2021

VILLAGE OF WARWICK CYBER SECURITY GUIDE & POLICIES

Adopted & Effective: October 4, 2021

Version 9.17.2021

Table of Contents

Introduction

Local Governments have the responsibility to maintain documents from cradle to grave (birth certificates to death certificates) making them a desirable and vulnerable target for Identity Theft. Every Subscriber is dependent on information technology to run their municipality. Even small municipalities with limited information technology generate, store and maintain data. Losing or compromising this data can have serious ramifications for your municipality.

In order to comply with the notification requirements imposed by NYS Technology Law -208-; the Village of Warwick is required to have a breach notification policy in place to specify procedures to be taken in the event of an unauthorized access of private information- which has compromised the security, confidentiality or integrity of that information.

In order to create the most comprehensive guide, NYMIR included a checklist encompassing recommendations from the NYS Comptroller's office along with NYMIR's risk management team. NYMIR's goal is to help our members have the best form of protection in place to avoid security incidents. This guidebook provides suggested controls, policies, assessments, reporting forms and other resources.

Village of Warwick Internet and Acceptable Use Policy

Introduction:
The Village of Warwick's Acceptable Use Policy specifies policies and procedures for the use of information resources and information technology systems. Enforcement of this Acceptable Use Policy is consistent with the policies and procedures of this municipality.

Being informed is a shared responsibility for all users of the Village of Warwick's information systems. Being informed means, for example:

- Knowing these acceptable use policies and other related rules and policies,
- Knowing how to protect your data and data that you are responsible for,
- Knowing how to use shared resources without damaging them,
- Knowing how to keep current with software updates,
- Knowing how to report a virus warning, a hoax, or other suspicious activity, and
- Participating in training.

Policy:

Compliance with this policy is mandatory for all officials, employees and contractors of this municipality. This policy applies to all Village of Warwick information, computer systems and data that are used for official Village of Warwick business regardless of location.

1. *Authorized Use*

   Users must not use other users' passwords, user IDs, or accounts, or attempt to capture or guess other users' passwords. Users are also restricted from using business equipment for personal use, without authorization from your municipality. Users must not hide their identity for malicious purposes or assume the identity of another user.

2. *Privacy*

   User files may be subject to access by authorized employees of the Village of Warwick during the course of official business. Accordingly, users should have no expectation of privacy and their activity may be monitored.

3. *Restricted Access*

   Users must not attempt to access restricted files or portions of operating systems, security systems, or administrative systems to which they have not been given authorization. Accordingly, users must not access without authorization: electronic mail, data, programs, or information protected under state and federal laws. Users must not release another person's *restricted information*.

4. *Complex Passwords*

   Users are required to protect their computer using a complex password to greatly diminishes the ability of an attacker to compromise a system. A complex

password must include at least ten characters and be mixed-case such as numbers, upper and lower case, and symbols.

Village of Warwick Passwords Complex Password Requirements:

- at least ten characters long
- at least 1 uppercase letter
- at least 1 lowercase letter
- at least 1 number
- at least 1 symbol (!,@,#,$, etc.)
- combinations that do not spell a word or proper name as malicious actors
- no personal information –such as your name, children's name, birthdates

5. *Proper Use of Resources*

Users should recognize that computing resources are limited and user activities may have an impact on the entire network. They must not:

● misuse email – spread email widely (chain letter) and without good purpose ("spamming") or flood an individual, group, or system with numerous or large email messages ("bombing").

● use streaming audio, video or real-time applications such as: stock ticker, weather monitoring or Internet radio.

6. *Protecting Information and Shared Resources*

Users must:

● Follow established procedures for protecting files; including managing passwords, using *encryption* technology, and storing back-up copies of files.

● Protect the physical and electronic integrity of equipment, networks, software, and accounts on any equipment that is used for Village of Warwick's business in any location.

● Not visit non-business related websites.

● Not open email from unknown senders or email that seems suspicious.

● Not knowingly introduce worms, viruses or other malicious code into the system; nor disable protective measures (i.e.: antivirus, spyware fire-walls).

● Not install unauthorized software.

● Not send restricted or confidential data over the Internet or off your *locally managed network* unless appropriately encrypted.

● Not connect unauthorized equipment or media, which includes but is not limited to: laptops, thumb drives, removable drives, wireless access points, pdas, and mp3 players.

● Not use organization passwords on any other account that is not controlled by the Village of Warwick.

7. *Reporting Suspicious Activity/Emails*

a. Users must immediately report suspicious emails or suspicious activity directly to the Village of Warwick Contracted IT Professional & the Village of Warwick

Cyber Incident Response Manager using the Village of Warwick Cyber Incident Response Form. *See Cyber Incident Response Policy.*

Village of Warwick Contracted IT Professional: TCG Solutions
Report Suspicious Activity/Emails to: helpdesk@thecomputerguy.pro

Village of Warwick Cyber Incident Response Manager: Village Clerk
Email: clerk@villageofwarwick.org

8. *Civility*

   Users must not harass other users using computer resources or make repeated unwelcome contacts with other users. Users must not display material that is inappropriate in an office environment for example, consistent with the Village of Warwick's policies.

9. *Applicable Laws*

   Users must obey local, state, and federal laws including laws on copyright and other intellectual property laws.

Village of Warwick Internet Access and Acceptable Usage Policy

(For Confidential Information)

1. Authorization

Village of Warwick employees requesting access to the Village of Warwick's internet connection must complete an **Application for User Internet Access** (*see Appendix A*). Employees shall not access the Village of Warwick's internet connection without approval. Authorization for internet access will be determined by the Cyber Incident Response Manager. Name of Cyber Incident Response Manager: Village Clerk

2. Training

After receiving approval to use the Village of Warwick's internet connection, training will be provided. Contact the Village Clerk to register or receive additional training information.

