450 S. Parish Avenue
Johnstown, CO 80534
970.587.4664
JohnstownCO.gov

Cybersecurity Policy and Procedures

1. Purpose

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

2. Scope

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

3. Policy

The Town of Johnstown is committed to building a strong cybersecurity program to support, maintain, and secure critical infrastructure and data systems. To achieve this, the Town will identify, evaluate, and take steps to avoid or mitigate risk to the Town's information assets and prevent unauthorized digital or physical access, damage, theft, compromise, or interference to the Town's information systems and facilities. These steps include implementing and operating controls to manage the Town'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. The Town Manager or his/her designee will ensure that a written Cybersecurity Policy is implemented, reviewed and updated on a periodic basis; including providing training and updates to Town 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 Town; 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 Town Manager or his/her designee, the IT staff will help implement and enforce the items outlined in this policy. They will manage logs and events of all systems, utilizing a SIEM (Security Information and Event Management) system, and conduct periodic reviews to ensure our cybersecurity.

All users, including employees, elected 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 Town 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
- 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.

Location	PII by Type	Essential	Location	Owner
Website				
Contractors				
File in staff office				
File in building				
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 Colorado records retention schedule and as approved by the Town Clerk per Town policy and procedures. The Town will not collect sensitive information, such as Social Security numbers or EIN numbers if there is no legitimate business need.

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

The Town Manager or his/her designee is responsible for ensuring that access to the Town's systems and data is appropriately controlled. All systems housing Town 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 Town systems and data shall not share passwords with anyone.

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

- Minimum password length: 8 characters
- Password complexity: use a passphrase rather than a password
- Prohibited reuse for six (6) iterations
- 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 Town'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.
- All user access requests must be approved by the Town Manager or his/her designee.
- The Town Manager or his/her designee shall make sure all system access is removed for all users who separate from the Town within 48 hours.

On an annual basis, a review of user access will be conducted by the departments under the direction of the Town Manager or his/her designee, to confirm compliance with the access control policies outlined above.

5.4 Awareness and Training

Town staff are required to complete Town assigned security training:

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

2. Annually

On an annual basis, the Town Manager or his/her designee, will conduct email phishing exercises for 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 Town's Records Policy regarding the storage and destruction of data. Data residing on Town'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). Most 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
  - Protected Health Information (PHI)
  - Network diagrams and security configurations
  - Privileged communications regarding legal matters
  - Passwords/passphrases
  - Bank account information and routing numbers
  - Payroll information
  - 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.

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
    - Transmitted outside the Town's network without the use of strong encryption
    - Left on voicemail systems, either inside or outside the organization's network.
    - Transmitted via email, outside of the organization's network.

Data while transmitted includes any data sent across the Town's network or any data sent to or from a Town-owned or Town-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 the State's and Town'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 Town owned or Town-provided systems, devices, media, etc.:

- Storage media (CD's, DVD's): 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 Town shall use the most secure commercially available methods for data wiping. Alternatively, the Town may physically destroy the storage media.

5.5.5 Data Encryption

Stored Data includes any data located on Town-owned or Town-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 the Town 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 Town'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 daily. Confirmation that backups were performed successfully will be conducted daily. Testing of cloud backups and restoration capability will be performed monthly.

During a contingency event, all IT decisions and activities will be coordinated through and under the direction of the Town Manager. The following are some examples of possible business contingency scenario procedures:

- In the event that one or more of Town 's systems or applications are deemed corrupted or inaccessible, the Town Manager or his/her designee 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 Town systems are no longer accessible, the Town Manager or his/her designee will work with the respective vendor(s) to acquire any necessary replacement hardware and software, implement these at one of the Town's other sites, and restore data from the most recent cloud, off-site, or local backup.

6.3 Network Infrastructure

The Town 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 the firewall and router configuration will be approved by Town Manager or his/her designee.
- 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. Generally, 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 Town'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 Town'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 Town network based upon data sensitivity. The Town 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 Town staff and devices and provides the user access to the intranet. Under the direction of the Town Manager or his/her designee, a third-party network administrator manages the network user accounts, monitors firewall logs, and operating system event logs. The Town Manager or his/her designee authorizes vendor access to the system components as required for maintenance.

7. Protective Technology

7.1 Email Filtering

The Town shall filter email, at a minimum, 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 Town'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 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 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 Town Manager or his/her designee 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 under the direction of Town Manager or his/her designee:

- 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.

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 Town 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 the IT System Administrator to confirm the status of virus definition updates and scans.

9.2 Patch management

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

- Workstations shall be configured to install software updates automatically.

- Server software updates shall be manually installed at least quarterly.

- Any exceptions shall be documented.

10. Response Planning

The Town'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 Town's information assets, can be defined as either an Electronic or Physical Incident. The Town Manager or his/her designee 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.

10.1 Electronic Incidents

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. 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 Town's information. All instances of a suspected physical security incident should be reported immediately to the IT System Administrator or Town Manager or his/her designee.

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 Town Attorney 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.

The Town Manager or his/her designee 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 Town Manager. Recovery activities are communicated to internal stakeholders, executives, and management teams.

12. 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.