Town of Corning
Computer and Internet Use Policy

1. PURPOSE

The Town of Corning's (the "Town") has adopted this policy to provide all town employees, including elected town officials, for using the Town's computers, networks, internet services, and email services.

II. SCOPE

This policy is the standard that applies to all regular and temporary, part-time, and full-time employees, consultants, vendors, interns, volunteers, elected officials or others authorized to use the Town of Corning computer systems.

III. PRIVACY

The Town of Corning respects the individual privacy of its employees; however, to the extent permissible by law employee privacy does not extend to the employee's work-related conduct or to the use of Town operated equipment or supplies. Employees are to understand that personal messages or files have no guarantee or expectation of privacy since such messages or files are commingled with all other messages or files on our system and are subject to the same legal and regulatory exposure, internal review, and monitoring. It is further understood that there is no expectation of privacy for employees who use their personal email for Town business.

The Town retains control, custody, and supervision of all computers, networks, internet services, and email services. Employees waive and have no expectation to privacy in their use. The Town reserves the right to at any time to inspect and/or monitor computer system files, logs, and other activity including e-mails stored on any Town server or Town's computer.

Commented [SS1]: Do we store data in the cloud?

Commented [TS2R1]: @Stuart Sammis we have a server backup and microsoft one drive account for data storage. So yes.

IV. TOWN PROPERTY

The Town computers, networks, internet, and email services, and all associated hardware and software are the property of the Town of Corning. Additionally, all documents composed and messages and attachments composed, sent, received, or stored on Town computers, networks, internet services, and email services are and remain the property of the Town.

V. SECURITY

The Town of Corning employs various measures to protect its equipment and data from deliberate or inadvertent destruction or misuse. Such measures include the designation of individual accounts, log-ins, and passwords. Sharing of accounts, log-ins and passwords is prohibited unless the system administrator or department head grants an exception. Passwords shall be safeguarded and not divulged. If it is necessary to maintain a written copy of a password, that copy shall be placed in a secure location. When employees are required to choose a password, they should refrain from selecting a password that may be easily linked to the

employee such as birth dates, children's names etc. Passwords should be at least 12-14 characters long and include a combination of both letters (capitalized and non-capitalized) and numbers.

VI. PERSONAL USE

Minimal personal use of the Town's computers, networks, internet services and e-mail services is permitted so long as such use does not interfere with the employee's job duties and performance, with system operations, or other system users. This also includes personal use of the internet/social networks using one's personal cell phone or other electronic device while on Town time. For the purposes of this policy, anything beyond ten (10) minutes per day is presumptively excessive. Such personal use must be consistent with appropriate professional conduct. Employees are reminded that all personal use must comply with this policy as well as all other procedures, regulations, and laws. Employees are further reminded that all use may be monitored and inspected.

Employees shall not install, or attempt to install, whether for personal or Town use, on any Town computer or system, any software or shareware downloaded from the internet, without first consulting with the Town's outside computer administrator and receiving approval from their respective Department Head.

VII. INTERNET and WEBSITES

Internet access is provided primarily for research in connection with an employee's specific job duties. Employees are reminded that use of the internet must not interfere with an employee's job duties. Without the approval of a department head, general web browsing is considered an unproductive use of the resource and an employee's time. Any unproductive use of the internet by an employee is strictly prohibited. Only software approved by the Town's system administrator may be used to browse internet websites. Employees are encouraged to exercise care in selecting websites to visit on the internet, including sites received in, or linked from, email. Viruses can be transmitted simply by viewing a site that contains computer code written to transmit viruses to others. Employees shall not use streaming media applications without requesting and receiving permission from the system administrator or department head. Permission may only be granted on a limited basis for limited durations.

VIII. INAPPROPRIATE USE

Employees are prohibited from using the Town's computer, network, internet services, and email services in violation of the further terms of this policy, or in any way that reasonably could be viewed as inappropriate, malicious, obscene, threatening, or intimidating, that disparages coworkers, constituents, suppliers, or contractors or that might constitute harassment or bullying. Examples of such prohibited conduct include, but are not limited to:

- Profane or vulgar language
- Any use that is illegal
- Any use involving materials that are obscene or sexually explicit
- Any comments that may be construed as discriminatory
- Unauthorized mass electronic mailings or chain letters
- Use of systems for political campaigns, endorsements, or any other political activity