3. Security

A unique IP address is assigned to each authorized user. The unique address does not guarantee privacy rights to the user. Downloading internet data is allowed only with prior written approval from the PC/LAN Administrator. Users who need to download information should write, "requesting download privileges", on their application.

Users should be aware of the risk of proper file storage procedures and of receiving computer viruses. Up-to-date virus scanning software must be running while the user downloads information.

Employee information inquiries (i.e. references, employee verification, etc.) are not permitted via the Internet.

4. Monitoring Usage

Employee internet use may be monitored through mechanical safeguards or direct observations. Each user must use discretion when using the internet. The authorizing manager may request a user to maintain the Internet Activity Log.

5. Policy Compliance

All employees including Department/Division Directors shall comply with this policy. The policy will be reviewed in six months for applicability.

6. Policy Exception

Policy exceptions shall be brought to the Director's attention for review. Exceptions may result in the withdrawal of the user's authorized Internet use.

Village of Warwick Security of Information – Policy Statement

Introduction

The Village of Warwick recognizes the importance of securing various types of information in order to reduce the risk of identity theft and fraud. The Village of Warwick is required to protect and secure various types of information as defined in the Federal Trade Commission Identity Theft Act Red Flag Legislation ("FTC Act"), the Criminal Justice Information Services Security Policy and through contractual obligations related to merchant services (credit card acceptance). Under state statute, the Village of Warwick also has an obligation to secure and limit access to other private information involving customers and employees.

Definitions

Sensitive Information

Sensitive information includes the following items, as well as any other information that may be included in the State Act or the FTC Act:

- Social Security Information
- Tax ID Information
- Credit Card Information
- Bank Account Information
- Driver's License Information
- Criminal Justice Information
- Health Information

Private Information

Private information includes employee, residents, vendors, and customers information that is protected by state statute or other regulatory agencies. This may include, but is not limited to addresses, phone numbers and other personnel file contents.

Policy

The Village of Warwick will adhere to all applicable requirements regarding the protection of sensitive information as stated in the FTC Act, Criminal Justice Information Services Security Policy and merchant services agreements. As a part of these efforts, the Village of Warwick will do the following:

- Develop and maintain standard procedure(s) to provide guidance on the protection of sensitive information in order to reduce fraud and identity theft.
- Develop and maintain a formal breach response plan.
- Develop and maintain a training program in order to effectively communicate information provided in the standard procedure(s) and breach response plan to necessary staff.
- Review and update (as needed) all procedures, plans and training programs on an annual basis (at a minimum).

- Ensure service providers, who are in contact with sensitive information, are aware of security requirements as well as the need for confidentiality, through proper contractual agreements and arrangements.

The Village of Warwick will also adhere to all applicable requirements regarding the protection of private information as stated in State and Federal guidelines and will provide proper security and confidential treatment of this information, while still adhering to all public record requirements. Efforts may include special contractual language to ensure service providers are aware of statutory requirements and the need for confidentiality.

Program for the Security of Sensitive Information

The procedures surrounding the program for the security of sensitive information shall include:

- Identification and definition of risk factors regarding customer accounts and all other systems that include the management, storage and handling of sensitive information.
- Measures to adequately detect these risk factors on a timely basis and in an efficient manner.
- A detailed breach response plan to respond appropriately when detection occurs in order to prevent and/or mitigate identity theft.
- Methods for reviewing and testing the program on an annual basis, including the communication of information to appropriate personnel and the testing of the incident response plan.

Detailed procedures related to this program will be approved by the Village Board or Contracted IT Professional through the Village of Warwick's standard procedure process.

New York State Technology Law § 208. Notification; person without valid authorization has acquired private information:

1. As used in this section, the following terms shall have the following meanings:

(a) "Private information" shall mean personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

(1) social security number;

(2) driver's license number or non-driver identification card number; or

(3) account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

(4) Biometric information

(5)email addresses and corresponding passwords or security questions and answers

(6) Financial account number without a required security code if an unauthorized person

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(b) "Breach of the security of the system" shall mean access or unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by a state entity. Good faith acquisition of personal information by an employee or agent of a state entity for the purposes of the agency is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure. Breach notification is not required for inadvertent disclosures of private information that are not likely to result in misuse of information; if the following is done;(a) employer must document its determination that the inadvertent disclosure is not likely to result in misuse, and (b) maintain that documentation for five years. Moreover, if the incident were to involve the private information of more than 500 New York residents, the employer is required to submit documentation to the state's attorney general within 10 days of that determination.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such state entity may consider the following factors, among others:

(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

(2) indications that the information has been downloaded or copied; or

(3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(c) "State entity" shall mean any state board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the state of New York, except:

(1) the judiciary; and

(2) all cities, counties, municipalities, villages, towns, and other local agencies.

(d) "Consumer reporting agency" shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to state entities required to make a notification under subdivision two of this section.

2. Any state entity that owns or licenses computerized data that includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The state entity shall consult with the state office of information technology services to determine the scope of the breach and restoration measures.

3. Any state entity that maintains computerized data that includes private information which such agency does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

4. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:

(a) written notice;

(b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the state entity who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction;

(c) telephone notification provided that a log of each such notification is kept by the state entity who notifies affected persons; or

(d) Substitute notice, if a state entity demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) e-mail notice when such state entity has an e-mail address for the subject persons;

(2) conspicuous posting of the notice on such state entity's web site page, if such agency maintains one; and

(3) notification to major statewide media.

