Agenda
July 3, 2023
at School
Town of Arietta

- Call to Order
- Pledge of Allegiance
- Roll Call
- Motion to approve minutes for the June 20, 2023 meeting
- Resolutions
  23-07-36 IT Policies

  Snowmobile Trails – Grier
  Town Buildings and Grounds - Stobo
  Internal Management / Insurance,
  Recreation, Website & Chamber- C Wilt
  Finance / Airport-C. Rhodes
  Lake / Dam / Invasive/campsite -Rudes
  Craig Small – Highway Superintendent
  Mel Lascola - Zoning

- **Old Business**
  - Frontier Lease
  - Veterans- roll of honor and memorial
- **New Business**

- Motion to accept the bills
- Public Comment
- Designation of next Meeting July 17, 2023
- **Motion to adjourn**

TOWN OF ARIETTA

At a regular meeting of the Arietta Town Board at the Piseco Common School, 1722 State Route 8, Piseco in the Town of Arietta, Hamilton County, New York on:

July 3, 2023, at 5:00 pm

Resolution # 23-07-36

Subject: **Accept IT and Security Policies and IT Security Training**

Resolution Offered By: _____

WHEREAS: the Arietta Town Board approved entering into an agreement with Canada Lake Computer Services, Inc. to provide and manage written IT and Security Policies and IT Security Training for one year, starting June 1, 2023 thru May 31, 2024. (Resolution #23-06-31), and

WHEREAS: the Town of Arietta has received a written IT and Security Policies package from Canada Lake Computer Services, Inc., as outlined in the attached IT and Security Policies, and

THEREFORE, LET IT BE RESOLVED: the Arietta Town Board, after reviewing the attached, does hereby approve and adopt the IT and Security Policies package from Canada Lake Computer Services, Inc., effective immediately.

Seconded by: _____ and put to a vote, which resulted as follows:

AYES:		NOES:		ABSTAIN		ABSENT:	
Jacquelyn Grier	_____	Jacquelyn Grier	_____	Jacquelyn Grier	__	Jacquelyn Grier	____
Sarah Rudes	_____	Sarah Rudes	_____	Sarah Rudes	_	Sarah Rudes	_____
Douglas Stobo	_____	Douglas Stobo	_____	Douglas Stobo	__	Douglas Stobo	_____
Christy Wilt	_____	Christy Wilt	_____	Christy Wilt	__	Christy Wilt	_____
Christian Rhodes	_____	Christian Rhodes	_____	Christian Rhodes	__	Christian Rhodes	_____

_____ _____

Town Clerk Date

Town of Arietta

IT and Security Policies

2023

Clean Desk

Table of Contents

Assigned Roles and Contact Info

Emergency Contacts

Chris Rhodes	518 548 3415 518 571 6066	chris@townofarietta.com
Craig Small	518 548 7302	highway@townofarietta.com
Joyce Page	518 548 3415	joyce@townofarietta.com
Brian McIntosh	518 835 4103 518 774 5334	brian@clcsinc.com

IT Security Officer

Brian McIntosh

Senior Management

Chris Rhodes (Supervisor)

Management

Craig Small
Joyce Page

Acceptable Use Policy

Purpose - To communicate Town of Arietta management's expectations regarding acceptable use of town information assets. Inappropriate use exposes Town of Arietta to risks including virus attacks, compromise of network systems and services, and legal issues.

Roles and Responsibilities

IT Security Officer
Annually – The IT Security Officer will review controls relating to acceptable use as part of the IT risk assessment.

Senior Management
Monthly – review any infractions and adjust assure compliance.

Management
Weekly –Supervisor will perform a walkaround of the office to ensure that confidential, sensitive data is secure and that employees and town officials are adhering to the clean desk policy as described below.

All Employees
All employees, including management, board members, as well as contractors, consultants or other parties with access to town information technology resources or data are required to adhere to this policy.

All employees, including management and board members, are required to certify in writing that they have read and understood all relevant policies, standards and procedures.

Details

- Employees and town officials shall use information resources for business in accordance with their job functions and responsibilities, except as otherwise provided by management directives.
- Employees and town officials are permitted limited personal use of information resources if the use does not result in a loss of employee productivity, interfere with official duties or business, and involves minimal additional expense to the town. Unauthorized or improper use of information resources may result in loss of use or limitations on use of those resources.
- When using information resources, employees and town officials are expected to:
    - Act responsibly to ensure the ethical use of town information resources.
    - Acknowledge the right of Town of Arietta to restrict or rescind computing privileges at any time.
    - Use security measures to protect the confidentiality, integrity, and availability of information, data, and systems.
    - Conduct themselves professionally in the workplace and to refrain from using information resources for activities that are inappropriate.
    - Respect all pertinent licenses, copyrights, contracts, and other restricted or proprietary information.

