records, notes, and other written, printed, or tangible materials in its possession pertaining to Confidential Information immediately if Disclosing Party requests it in writing.

4. Time Periods. The nondisclosure provisions of this Agreement shall survive the termination of this Agreement and Receiving Party's duty to hold Confidential Information in confidence shall remain in effect until the Confidential Information no longer qualifies as a confidential or until Disclosing Party sends Receiving Party written notice releasing Receiving Party from this Agreement, whichever occurs first.

5. Relationships. Nothing contained in this Agreement shall be deemed to constitute either party a partner, joint venture or employee of the other party for any purpose.

6. Severability. If a court finds any provision of this Agreement invalid or unenforceable, the remainder of this Agreement shall be interpreted so as best to affect the intent of the parties.

7. Integration. This Agreement expresses the complete understanding of the parties with respect to the subject matter and supersedes all prior proposals, agreements, representations, and understandings. This Agreement may not be amended except in a writing signed by both parties.

8. Waiver. The failure to exercise any right provided in this Agreement shall not be a waiver of prior or subsequent rights.

This Agreement and each party's obligations shall be binding on the representatives, assigns, and successors of such party. Each party has signed this Agreement through its authorized representative.

**Disclosing Party**

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

Printed Name: \_\_\_\_\_

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

Dated: \_\_\_\_\_

Receiving Party By: \_\_\_\_\_

Printed Name: \_\_\_\_\_

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

Dated: \_\_\_\_\_



## CITY OF ELKINS AGENDA ITEM REPORT

<b>Meeting Date:</b>	October 14, 2024
<b>Section:</b>	New business
<b>Category:</b>	Action Item
<b>Agenda Item Name:</b>	Consideration of changes to the floodplain ordinance
<b>Recommended By:</b>	City Attorney
<b>Summary:</b>	When FEMA submitted their Community Assistance Visit (CAV) report, they suggested several changes to the City's Floodplain ordinance. The City Attorney will present more information at the meeting.
<b>Fiscal Impact:</b>	TBD
<b>Recommendation:</b>	Consider for recommendation to Council
<b>Attachments:</b>	None