6. Regardless of the method by which notice is provided, such notice shall include contact information for the state entity making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired or accessed by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired or accessed.

7. (a) In the event that any New York residents are to be notified, the state entity shall notify the state attorney general, the department of state and the state office of information technology services as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

(b) In the event that more than five thousand New York residents are to be notified at one time, the state entity shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

8. Any entity listed in subparagraph two of paragraph (c) of subdivision one of this section shall adopt a notification policy no more than one hundred twenty days after the effective date of

this section. Such entity may develop a notification policy which is consistent with this section or alternatively shall adopt a local law which is consistent with this section.

Village of Warwick - Data Breach Notification Policy

New York State Technology Law 208

1. This policy is consistent with the State Technology Law, section 208, as added by Chapters 442 and 491 of the laws of 2005. This policy requires notification to impacted New York residents and non-residents. **The Village of Warwick** values the protection of private information of individuals. **The Village of Warwick** is required to notify an individual when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and this policy.

2. **The Village of Warwick**, after consulting with CISA (The Critical Infrastructure Security Agency) to determine the scope of the breach and restoration measures, shall notify an individual when it has been determined that there has been, or is reasonably believed to have been a compromise of private information through unauthorized disclosure.

3. A compromise of private information shall mean the unauthorized access or acquisition of unencrypted computerized data with private information.

4. If encrypted data is compromised along with the corresponding encryption key, the data shall be considered unencrypted and thus fall under the notification requirements.

5, Notification may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. In such case, notification will be delayed only as long as needed to determine that notification no longer compromises any investigation.

6. **The Village of Warwick** will notify the affected individual. Such notice shall be directly provided to the affected persons by one of the following methods:

Written notice;

- Electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by **Village of Warwick** who notifies affected persons in such form;
- Telephone notification provided that a log of each such notification is kept by the **Village of Warwick** who notifies affected persons; or
- Substitute notice, if the **Village of Warwick** demonstrates to the State Attorney General that the cost or providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the **Village of Warwick** does not have sufficient contact information.

Substitute notice shall consist of all the following:

A. E-mail notice when the **Village of Warwick** has an e-mail address for the subject persons.

B. conspicuous posting of the notice on the **Village of Warwick's** web site page, if Municipality X maintains one; and

C. notification to major statewide media

7. The **Village of Warwick** shall notify CISA as to the timing, content, and distribution of the notices and approximate number of affected persons.

8. The **Village of Warwick** shall notify the Attorney General and the Consumer Protection Board, whenever notification to a New York resident is necessary, as to the timing, content, and distribution of the notices and approximate number of affected persons.

9. Regardless of the method by which notice is provided, such notice shall include contact information for the **Village of Warwick** making the notification and a description of the categories of information that were or are reasonably believed to have been acquired or accessed by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired or accessed.

10. This Policy also applies to information maintained on behalf of the **Village of Warwick** by a third party.

11. When more than five thousand New York residents are to be notified at one time, then the **Village of Warwick** shall notify the consumer reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected individuals. This notice, however, will be made without delaying notice to the individuals.

Village of Warwick Cyber Incident Response Form

Reported by: _____

Name: _____
Phone: _____
E-mail: _____

Date & Time of incident detection:

Nature of Incident:

- ☐ Denial of Service
- ☐ Unauthorized Access
- ☐ Malicious Code (worm, virus)
- ☐ Website Defacement
- ☐ Scans and Probes
- ☐ Other (describe)

Incident Descriptions (What were the signs?):

Details (e.g. virus name, events, etc.):

Business Impact (e.g. what information or services are impacted?):

Course of Action:

Additional Notes:

Village of Warwick Cyber Incident Response Policy

This policy is established to clarify roles and responsibilities in the event of a cyber incident. The availability of cyber resources is critical to the operation of government. A swift and complete response to any incidents is necessary in order to maintain that availability and protect public and private information.

Responsible Elected Official:
If the incident affects multiple departments, the Mayor shall be the responsible Elected Official. If only one department is impacted, the Elected Official responsible for that department shall fill this role. The responsibilities of the elected official include, but are not limited to:

- Receiving initial notification and status reports from the Cyber Incident Response Manager.
- Consulting with other elected officials on public notification, involvement of the municipal attorney and notification of law enforcement.
- Preparing and delivering press releases.
- Consulting with other elected officials and appropriate staff on priorities for response and recovery.
- Advising the Incident Response Manager on priorities.

Incident Response Manager:
The Village Board of Trustees designates that the Village Clerk as the Cyber Incident Response Manager with the responsibility for preparing for and coordinating the response to a cyber incident. Responsibilities include, but are not limited to:

- Training users to recognize and report suspected incidents.
- Developing and testing response plans.
- Being the point of contact should any employee or official believe an incident has occurred.
- Involving the identified Technical Support to address the incident.
- Notifying the appropriate elected officials that an incident has occurred, if significant.
- Advising Elected Official(s) regarding notification of law enforcement and the Village of Warwick attorney if appropriate.
- Providing information to Elected Official(s) responsible for notifying the press and public.
- Coordinating the logging and documentation of the incident and response to it.
- Making recommendations to reduce exposure to the same or similar incidents.

Technical Support Staff:
The Village of Warwick shall provide Technical Support to the Incident Response Manager. Responsibilities include, but are not limited to:

- Assessing the situation and providing corrective recommendations to the Cyber Incident Response Manager.
- Helping the Cyber Incident Response Manager make initial response to incidents.