- Use good judgment in accessing the Internet. Each use of the Internet should be able to withstand public scrutiny without embarrassment to Town of Arietta.
- Safeguard their user IDs and passwords and use them only as authorized. Any actions taken under an assigned identification (e.g., userid) are the responsibility of the user.
- Respect Town of Arietta property.
- Make only appropriate use of data to which they have access.
- Exercise good judgment regarding the reasonableness of personal use.
- Use information resources efficiently.
- Immediately notify the IT Security Officer or a supervisor if suspicious or malicious behavior or activity is noticed.
- Protect non-public information, as defined below, whether in electronic or non-electronic format:
  "(n) Nonpublic information means:
  (i) Personally identifiable financial information; and
  (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available."
  This is a legal requirement and is not subject to interpretation. All entities described under "Roles and Responsibilities" must protect customer and consumer non-public personal information. This includes adhering to a "clean desk" policy, where work areas are kept free of sensitive or confidential information, especially at the end of the business day.
- Share non-public customer information or sensitive information, including, but not limited to, payroll data, human resources data, and credit data, only with authorized parties and only via approved methods. Unencrypted e-mail should never be used to transmit sensitive data. Web sites using Secure Sockets Layer (SSL) may be used to transmit sensitive data, though the IT Security Officer should be consulted if there are any questions concerning a web site's legitimacy or appropriateness.

Under no circumstances is an employee of Town of Arietta authorized to engage in any activity that is illegal under local, state, federal, or international laws or regulations while using town information resources.

- The following activities are strictly prohibited:
  - Intentionally corrupting, misusing, or stealing software or any other computing resource.
  - Accessing Town of Arietta systems that are not necessary for the performance of the employee's duties.
  - Performing functions that are not related to the employee's job responsibilities on systems that they are otherwise authorized to access.
  - Making unauthorized changes to Town of Arietta computer resources, including installation of unapproved software or interfering with security measures (such as audit trail logs and anti-malware software).
  - Copying town proprietary software or business data for personal or other non-business use.
  - Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the end user does not have an active license.
  - Transmitting, storing, or processing sensitive data except as authorized.
  - Unauthorized access to other computer systems using Town of Arietta information resources.

- Accessing information resources, data, equipment, or facilities in violation of any restriction on use.
- Using Town of Arietta computing resources for personal or private financial gain.
- Using another person's computer account, with or without their permission.
- Implementing any computer systems without authorization from management.
- Knowingly, without written authorization, executing a program that may hamper normal town computing activities.
- Adding components or devices (e.g., PDAs, USB/thumb drives, cameras, etc) to Town of Arietta desktops without explicit approval from management.
- Employees and town officials will ensure that equipment is sited in such a way as to reduce the possibility that any unauthorized individuals may covertly insert a USB or thumb drive in an effort to capture information or data. Employees and town officials will report any attempts by unauthorized individuals to insert a drive.
- Employees and town officials will take note of and report anyone that is behaving in an unusual manner while talking or using a cell phone. Special attention should be given if it appears that someone may be attempting to position themselves in such a way as to view sensitive information while using a cell phone that may contain a camera.
- Use of Instant Messaging (IM), peer-to-peer (P2P) file sharing, Internet Relay Chat and other similar programs or technologies
- Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e- mail bombs, etc.).
- Revealing account passwords to others or allowing the use of one's account by others, including family and other household members when work is being done at home.
- Revealing system passwords (e.g. Windows domain passwords, database passwords, etc.) to anyone who is not specifically authorized to use them.
- Effecting security breaches or disruptions of network communication.
- Unauthorized security scanning, network monitoring, or data interception that is not part of the employee's regular job duties.
- Circumventing any town information security measures.
- Interfering with or denying service to other information resource users.
- Providing information about, or lists of, Town of Arietta employees and town officials to parties outside of the town that are not required for business.
- Sending unsolicited e-mail messages (spam).
- Any form of harassment via e-mail, telephone, pager, IRC, SMS, or other communication method, whether through language, frequency, or size of messages.
- Creating or forwarding "chain letters," "Ponzi" or other "pyramid" schemes of any type.
- Posting Town of Arietta information to external news groups, bulletin boards or other public forums without authority, or conducting any activity that could create the perception that communication was made in one's official capacity as a Town of Arietta employee, unless appropriate approval has been obtained.
- Any personal use that could cause congestion, delay, or disruption of service to any Town of Arietta system or equipment.
- Using Town of Arietta office equipment or information resources for activities that are illegal, inappropriate, or offensive to fellow employees or the public. This includes, but is not limited to, materials related to:
  - Sexually explicit or sexually oriented content
  - Ethnic, racial, sexist, or other offensive comments
  - Anything that is in violation of sexual harassment or hostile workplace laws
  - Making fraudulent offers of products, items, or services.
  - Gambling
  - Illegal weapons or terrorist activities
  - Planning or commission of any crime

- Forging or misrepresenting one's identity.