- Solicitation of funds for commercial, personal, or religious causes not sponsored by the Town
- Use of streaming websites (internet radio and video)
- Use of Peer-to-Peer sharing websites (downloading and sharing music/video files)
- Installing unauthorized software applications
- Installing any networking, hardware, networking software or hacker tools, or modifying Town hardware, software or data without proper authorization
- Opening any email attachment from any spam account or entity without confirming their identity
- Posting or sending offensive remarks meant to intentionally harm someone's reputation
- Behavior that could contribute to a hostile work environment on the basis of race, sex, disability, religion, sexual orientation, or anything else prohibited by the law or Town's Non-Harassment, Discrimination, and Retaliation Policy
- Disseminating Town records without a proper business reason for doing so, or in violation of law or Town Policy
- Accessing another employee's account or files without proper authorization, or permitting another employee to access your account or files without proper authorization

IX. PROTECTION OF STORED DATA

Protecting sensitive information stored or handled by the municipality and its employees is essential for the Town of Corning. All sensitive information must be stored securely and disposed of in a secure manner when no longer needed for business reasons. Any media (i.e. CD's, paper, USB's, computer hard drives etc.) that contain sensitive information must be protected against unauthorized access. Media no longer needed must be destroyed in such a manner to render sensitive data irrecoverable (i.e. shredding, disassembly, degaussing etc.).

Credit Card Information Handling Specifics

- Destroy cardholder information in a secure method when no longer needed. Media containing card information must be destroyed by shredding or other means of physical destruction that would render the data irrecoverable (shred, degauss, etc.).
- It is prohibited to store the contents of the credit card magnetic strip (track data) on any media whatsoever.
- It is prohibited to store the card-validation code (3- or 4-digit value printed on the signature panel of the card) on any media whatsoever.
- All but the last 4 numbers of the credit card account number must be masked (i.e. x's or *'s when the number is displayed electronically or on paper.

Protection of Data in Transit

If sensitive information needs to be transported physically or electronically, it must be protected while in transit (i.e. secure storage handling bags that are locked/protected).

Credit card account numbers must never be emailed without using proper encryption technology.

Media containing credit card account numbers must be secured as noted above and only transported to off-site locations by approved personnel in completing their essential job duties (i.e. Town Supervisor, Deputy Town Supervisor, Town Clerk etc.)

Restriction of Data Access

Any sensitive information (i.e. business data and personal information) will be restricted to employees that have a need-to-know pertaining to their specific job function requiring access. Credit card account number access shall be limited to employees that have a specific job function requiring access.

Physical Security

Physical access to sensitive information or systems that house that information shall be restricted (i.e. filing cabinets, computers with secured passwords, locked offices etc.) to protect this information from those who do not have a direct need to access it. Media is defined as any printed or handwritten paper, faxes, USB, computer hard drives etc.

- Media containing sensitive information must be securely handled and distributed.
- Media containing stored sensitive information (especially credit card account numbers and social security numbers) should be properly inventoried and disposed of when no longer needed for business by deleting, shredding, degaussing before disposal.
- Visitors should always be escorted and easily identifiable when in areas that may contain sensitive information.
- Password protected screen savers should always be used on any computers that may contain sensitive information.

X. SECURITY MANAGEMENT/INCIDENT RESPONSE PLAN

The Town Supervisor will act as the designated Security Officer. The Security Officer is responsible for communicating security policies to employees and contractors and tracking the adherence to policies. The Security Officer will notify the affected individuals and companies of any breach and follow the Cybersecurity Notification Policy of the Town of Corning.

Incidence Response Plan:

1. If a compromise is suspected, alert the information security officer, Jenniffer L. Mullen 607-425-5534.
2. The security officer will conduct an initial investigation of the suspected compromise.
3. If compromise of information is confirmed, the security officer will alert the Town Board and begin informing parties that may be affected by the compromise per the Cybersecurity Notification Policy of the Town of Corning.
    - Contain and limit the extent of the exposure by shutting down any systems or processes involved in the compromise.
    - Alert necessary parties (Chemung Canal, Visa/Mastercard Fraud Control, law enforcement etc.)
    - Provide compromised or potentially compromised card numbers to Visa/Mastercard Fraud Control within 24 hours.

XI. SECURITY AWARENESS

Keeping sensitive information secure requires annual and periodic training. The Town of Corning will review policies annually with employees and have written documentation in each employee's file of training received.

- Employees are required to read this security policy and attend annual training on the policies. The employee will sign an acknowledgement form that this training was received, and this form will be placed in the employee file.
- Municipal security policies must be reviewed annually and updated as needed.

COPYRIGHT

It is the policy of the Town of Corning to fully comply with all laws pertaining to the reproduction, use, or distribution of copyrighted or otherwise protected materials. The Town will comply with all licensing requirements. Employees shall not install, or attempt to install, any software on any computer or system unless the Town is properly licensed and approval is obtained from the Town's administrator. Employees shall not make copies of software other than those copies authorized by the software license.

X. VIOLATIONS

Any employee violating this policy will be subject to discipline up to and including termination of employment pursuant to applicable disciplinary standards and procedures established by law and/or collective bargaining agreements.