- Responding to the incident to contain and correct problems.
- Reporting to the Cyber Incident response Manager on actions taken and progress.
- Participating in review of the incident and development of recommendations to reduce future exposure.
- Consulting with other Elected Official(s) on public notification, involvement of the municipal attorney, and notification of law enforcement.
- Assisting with preparation of press releases.
- Consulting with other Elected Official(s) and appropriate staff on priorities for response and recovery.
- Advising the Cyber Incident Response Manager on priorities.

Legal Counsel:

The Village of Warwick attorney shall provide advice as called upon.

Cyber Security	NYMIR Online Training
Complying with HIPAA for Covered Entities	The goal of this course is to help individuals within your organization refresh their knowledge and comply with the HIPAA training requirements, including those contained in the recent ARRA HITECH act. The ARRA stimulus bill altered a covered entity's responsibilities and increased the liabilities for non-compliance. Employee training is required under the rule.
PCI Security Standards at the Point of Sale	To comply with PCI Data Security Standard audit requirements (Req. 12.6.1), organizations are required to offer PCI awareness training. Our family of PCI Security Standards courses will help you meet this need and educate employees on how to effectively safeguard and protect payment card information gathered at the point of sale (POS). The goal is to create informed employees who make better data protections decisions at the POS and, ultimately, lower your risk.
PCI Security Standards for IT and Back Office	To comply with PCI Data Security Standard audit requirements (Req. 12.6.1), organizations are required to offer PCI awareness training. Our family of PCI Security Standards courses will help you meet this need and educate employees on how to effectively safeguard and protect payment card information in the IT department and/or in the Back Office. The goal is to create informed IT and Back Office employees who make better data protections decisions and lower your risk.
PCI Security Standards for Managers	To comply with PCI Data Security Standard audit requirements (Req. 12.6.1), organizations are required to offer PCI awareness training. Our family of PCI Security Standards courses will help you meet this need and educate those who managers others on how to effectively safeguard and protect payment card information handled by their direct reports.
PCI Security Standards on the Phone and Online	To comply with PCI Data Security Standard audit requirements (Req. 12.6.1), organizations are required to offer PCI awareness training. Our family of PCI Security Standards courses will help you meet this need and educate employees on how to effectively safeguard and protect payment card information gathered over the phone and online. The goal is to create informed employees who make better data protections decisions and lower your risk.
Preventing Phishing	Are your employees still falling for phishing schemes? Phishing remains the single biggest threat to information security, and if your employees continue to take the bait, it's time you addressed the problem with training that directly targets the kinds of behaviors that need to change. This engaging course helps people identify the ways that scammers attempt to get into their system and it offers practical advice and practice on avoiding phishing attempts on all kinds of devices.

Privacy Awareness	With the rapid increase in online activity and information accessibility, customers, employees, and the Federal government have become more concerned about how personal information will be stored and used. This course provides an overview of basic privacy policies and procedures, including both Personally Identifiable Information (PII) and proprietary business information.
Records Management	This course teaches your employees how to identify and classify business records in order to effectively protect, manage, store, and dispose of them. By following the best practices identified in this training, your employees will know when to dispose of information and how to keep your current information timely, accurate, and usable.
Responsible Use of Social Media	Social networking sites such as Twitter, Facebook, and LinkedIn have become increasingly popular places to post opinions and network with colleagues online. However, one inappropriate post could bring a range of legal liabilities and unforeseen consequences for both employers and employees. An organization's success relies on all employees understanding these risks and acting with integrity and responsibility when using social media.
Security Awareness	This course can act as a foundational component of your security awareness program and help your employees understand how good data protection practices relate to their individual actions and behaviors. An integrated assessment tracks learner comprehension and understanding of key data protection concepts. Realistic examples are presented that add relevance and increase learner comprehension.
Security Awareness with Privacy Principles	This course uses a stimulating and creative approach that engages and challenges the learner. Realistic situations, knowledge checks, case studies, and examples are presented that add relevance and increase learner comprehension and retention. The goal: to create informed employees who make better decisions and lower risk. Good data protection practices will strengthen the consumer's trust in your organization and foster customer loyalty. Trust and loyalty are essential to maintaining lifetime, profitable customers.

Purpose:

Guidelines for Backing up Information

Introduction - As a municipal manager you are responsible for the confidentiality, integrity and availability of all documents in your care. Your municipality should have formal, routine backup procedures in place to ensure you have access to essential information in the event that your documents, files or even your computer systems are damaged, lost, stolen or otherwise unavailable. The importance of such procedures cannot be overstated. For it is virtually inevitable that at some point in time you will experience an incident that could affect the information in your care: your computer system may crash, for example, or your electronic documents could be lost or compromised.

This guide will assist you in developing and implementing a backup procedure in your municipality to help protect your information and minimize risks.

What Is a Backup? - A backup is a copy of electronic information that is maintained for use if there is loss or damage to the original. Backups can be compressed to save space and encrypted to add security.

Think about what information is stored on your systems, e.g. accounting records, email, correspondence, meeting minutes, etc. To avoid prolonged disruptions in your operations, all critical files, as well as any information your municipality cannot easily replace, need to be backed up.

Note: Archival storage is different than backup. Archival storage is the permanent maintenance of electronic information valuable to a municipality. Archival storage focuses on the storage of digital information that will no longer be changed, but must be maintained, uncorrupted and usable for a specified period of time.

Backup Process - There are four main components of a backup process to provide reasonable protection from loss. Several scenarios are provided below as examples of the importance of a backup process. The remainder of this document explains the backup process.

1. **Back up data at regular intervals.** What happened: A municipality backed up its data once a month, but occasionally less frequently. The municipality found the process of backing up tedious and assumed there would be little need to have the most up-to-date data always on hand. Unfortunately, its system crashed in the middle of tax season. The tax collector asked for a backup to the system and found the last system backup was before tax season, meaning that all the information on who had paid their taxes that year had been lost.