- Auditing and Privacy:
  - All use of Town of Arietta information resources may be monitored by the town.
  - Employees and town officials do not have an expectation of privacy or anonymity while using any Town of Arietta information resource at any time, including accessing the Internet and e-mail.
  - Users agree to be governed by acceptable usage policies and to have their usage audited. By using Town of Arietta information assets, employees and town officials imply their consent to disclosing the contents of any files or information maintained or passed through Town of Arietta information systems.
  - To the extent that employees and town officials wish that their private activities remain private, they should avoid using Town of Arietta information systems such as their computer, the Internet, or e-mail, for those activities.
  - Auditing procedures will be implemented to ensure compliance with Town of Arietta security policies.
  - System administrators can audit network logs, employ monitoring tools, and perform periodic checks for misuse.
- Employees and town officials agree to be bound by the following conditions for continued use of Town of Arietta information resources:
  - Employees, town officials and contractors will sign an agreement to comply with Town of Arietta information security policy.
  - Usage of Town of Arietta IT resources for illegal purposes will be reported to appropriate authorities.

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Access Control Policy

Purpose - To allow only authorized personnel and devices to access Town of Arietta information assets at the minimum level necessary to accomplish business purposes. Physical security is addressed in the "Physical Security Policy."

Roles and Responsibilities

IT Security Officer
Annually – The IT Security Officer will review access control as part of the IT risk assessment.

Internal Audit
Annually – Internal Audit will review access control.

Management
Annually, as job roles change or employee turnover occurs – A management member will review application access for appropriateness.

All ,
All Town of Arietta employees, including management, as well as contractors, consultants or other parties with access to information technology resources or data are required to adhere to this policy.

Details

Various personnel and devices need access to Town of Arietta information assets to accomplish the businesses purposes. This access should be minimized, controlled and audited. In specific:

- All users must read and sign the "Acceptable Use Policy" prior to accessing Town of Arietta information assets.
- All user access, including authorization, will be granted based on job role or function, per "User Access Procedures."
- All user access will be periodically reviewed or as job roles change, per "User Access Procedures."
- User authentication will use, at a minimum, single-factor authentication, such as unique usernames and passwords. If usernames and passwords are used, they must be unique and identify a single person.
- All device access will be periodically reviewed or as the computing environment changes.
- All devices will comply with the "Software Development, Acquisition, Maintenance and Auditing Policy."
- Network access to and from the Internet, as well as any other non-town network, will be protected by a firewall, configured per the "Perimeter Security Policy."
- Network access, operating system access and critical business application access will be regularly reviewed.
- All devices will be configured according to the concept of "least privilege." This includes:
    - Disabling or removing unnecessary services, features, modules, protocols or functions.

    - Restricting device access to approved personnel, per the "Access Control Policy."
    - Restricting user rights and permissions whenever possible, including running as a non-root or non-Administrator user, and restricting permissions to files, directories, configuration files, registry entries, etc.
- All devices will be configured with relevant auditing enabled, as determined by management and the IT Security Officer. The auditing should be configured to track, if possible:
    - Who
    - What
    - When
- Auditing should be configured to log to a central location, if possible, preferably using SYSLOG.

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Social Engineering Awareness Policy

Purpose –

1 To make employees and town officials aware that (a) fraudulent social engineering attacks occur, and (b) there are procedures that employees and town officials can use to detect attacks.

- Employees are made aware of techniques used for such attacks, and they are given standard procedures to respond to attacks.
- Employees and town officials know who to contact in these circumstances.
- Employees and town officials recognize they are an important part of Town of Arietta's security. The integrity of an employee is the best line of defense for protecting sensitive information regarding Town of Arietta's resources.

2 To create specific procedures for employees and town officials to follow to help them make the best choice when:

- Someone is contacting the employee - via phone, in person, email, fax or online - and elusively trying to collect Town of Arietta's sensitive information.
- The employee is being "socially pressured" or "socially encouraged or tricked" into sharing sensitive data.

Roles and Responsibilities

IT Security Officer
Annually – Provide awareness training.

All Employees
All Town of Arietta employees, including management, as well as contractors, consultants or other parties with access to information technology resources or data are required to adhere to this policy.

Details

Sensitive information of Town of Arietta will not be shared with an unauthorized individual if he/she uses words and/ or techniques such as the following:

- An "urgent matter"
- A "forgotten password"
- A "computer virus emergency"
- Any form of intimidation from "higher level management"
- Any "name dropping" by the individual which gives the appearance that it is coming from legitimate and authorized personnel.