2. **Verify the data has been backed up.** What happened: A municipality carefully managed its assessment data for properties, constantly updating data and backing up the system to make sure their data would not be lost. To be safe, they produced daily

backups of the system and kept each backup for a week until it was replaced by a new one. Subsequently, a computer crash destroyed all their data. When they attempted to restore the data from their last backup, they discovered their backup tape was blank. Although they followed their backup procedures precisely, none of their data transferred onto the backup tapes and all their electronic data had been lost. It took the municipality a full month to recreate the data in the system.

3. **Store the backup media in a secure, safe place.** What happened: A municipality regularly produced backups of the voluminous records on its system. These included payroll and personnel records, among others. They assumed that the frequency of their backups would protect them from potential record loss. When their main administrative building was flooded, they discovered they were wrong. Although their backup data was stored separately from the computers, they were both stored in the same building, thus they were destroyed simultaneously.

4. **Verify the ability to restore**. What happened: A municipality was running two different network operating systems and used the same backup drives and backup software on both. Restores were regularly done back onto the same servers with no problems. When a server running one operating system crashed and its applications were to be moved to a server running the other operating system, it was discovered that the backup software could not restore onto a server with a different operating system. A temporary server with the same operating system had to be set up and the files transferred over the network. That backup software was replaced and cross operating system restores tested.

What to Back Up - Understanding potential risks and threats to your municipality can guide you in developing effective backup procedures to guard against those risks. The key question is "How much can your municipality afford to lose?". To determine the answer, the municipality needs to understand its flow of information and the cost of temporarily or permanently losing information.

In addition to the data used in day-to-day operations (such as financial systems), you should also consider long-term preservation of data that cannot be recreated (e.g., municipality's history or vital statistics records). This may include current files, such as those found on your desktop or server, or other files produced at various locations not linked to a centralized storage area. Software and application files and settings may also need backup to ensure a fast and efficient reinstall of your system.

Backup Media and Devices - Choosing the best media type for backups is dependent upon how much data the municipality needs to back up and how often. Any type of writeable media can be used as backup as well as any device that can be connected to a computer to copy information.

This may include tapes, CD-Rs, DVD-Rs, external hard drives, or similar devices. Each has its own advantages and disadvantages. The following are common types of backup media:

- **Tape**: Data is stored on magnetic tapes, similar to a cassette tape.
- **CD and DVD**: Data is stored similarly to music CDs or movie DVDs.
- **External Hard Drives:** An external device that uses removable drives similar to those inside your computer. These drives are portable and usually come with backup software.
- **Flash Drives:** A small device that plugs into your computer, also called thumb drives or memory sticks.
- **Online Backup**: Store files on a remote server, uploaded through an Internet connection, eliminating your need to manage tapes, disks or CDs.

Pros and Cons of Media Types

Type	Pro	Con
Tape	Inexpensive, Can be used repeatedly, Good for daily backups	Relatively Slow, Sensitive to Heat and magnetism
CD and DVD	Compact, Inexpensive, Portable	Sensitive to Heat, Unusable if Mishandled, Rapidly Evolving technology makes today's storage media outdated
External Hard Drive	Most Include backup software, Can be automated, Can be used to replace faulty drives	Expensive, Maintaining compatibility with your source systems, Sensitive to heat and magnetism
Flash Drives	Easily portable, Fast data transfer	Easy to lose, Can be expensive, Difficult to label, Sensitive to heat and magnetism
Online Backup	Easy Data Transfer, Can be automated	Expensive, Provider System can be compromised, Provider can go out of business, Reliant on provider Standards

Backup Process Steps

1. **Back Up Data at Regular Intervals**

Frequency and types of backups - It is important to develop a regular backup routine that reflects the frequency of change in data. If the computer is used daily, it is best practice to back up important files daily. At a minimum, back up all important current files at least once a week. To determine how frequently your municipality should back up, think about how much data the municipality can afford to lose. If it is a week's worth

of data, developing a weekly backup system would be sufficient. If it is a day's worth of data, a daily backup schedule would be necessary. Many municipalities collect data electronically; such as tax records, cash receipts, or client documents. This information may need to be backed up daily, as it may be impossible to recreate the data; thus the risk of loss is great. In general, it is recommended to replace all backup media every two to five years.

There are three types of backup schedules: Full, Incremental, and Differential. An example of these follows at the end of this section. Full backups copy every file on the system to a backup device. Many municipalities need to schedule full backups during non-operational hours to ensure no files are in use and the full backup can be completed. If possible, full daily backups should be done.

However, incremental or differential backups can be used when there is not enough time to do a full backup. They are frequent backups used to capture new or changed information. An incremental backup copies every file that has been created or changed, since the last backup of any type; while differential backup copies every file that has been created or changed since the last full backup.

The following examples demonstrate the difference between incremental and differential backups. Say a municipality does a full backup on Sunday night. Assume that file "A" is modified on Monday, file "B" is created on Tuesday and file "A" is modified again on Wednesday. These files are already on the Sunday full backup in their unmodified versions.

- If the municipality did incremental backups, then Monday's backup would contain "A" in its first modified form. Tuesday's Incremental backup would contain just "B." Wednesday's backup would contain only file "A," in its second modified form. On Thursday, when the hard drive fails, the municipality would recover the files from Sunday's full backup and the files from each day's incremental backup in the order they were created.
- If the municipality does a differential backup on all other nights, Monday night's differential contains "A" in its first modified form. Tuesday night's differential contains "A" in its first modified form and file "B." Wednesday night's differential contains "A" in its second version and "B." On Thursday the hard drive fails. To recover, the municipality would first copy the files from Sunday's full backup and then the files from Wednesday's differential backup to have all current versions of the files.

Differential backups can increase in size each day and may approach the size of a full backup. Since each differential backup includes everything in the previous differential

backup, many municipalities often do not retain all differential backups created between each full backup.

Incremental backups are usually smaller and fairly constant in size from day to day. All incremental backups must be retained until the next full backup is complete. The incremental backup offers the ability to recover any day's activity during the period between full backups. Consequently, if changes were made to a file that should not have been made, the incremental backup can be used to restore the file back to the unchanged form.

To provide timely and flexible recovery daily incremental backups are recommended, with a full weekly backup. It is good practice to devise a series of backups to ensure at least two new backups exist before one is destroyed.

For example: Business A uses a tape backup system. All users save their files to the business' central server. These files are backed up to a single tape, overwriting any data already on it. Backups are done on a daily basis using a series of four tapes. The business also uses a second series of tapes for weekly backups. In this example, the business has determined this is the schedule that best fits its needs based on how much data they could afford to lose:

Day	M	T	W	TH	F
Week 1	Daily Tape 1	Daily Tape 2	Daily Tape 3	Daily Tape 4	Weekly Tape 1
	M	T	W	TH	F
Week 2	Daily Tape 1	Daily Tape 2	Daily Tape 3	Daily Tape 4	Weekly Tape 2
	M	T	W	TH	F
Week 3	Daily Tape 1	Daily Tape 2	Daily Tape 3	Daily Tape 4	Weekly Tape 3
	M	T	W	TH	F
Week 4	Daily Tape 1	Daily Tape 2	Daily Tape 3	Daily Tape 4	Weekly Tape 4

The Daily group is used Monday through Thursday. The Weekly group is used on Fridays for a full backup.

2. Verify the Data Has Been Backed Up

Backup media needs to be reviewed periodically to determine if all of the data has been backed up accurately. Verification can consist of looking at the backup to verify specific pieces of data are there, confirming that files will open; or verifying the total size of the backup is the same size as the original data file.

Backup vs. Archival Storage

A backup is a copy of electronic information that is maintained for use if there is loss or damage to the original as a way to ensure business recovery. Backups can be compressed

to save space, and encrypted (plaintext or data converted into unintelligible form means of a reversible translation based on a translation table or algorithm), if files contain sensitive and confidential information to add security. Best practices require that municipalities keep multiple versions of backups to increase the chances of retrieving damaged or destroyed information. Best practices also recommend the backed-up file be labeled.

Archival storage is focused on the permanent maintenance of digital information valuable to a municipality that must be maintained uncorrupted and usable for a specified amount of time. Archival storage includes one master copy and at least one duplicate copy maintained a safe distance from the master. Unlike backups, stored archival records are the primary copy of the record, not a copy to be used in disaster recovery. Archival best practices dictate that records stored for archival purposes not be compressed or encrypted as such actions might limit the ability of a municipality to access and use those records in the future. Information security best practices, however, require sensitive or confidential information be encrypted where data is stored.

Sound archival procedures also include media migration, or refreshing, which is the process of copying data from one digital media type to another before the original media becomes obsolete. This process works only if the municipality does the refreshing on a regular basis. It must occur before the municipality loses the ability to read the data off the media. Digital media have a wide range of life expectancies; but magnetic media, such as computer tapes are generally more reliable than digital media, such as CDs and DVDs. Refreshing is most often conducted every five years, but the exact schedule for refreshing will depend on the longevity of the media and whether the media are becoming obsolete. Be aware that no media lasts forever, and factors such as climate conditions and constant reuse can cause the media to go bad.

Electronic data also face the danger of being rendered unusable because the file formats used to store the data are obsolete. It is always best to use file formats that are commonly used and non-proprietary. Open formats, such as TIFF image files or Open Document Format, are formats supported by a number of hardware and software platforms because the code needed to understand the format is published and publicly available. Municipalities using proprietary formats, which are formats controlled by a single company, will need to have a plan in place to migrate their data when they change electronic data systems or when the proprietary formats become obsolete.

Additional information on archival storage is available at:

- Digital Preservation Coalition: www.dpconline.org/graphics/reports

- CoOL (Conservation Online): http://palimpsest.stanford.edu/bytopic/electronic-records/electronic-storage-media

3. Store the Backup Media in a Secure, Safe Place

One of the biggest mistakes made with backups is storing them too close to the original sources, assuming that computer crashes are the only types of incidents a municipality may face. To protect its information, a municipality should always store backups in a physically secure facility far enough from its office not to be affected by the same fire, flood, or storm that might destroy records in the office. If backup media remains on-site, it should be stored in a non-adjoining building if possible and in a location secure from intrusion, fire, flood or other natural disasters.

Both backup and archival media should be stored in a physically secure location, ideally an off-site storage facility. Additionally, backups and archives should be protected from access with the same level of protection as working data.

4. Verify the Ability to Restore

It is best practice to frequently test that your backup data can be restored to your systems if loss occurs. Backing up data does little good if it cannot be restored to normal use.

Periodically test that the information can be restored from the backup copies. Periodically review your backup procedures to ensure that all important files are being included.

Provide training so that all personnel understand the need for backup procedures. Ensure that each makes all his or her important files available for inclusion in the backup procedures or follows individual procedures as part of the overall plan.