- The requester requires the release of information that will reveal passwords, model, serial number, or brand or quantity of Town of Arietta resources.
- The techniques are used by an unknown (not promptly verifiable) individual via phone, email, online, fax, or in person.
- The techniques are used by a person that declares to be "affiliated" with Town of Arietta such as a sub-contractor.
- The techniques are used by an individual that says he/she is a reporter for a well-known press editor or TV or radio company.
- The requester is using ego and vanity seducing methods, for example, rewarding the front desk employee with compliments about his/her intelligence, capabilities, or making inappropriate greetings (coming from a stranger).

Action

- All persons MUST attend the security awareness training annually.
- If one or more circumstances described is detected by a person the identity of the requester MUST be verified before continuing the conversation or replying to email, fax, or online.
- If the identity of the requester described CANNOT be promptly verified, the person MUST immediately contact his/her supervisor or direct manager.
- If the supervisor or manager is not available, that person MUST contact the security personnel.
- If the security personnel is not available, the person MUST immediately drop the conversation, email, online chat with the requester, and report the episode to his/her supervisor before the end of the business day.

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Anti-Malware Policy

Purpose - To protect Town of Arietta information assets from malware, including viruses, worms, trojans, keystroke loggers, spyware, rootkits, etc.

Roles and Responsibilities

IT Security Officer

- Quarterly – The IT Security Officer will review anti-malware reports to ensure definitions are current on all machines and to isolate any machines experiencing malware infections.
- Annually – The IT Security Officer will review anti-malware controls as part of the IT risk assessment.

Internal Audit

Annually – Internal Audit will review anti-malware controls.

All Employees

All Town of Arietta employees and town officials, including senior management, as well as contractors, consultants or other parties with access to information technology resources or data are required to adhere to this policy.

Details

All devices on, or connecting to, Town of Arietta network must remain free of malware.

- Personnel will comply with safe computing practices as described in the "Acceptable Use Policy."
- Personnel will follow recommended processes to prevent malware attacks.
  - NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
  - Delete spam, chain, and other junk email without forwarding, in with Town of Arietta's *Acceptable Use Policy*.
  - Never download files from unknown or suspicious sources.
  - Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Personnel must NOT attempt to circumvent or disable anti-malware software without explicit, written permission from management.

Town of Arietta-owned Devices

- All devices must be configured, maintained and audited per the "Access Control Policy" and "Software Development, Maintenance and Auditing Policy."

- All devices running any version of the Microsoft Windows operating system must have anti-malware software installed and updated, per the "Anti-malware Standard."
- All devices connecting to the Internet must be protected by a firewall as defined in the "Perimeter Security Policy."

Non-town-owned Devices

- All devices must be reviewed and approved by management.

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Asset Management Policy

Purpose - To protect Town of Arietta assets through basic asset management, including inventory and ownership.

Roles and Responsibilities

IT Security Officer
Annually – The IT Security Officer will review the inventory to ensure that policies and procedures for each asset and asset type exist and are relevant.

All Employees
All Town of Arietta employees and town officials, including management, as well as contractors, consultants or other parties with access to information technology resources or data are required to adhere to this policy.

Details

- An inventory of all Town of Arietta information assets will be maintained by IT management.
- An owner will be assigned to each information asset indicated in the inventory. All computers, printers, scanners, etc. that are issued to employees or town officials are the sole property of the Town of Arietta and must be cared for in an appropriate manner. When a device is no longer needed, or the user is no longer an employee town official all devices must be returned with all its associated parts. Including but not limited to, power cords, mice, keyboards, interface cables, hard drives, external media, software, carrying cases, etc.
- When any asset is no longer of use to the town all data will be securely removed and the media destroyed in a manor that will prevent any data recovery. All electronic devices will be placed in the recycling stream in accordance with NYS DEC LAW ARTICLE 27 TITLE 26

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Audit Policy

Purpose - To provide reasonable assurance that:

- Assets are safeguarded.
- Information (financial and other) is timely and reliable.
- Errors and irregularities are discovered and corrected promptly.
- Operational efficiency is promoted.
- Compliance with managerial policies, laws, regulations, and sound fiduciary principles is encouraged.

Roles and Responsibilities

Audit Committee

- Analyze the extent of external auditing coverage needed by Town of Arietta annually.
    - At a minimum, annual audit activities will include:
        - User access
        - Handling of confidential information
        - Alignment of business objectives and IT solutions
        - Monitoring systems for transactions and processing
        - Audit trails
        - Business Continuity Plans
        - System outages
        - Segregation of duties
        - IT vendor oversight
        - Employee training

- Review the adequacy of the internal audit program, including review of the audit schedule.

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Business Continuity Policy

Purpose - To minimize the effect of unexpected disruptions to the business through a defined process of planning, testing, implementing and reporting.