Summary - Your residents and business partners expect you to keep your municipality operating at all times. You cannot prevent natural disasters, human error or even malicious acts by employees or others; but you can have a plan that will keep you in business if any of these events occur. This guide has given you some basic information on backup and archival procedures that will enable you to restore your operations when the information you depend on has been destroyed, lost or corrupted. As with all of your important decisions, your approach to backup and archiving should be based on a careful analysis of your municipality's functions and the risks to your operations.

Destruction & Disposal of Electronic Equipment & Data

(Erasing Information and Disposal of Electronic Media)

Deleting Files Does Not Erase Information!

Introduction:

The intent of this policy is to describe how to dispose of computers and electronic storage media effectively; and prevent the inadvertent disclosure of information that often occurs because of inadequate cleansing and disposal of computers and electronic storage media.

There are many laws that require information be protected. Some examples of these laws are public health laws, privacy laws and the Health Insurance Portability and Accountability Act. Social Security numbers, credit card information, health-related information and trade secrets are examples of sensitive information requiring protection from disclosure. To the extent that electronic media is used to store official records, municipalities must also adhere to records management rules, including records retention schedules.

Sensitive documents and data containing personally identifiable information can be stored electronically in multiple formats and locations. For example, the information might first exist on a CD then be copied to the computer's hard drive and subsequently backed up to a tape for disaster recovery purposes. In this example, there are three different storage median to consider: CD, hard drive and backup tape.

Remember: Simply viewing a file with a computer can create a copy of the file on the computer's hard drive.

Deleting files does not erase information:

Information that is deleted from a computer may be retrieved by using forensic or other recovery tools. As new computers are purchased, older computers may be redeployed, discarded or surplused. It must be assumed that at some point in time sensitive information may have been stored and is still retrievable from all electronic storage media including computer and network hard rives, CDs, DVDs, floppy disks, tapes, thumb drives, memory sticks, PDAs, cell phones and other storage devices not enumerated here.

Policy:

When a municipality determines that its computer or electronic storage media should be redeployed, discarded or surplused, the municipality should use one or more of the following techniques.

Techniques for Erasing and Disposing:

Information at a municipality carries both benefits and risks. The benefits are that it allows a municipality to carry out its work making this information a valuable asset to the municipality. The risks can include accidental or malicious destruction of and unauthorized access to sensitive information. Municipalities must carefully manage the risks of unauthorized access by knowing what information it must keep private and setting up protocols for securing that information. Most importantly, municipalities need to develop and follow a set of policies and procedures that guide the process of destroying sensitive information on any media.

Ensuring Proper Erasure or Disposal:

Some tools may necessitate a knowledgeable and competent person to ensure the storage media is appropriately erased. If your municipality cannot ensure erasure of the media, you must find trained personnel who can carry out that activity and demonstrate that they have succeeded. Some commercial services may be available through IT consultants for municipalities. Your records office may be aware of additional tools and services. When in doubt, contact the device manufacturer.

Wiping Programs:

Wiping is a process of overwriting the space where files are located with random data. Read/writeable media should be "wiped" using a utility that is compliant with the Department of Defense (DOD) 5015.2-STD RMA Design Criteria Standard.

Issues:

- All appropriate options should be set to meet the DOD Standards.
- It may take a long time to rewrite the drive or media.
- A defective drive may not be able to be wiped.
- Additional procedures specified by the device manufacturer may need to be employed to ensure a complete wiping process.

Degaussing:

Degaussing is the erasure of information through the use of a very strong magnet. Degaussing is generally used for erasing of magnetic media - examples include tapes and floppy disks. Magnetic media should be "degaussed" using a Department of Defense (DOD) rated unit.

Issues:

- Since a very strong magnet is required to erase information, a municipality needs to remember to keep ALL magnetic media a sufficient distance from the degaussing unit

to prevent accidental erasure of essential information. Some examples include credit cards, cell phones and watches.

- Individuals with pacemakers need to maintain a safe distance from active degaussing.
- Degaussing any current generation hard disk will render the drive permanently unusable.

Physical Destruction:

Certain media can be read many times but can only be written once. These cannot be overwritten. Sometimes the media are defective and can no longer be used for retrieval or storage. In each of these cases the media should be physically destroyed.

Certain types of shredders are capable of shredding storage media such as CDs and DVDs. If this type of shredder is unavailable to your municipality then safely breaking the media into four or more pieces would be an appropriate destruction measure.

Any storage media can be physically destroyed through burning, crushing or smashing.

Issues:

- Environmental concerns may exist with incinerating media.
- Mechanisms need to be implemented to ensure the media is appropriately destroyed. Requiring a contractor to crush the media on site would be an appropriate control.
- Safety concerns include, but are not limited to, the use of safety goggles when using physical destruction techniques.

Recommended Techniques for Disposal of Electronic Storage Media:

Once a municipality has decided to dispose of electronic storage media, the following table can be used as a reference of recommended techniques to accomplish the job. This is not an all inclusive list of devices but a sample of the most commonly used pieces of equipment. Any device used to process information electronically may store information.

Erasure and Disposal Technique Matrix:

Media Type	Wipe or	Degauss or	Physical Destruction
Computer Hard Drive Network Hard Drive External Hard Drive	✓	✓	✓
Fax Machine Printer Copier	✓		✓

CDs DVDs			✓
USB Drives Thumb Drives Memory Sticks	✓		✓
Floppy Disks	✓	✓	✓
Tapes	✓	✓	✓
PDAs Cell Phones	✓		✓

Other Considerations:

Returning Media Under Warranty:

Many hard drives are purchased with a warranty period. When devices fail during the warranty period, the vendor normally requires the return of the defective drive before a warranty replacement is provided. Warranty return of a defective drive includes all the data, documents and information stored on the drive prior to the fatal problems. Since sensitive data could potentially be exposed on a warranty returned defective drive, the municipality should resort to physical destruction instead of returning the drive to the vendor. Your vendor may have an option to not return the hard drive.

Audit Trail:

A log should be maintained of all media that have been disposed. The log should include the date, type of device, manufacturer, serial number (if one exists), sanitation or destruction method used, disposal method (such as sold or crushed).

Retention and Disposition Schedule for New York Local Government Records (LGS-1):

All records, including electronic records must be retained and disposed of in accordance with the Retention and Disposition Schedule for New York Local Government Records (LGS-1), issued pursuant to Article 57-A of the Arts and Cultural Affairs Law, containing legal minimum retention periods for local government records, for use by all officers in legally disposing of valueless records listed therein.

In accordance with Article 57-A:

(a) only those records will be disposed of that are described in Retention and Disposition Schedule for New York Local Government Records (LGS-1), after they have met the minimum retention periods described therein;

(b) only those records will be disposed of that do not have sufficient administrative, fiscal, legal, or historical value to merit retention beyond established legal minimum periods.

Village of Warwick Application for User Internet Access

Check one: Add _____ Change _____ Delete_____ Date_____

LAN/Login ID _____

Name _____ Employee No. _____

Org. Name _____ Location/Floor _____ Phone _____

Primary Internet administrative, instructional, or research objectives or interests:

_____

_____

User Acknowledgement of Responsibility:

The internet has the potential to enhance user's access to and use of relevant job-related information and knowledge. As an internet participant, I understand and agree to maintain the trust placed in me by the Village of Warwick to protect the privileges and access given to me. I specifically agree that:

- I will comply with:
  1.) The Village of Warwick's Internet Access and Acceptable Usage Policy.
  2.) The policies of any host machine to which I am granted access.
- I will change my LAN password when I suspect it has been compromised.
- I am responsible for any security breach traceable to my assigned LAN LoginID and password.

Read and Understood:

I have received, read, and understand the Village of Warwick's Internet Access and Acceptable Usage Policy - (initial) _____ Date: _____

Please attach training certificate copies or a list of classes attended (include location and date) and approved by the Training Division.

Failure to follow these responsibilities will be subject to management review and action appropriate to the severity of the security violation.

Acknowledgement:

Employee: _____ Date: _____

Authorization:

Manager:_____ Date: _____

Glossary

- Application – Another word for program or software

- Anti-virus – Software program that searches for specific malicious characteristics (called signatures) in files on a computer system and prevents malicious ones from executing and infecting your network.

- Data Breach – A data breach is the unauthorized exposure – either intentional or unintentional – of private information to an untrusted environment.

- Encryption – The cryptographic transformation of data to render it unintelligible through an algorithmic process using a cryptographic key.

- Firewall – A security system that uses hardware and/or software mechanisms to prevent unauthorized users from accessing an organization's internal computer network.

- Locally Managed Network – Safeguards in place:
    - On a secure server.
    - Restrict administrator rights.

- Malware – A general term for malicious software. Malware includes virus, worms, Trojans and spyware.

- Network – A system of connected computers and other devices.

- Password – Specific word or mixtures of characters (letters, numbers, symbols) that grant access to a secure account or file.

- Restricted Information – pertains to information which is not public information, but can be disclosed to or used by municipal representatives to carry out their duties, so long as there is no legal bar to disclosure.

Other Resources

Center for Internet Security

www.cisecurity.org

The Center for Internet Security, Inc. (CIS) is a 501c3 nonprofit organization focused on enhancing the cyber security readiness and response of public and private sector entities, with a commitment to excellence through collaboration. CIS provides resources that help partners achieve security goals through expert guidance and cost-effective solutions.
Free incident response services available.

Internet Crime Complaint Center

www.ic3.gov

The IC3 was established as a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) to receive Internet related criminal complaints and to further research, develop, and refer the criminal complaints to federal, state, local, or international law enforcement and/or regulatory agencies for any investigation they deem to be appropriate.

OWASP Secure Coding Practices

https://www.owasp.org

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software.

Web Application Firewalls

AQTRONIX WebKnight is an application firewall for IIS and other web servers and is released under the GNU General Public License. More particularly it is an ISAPI filter that secures your web server by blocking certain requests. If an alert is triggered WebKnight will take over and protect the web server. It does this by scanning all requests and processing them based on filter rules, set by the administrator. These rules are not based on a database of attack signatures that require regular updates. Instead WebKnight uses security filters as buffer overflow, SQL injection, directory traversal, character encoding and other attacks. This way WebKnight can protect your server against all known and unknown attacks. Because WebKnight is an ISAPI filter it has the advantage of working closely with the web server, this way it can do more than other firewalls and intrusion detection systems, like scanning encrypted traffic.

https://www.aqtronix.com/?PageID=99

ModSecurity is an open source, cross-platform web application firewall (WAF) module. Known as the "Swiss Army Knife" of WAFs, it enables web application defenders to gain visibility into HTTP(S) traffic and provides a power rules language and API to implement advanced protections.

https://www.modsecurity.org/

Web Application Security Resources

The below companies offer for fee web application and network scan solutions that are utilized by many state and local governments:

https://www.qualys.com/

http://www.tenable.com/products/nessus

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6,700 potentially dangerous files/programs, checks for outdated versions of over 1,250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

http://www.cirt.net/Nikto2

Anti-Virus Software and Other Security Solutions

The below companies offer for fee anti-virus and other security products that are utilized by many state and local governments:

http://www.symantec.com/endpoint-protection

http://www.mcafee.com/us/

Malwarebytes and AVG offers free anti-malware software.

https://www.malwarebytes.org/

http://www.avg.com/us-en/homepage