Roles and Responsibilities

All Town of Arietta employees and town officials, including management, as well as contractors, consultants or other parties with access to information technology resources or data are required to adhere to this policy.

Management

- Will oversee development, implementation and testing of business continuity plan
- Annually – Management will review and prioritize each business function and unit, updating the business impact analysis as necessary.
- Annually – Management will review critical service provider business continuity plans for adequacy and compatibility with institution's business continuity plan

IT Security Officer

Annually – The IT Security Officer will review the BCP as part of the IT risk assessment.

Internal Audit

Annually – Internal Audit will review the BCP.

Details

- Business Impact Analysis (BIA) – this analysis should delineate all business functions across all lines of business, prioritize them in order of criticality, define the recovery time objective (RTO) per function, the recovery point objective (RPO) per function, dependencies and workarounds.
- Risk Assessment – along with the other components and objectives of the IT security risk assessment, potential disaster scenarios should be considered for business continuity planning purposes. These should not be limited to natural disasters but should also include items such as connectivity disruptions, equipment failure, utility failures, chemical spills, terrorism, pandemic influenza and more.

- Town of Arietta must test the BCP at least annually or more often, if significant changes occur.

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Vendor Notification Policy

Purpose – To protect Town of Arietta information resources and employee data.

Roles and Responsibilities

All Town of Arietta employees and town officials, including management, as well as contractors, consultants or other parties with access to information technology resources or data are required to adhere to this policy.

Management

- Will include a notification clause in all vendor contracts that involve information resources to notify Town of Arietta in the event of sensitive data disclosure, as described in the "Definitions" section below.

IT Security Officer

Annually – The IT Security Officer will review the Vendor Notification Policy as part of the IT risk assessment.

Details

- Town of Arietta will notify the affected personnel or affected parties, assuming that misuse of said information has occurred or it is reasonably possible that it will occur.
- Notification will follow guidelines defined in Customer Notification Policy.

Definitions

Sensitive Data

> "For purposes of this guidance, sensitive customer information means a customer's name, address or telephone number in conjunction with the customer's Social Security number, driver's license number, policy number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. It also includes any combination of components of customer information that would allow someone to log on to or access the customer's account or policy, such as user name and password or password and account number."

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Customer Notification Policy

Purpose - Town of Arietta policy regarding customer notification in the case of disclosure.

Roles and Responsibilities

All Employees

All Town of Arietta employees and town officials, including management, as well as contractors, consultants or other parties with access to information technology resources or data are required to adhere to this policy.

Details

- In the event of sensitive data disclosure, as described in the "Definitions" section below, Town of Arietta will notify the affected customer(s), assuming that misuse of said information has occurred or it is reasonably possible that it will occur. This is in addition to the actions described in the incident response program.

- The customer notice will include:
  - An incident description
  - A description of the compromised data
  - Mitigation steps taken by the institution to prevent further unauthorized access.
  - Town of Arietta phone numbers for further information and assistance
  - A customer reminder to be "vigilant" for the next year to two years, and to report any identity theft issues to the institution.
  - Contact information for credit reporting agencies if a large number of customers is affected.

- Town of Arietta will, at its discretion, notify customers by whatever method, or combination of methods, is most likely to ensure the receipt of the notice, whether by mail, telephone, or e-mail.

- The format of the notice is contained in the "References" section. The notice will be tailored to fit the actual incident that has occurred and will be as descriptive as possible.

Definitions

Sensitive Data

"For purposes of this guidance, sensitive customer information means a customer's name, address or telephone number in conjunction with the customer's Social Security number, driver's license number, policy number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. It also includes any combination of components of customer information that would allow someone to log on to or access the customer's account or policy, such as user name and password or password and account number."

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

References

Customer Incident Notification Letter

RE: Notice Regarding Unauthorized Access to Customer Information

Dear _____,

Town of Arietta believes in acting quickly in our customers' best interest. Thus, please be advised of a recent incident involving unauthorized access to certain customers' personal identifying information. (describe the incident in general terms)

Please do not hesitate to contact Town of Arietta at (518)548-3415, the main office number, for assistance and/or information about how to minimize the potential effect this incident could have on you, our valued customer. You may wish to visit the Federal Trade Commission's (FTC) web site address and toll-free number to obtain identity theft guidance and to report suspected incidents of identity theft:
www.consumer.gov/idtheft/; 1-877-IDTHEFT is the FTC's toll-free ID Theft Hotline.

Trained staff is here to assist you in:
1) Correcting and/or updating information in any consumer report that ties back to this incident; or

2) Placing a fraud alert in your consumer reports, as required by the Fair Credit Reporting Act. Under this Act, you have the right to obtain a credit report free of charge if you have reason to believe that the file at the consumer-reporting agency contains inaccurate information due to fraud. Subscription services are available that can provide notification to you anytime there is a request for your credit report, which the town can assist you in subscribing to, free of charge, for a period of time. We also offer the following recommendations:

1. Contact each nationwide credit-reporting agency (see attached addresses) is advised in order to place a "fraud alert" on your consumer reports.

2. Periodic credit reports are advised from each nationwide credit-reporting agency in order to have information relating to fraudulent transactions deleted.

Because of the unfortunate incident disclosed today, we want to remind you to remain vigilant over the next twelve to twenty-four months, carefully examining all credit card billings and other such statements to verify charges. If anything looks suspicious, promptly report the incident as suspected identity theft.

Again, we want to assure you that Town of Arietta is here, at your convenience, acting in your best interest.

Sincerely,

Enclosure: A brochure regarding steps you can take to protect against identity theft.
Enclosure: Credit Bureau Information

Data Backup and Recovery Policy

Purpose - To describe Town of Arietta expectations regarding critical data backup and recovery.

Roles and Responsibilities

IT Security Officer
Quarterly – The IT Security Officer will review backup results.

IT Staff
Annually – IT Staff will select a random file and test that a restore successfully completes. Results will be included in BCP/DR test results.

All Employees
All Town of Arietta employees and town officials, including management, as well as contractors, consultants or other parties with access to information technology resources or data are required to adhere to this policy.

Details

Regular backup and recovery processes help ensure the ongoing stability of Town of Arietta operations.

Whether backups are performed by Town of Arietta personnel using town equipment, or some or all of the process is outsourced, the town will:

- Regularly back up all critical data as indicated in the Business Impact Analysis, risk assessment, and Disaster Recovery Plan.
- Town of Arietta will develop and maintain accurate backup and restore procedures for all critical assets.
- Periodically (but regularly) restore data to validate backup methodology
- Backups will be stored offsite
- Ensure the security of backup data in storage or transit, whether by encrypting backup tapes or encrypting data as it passes over non-town network links.
- In the event a third-party backup vendor is retained, ensure contracts with third parties require the return of all Town of Arietta data in the event of contract termination, as well as the secure deletion or wiping of any residual town data residing at the third-party location.

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Perimeter Security Policy

Purpose - To clarify management's expectations concerning perimeter security, including firewall technology and configuration, intrusion detection, web content filtering, etc.

Roles and Responsibilities

IT Security Officer

Annually or as changes occur:

- Will review firewall configuration as part of the IT risk assessment or if changes to the current configuration are requested.
- Will review intrusion detection or prevention technologies' configuration as part of the IT risk assessment or if changes to the current configuration are requested.
- Will review web content filtering configuration as part of the IT risk assessment or if changes to the current configuration are requested.

All Employees

All Town of Arietta employees and town officials, including management, as well as contractors, consultants or other parties with access to information technology resources or data are required to adhere to this policy.

Details

Firewall

- A firewall will separate networks under Town of Arietta control from networks not under the town's control with a default policy that denies all traffic.
- NAT will be used to abstract networks under the town's control from networks not under the town's control.
- Any Town of Arietta computing assets exposed to traffic initiated from the Internet, unless restricted by the firewall rules to the IP range(s) of a contracted service provider, must be on a DMZ network connected through the firewall. Access from any DMZ networks to the internal network must be filtered through the firewall.
- All firewall traffic must be monitored for misuse or attacks, and the town's incident response plan implemented if necessary.
- Firewall management, including firewall policy changes, patching or updates, may be outsourced to an appropriate service provider.
- Firewall management will only occur using secure management protocols such as SSH or SSL.
- Firewall policy or rule changes will only occur after written approval from the IT Security Officer.

Intrusion Detection

- A layer of intrusion detection, if not intrusion prevention, technologies will separate networks under the town's control from the Internet with a default policy that examines all traffic.

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Insurance Policy

Purpose - To communicate Town of Arietta management's intent regarding using insurance to mitigate information security risk.

Roles and Responsibilities

All Employees

All Town of Arietta employees and town officials, including senior management, as well as contractors, consultants or other parties with access to information technology resources or data are required to adhere to this policy.

Details

Town of Arietta will regularly review insurance options for information security concerns. The IT Security Officer will interact with management as necessary to ensure insurance coverage is adequate, relevant and that insurance requirements are met by the town.

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Password Construction Policy

Purpose - To provide best practices for the creation of strong passwords.

Roles and Responsibilities

All Employees
All Town of Arietta employees and town officials, including senior management, as well as contractors, consultants or other parties with access to information technology resources or data are required to adhere to this policy.

Details

Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of 14 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include "*It's time for vacation*" or "*block-curious-sunny-leaves*". Passphrases are both easy to remember and type, yet meet the strength requirements. Poor, or weak, passwords have the following characteristics:

- Contain eight characters or less.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Are some version of "Welcome123" "Password123" "Changeme123"

In addition, every work account should have a different, unique password. To enable users to maintain multiple passwords, we highly encourage the use of 'password manager' software that is authorized and provided by the organization. Whenever possible, also enable the use of multi-factor authentication.

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Clean Desk Policy

Purpose - To ensure sensitive data, is appropriately secured, whether it is being handled, transmitted, stored, or disposed of.

Roles and Responsibilities

Senior Management

Weekly –Supervisor will perform a walkaround of the office to ensure that confidential, sensitive data is secure and that employees and town officials are adhering to the clean desk policy as described below.

All Employees

All Town of Arietta employees and town officials, including senior management, as well as contractors, consultants or other parties with access to information technology resources, data, files, or documents are required to adhere to this policy.

Details

All Town of Arietta work areas are to be kept clear of documents, files, folders and notes that may contain sensitive data.

- All work areas are to be kept free of sensitive or confidential information. All files and papers not needed for tasks currently active are to be covered or placed in a drawer.
- At the end of each business day all files should be placed in a secure location and desks should be cleared of all documents and files and notes.
- File cabinets containing Restricted or Sensitive information must be kept closed when not in use or when not attended.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Personnel Security Policy

Purpose - To ensure risks posed by employees and town officials are mitigated.

Roles and Responsibilities

IT Security Officer
Annually – The IT Security Officer will perform information security awareness for all employees and town officials.

All Employees
All Town of Arietta employees and town officials, including management, as well as contractors, consultants or other parties with access to information technology resources or data are required to adhere to this policy.

Details

All employees and town officials must sign agreements covering confidentiality, non-disclosure and acceptable use.

Town of Arietta must regularly train employees and town officials on their security roles and responsibilities, including increasing overall security awareness and compliance with relevant policies and procedures.

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Remote Access Policy

Purpose - To define minimum expectations and acceptable methods for remote access to Town of Arietta information assets.

Roles and Responsibilities

IT Security Officer

- Annually – The IT Security Officer will review remote access controls and authorized users as part of the IT risk assessment.

All Employees

All Town of Arietta employees and town officials, including senior management, as well as contractors, consultants or other parties with access to information technology resources or data are required to adhere to this policy.

Details

Remote access must be provided to support a clear business purpose. In specific, remote access has the following requirements:

- Requires IT Security Officer approval.
- Approvals must be reviewed by the IT Security Officer annually or sooner, per the "Access Control Policy."
- Occurs via VPN through Town of Arietta firewall, unless specific modem access to designated devices by a support vendor is required.
- VPN authentication requires, at a minimum, a shared secret (or pre-shared key) as well as a username and password. A group name and password are also acceptable instead of a shared secret.
- Authentication information must be encrypted.
- Remote access must be logged and regularly reviewed.
- Remote access via modem for support vendors must remain disabled via unplugging the modem until needed.

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

IT Risk Assessment Policy

Purpose - The risk assessment program is a foundational element of Town of Arietta overall security program and is the primary instrument for assessing and addressing information security risks. This policy describes the town's intent and requirements regarding the risk assessment and remediation processes included in its risk assessment program.

Roles and Responsibilities

IT Security Officer

- Annually – The IT Security Officer will manage or oversee the risk assessment process.

Senior Management

- Determine and communicate clear lines of responsibility for risk management decisions.
- Define risk measurement definitions and criteria.
- Establish acceptable levels of risk.
- Oversee risk mitigation activities.

Details

Per best practices and regulatory guidelines, Town of Arietta will maintain a *risk assessment program* that is:

1. Based on a formal framework

2. Considers:
   - Analysis of internal/external threats to confidential customer and consumer information
   - Spyware and other malware
   - Internet-based and e-mail-based fraud
   - Pharming attacks
   - Identity theft
   - Voice-over-IP (VoIP)
   - Disaster recovery and business continuity planning, including pandemic influenza planning
   - Imaging systems
   - General operational environment
   - Service provider monitoring
   - Any other business processes or assets that management deems relevant

   - ***Risk Identification***— Risk is the potential that events, expected or unanticipated, may adversely affect the institution's earnings, capital, or reputation. Risk identification should produce groupings of threats, including significant cybersecurity threats.

- ***Risk Measurement***— Management could use a taxonomy for security-related events to help accomplish the following:
    - Map threats and vulnerabilities.
    - Incorporate legal and regulatory requirements.
    - Improve consistency in risk measurement.
    - Highlight potential areas for mitigation.
    - Select proper controls to cover various attack stages, channels, and assets.
    - Allow comparisons among different threats, events, and potential mitigating controls.
- ***Risk Mitigation***— Management should develop and implement an appropriate plan to mitigate those risks. This plan should include an understanding of the extent and quality of the current control environment. When conducting an evaluation of the strength of controls, or the ability to mitigate risk, the institution should consider the system of controls rather than any discrete control.

The organization's *risk assessment* will include the following steps:

- **Information Gathering**
- **Asset Identification**
- **Information Analysis**
    - **Asset Ranking and Classification**
    - **Threats and Vulnerabilities Assessment (including probability and impact)**
    - **Control Effectiveness Evaluation**
- **Risk Rating Assignment**
- **Remediation Plan Creation**

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Sensitive Data Handling Policy

Purpose - To ensure sensitive data, is appropriately secured, whether it is being handled, transmitted, stored, or disposed of.

Roles and Responsibilities

IT Security Officer
Annually – The IT Security Officer will review the controls surrounding sensitive data as part of the IT risk assessment.

All Employees
All Town of Arietta employees and town officials, including senior management, as well as contractors, consultants or other parties with access to information technology resources or data are required to adhere to this policy.

Details

All Town of Arietta devices are assumed to handle, transmit or store sensitive data. Thus, the town is not defining a formal data sensitivity classification scheme.

- All non-mobile Town of Arietta devices are kept physically secure on the town's premise per the "Physical Security Policy."
- All mobile Town of Arietta devices must be configured with a username and password to prevent unauthorized access, as well as employing a limited number of login attempts before locking or data destruction, if possible.
- Sensitive data contained on any medium, including paper, must not be left unattended anywhere and must be shredded when no longer needed.
- Computing devices and components must be disposed of properly, including those devices such as photocopiers, Fax Machines, and Printers, which will have the hard drives removed and destroyed prior to disposal. The preferred method of disposal will be to destroy the platters. In addition, all CDs, DVDs, flash memory, etc. will be destroyed. Hardware assets will not be disposed of without management notification and consent. Logs of said disposal must be maintained, stating:
    - what was destroyed
    - when
    - by whom
    - who approved the destruction
- Sensitive data should never be sent outside of Town of Arietta network without being encrypted and secured with additional controls, such as passwords, to prevent viewing by unauthorized parties. The IT Security Officer should approve all processes, in writing, that transmit sensitive data outside of the town.

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Software Development, Acquisition and Maintenance Policy

Purpose - To ensure all software in Town of Arietta computing environment meets security requirements.

Roles and Responsibilities

All Employees
All Town of Arietta employees and town officials, including senior management, as well as contractors, consultants or other parties with access to information technology resources or data are required to adhere to this policy.

Details

- All Town of Arietta software should be acquired, installed and maintained (including patching) according to town standards, as determined by management, and the IT Security Officer. No software is developed by the town itself.
- All non-standard software must be approved in writing by the IT Security Officer.
- Unnecessary functionality, modules, services, etc., will be disabled if not needed for business purposes.
- All software will be configured with relevant auditing enabled, as determined by the IT Security Officer. The auditing should be configured to track, if possible:
    - Who
    - What
    - When
- Auditing should be configured to log to a central location, if possible, preferably using SYSLOG.

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Wireless Policy

Purpose - To communicate Town of Arietta expectations regarding wireless usage.

Roles and Responsibilities

IT Security Officer
Quarterly – The IT Security Officer will assess Town of Arietta environment for the presence of wireless activity and conformance with this policy as part of the IT risk assessment process.

All Employees
All Town of Arietta employees and town officials, including management, as well as contractors, consultants or other parties with access to information technology resources or data are required to adhere to this policy.

Details

- All wireless devices must be approved by the IT Security Officer before connection to the networks.
- Wireless access provided will be on a secure connection.
- No personal wireless devices are allowed on Town of Arietta's internal network.
- A separate wireless guest network is available when internet access is required for vendors and maintenance.
- Town of Arietta employees may not use the wireless guest network except during breaks.
- Town of Arietta employees must register any wireless devices with the IT department.

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.

Scheduled Reviews

Purpose – Calendar for annual reviews

Roles and Responsibilities

IT Security Officer
Monthly – The IT Security Officer will schedule reviews and updates in accordance with all IT policies..

All Employees
All Town of Arietta employees and town officials, including management, as well as contractors, consultants or other parties with access to information technology resources or data are required to adhere to this policy.

Details

- January – Acceptable Use, Access Control and Social Engineering
- February – Asset Management, Clean Desk and Audit
- March – Business Continuity, Customer Notification and Vendor Notification
- April – Perimeter Security and Insurance
- May – Password, Personnel Security, and Remote Access
- June – It Risk Assessment, Software and Sensitive Data Handling

Quarterly – Anti Malware – Patch Management – Backup review -- Wireless

Enforcement

Failure to comply with this policy could result in actions up to, and including, termination and legal action.