






# Village of Avoca – Cyber Incident Response Plan

Purpose: <b>CIRP – Cyber Incident Response Plan</b>						Policy <b>#30</b>	
Effective: <b>September 1, 2023</b>				Author: <b>Eric R. Tyner</b>			
Approved by Board:	Mayor:	Trustee:	Trustee:	Trustee:	Trustee:	Filed:	Clerk:
						8-12-23	

## I. Context and Purpose:

- A. Cyber security relates to the confidentiality, availability, and integrity (CIA) of information and data that is processed, stored, and communicated by electronic or similar means, and protecting it and associated systems from external or internal threat.
- B. It is commonly recognised that cyber security involves the protection of critical information and ICT infrastructure, including supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS), through the alignment of people, processes, and tools.
- C. As the technology that underpins ICT infrastructure and related systems is continually advancing, cyber criminals are also advancing their skills and exploiting technology to conduct cyber-attacks with the aim of defrauding funds, disrupting business, or committing espionage. Furthermore, advanced technology is also complex, which leads to human error and workflow mistakes such as misconfigurations and general cyber security behaviours that do not meet best practice.
- D. This document supports the Village of Avoca in managing contemporary cyber threats and incidents. The application of this document will support the Village of Avoca in reducing the scope, impact, and severity of cyber incidents.
- E. This document describes the Village of Avoca's overall plan for preparing and responding to both physical and electronic information security incidents. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The goal of this Security Incident Response Plan is to prepare for, detect, and respond to security incidents. It provides a framework by which the Incident Response Team (IRT) shall determine the scope and risk of an incident, respond appropriately to that incident, communicate the results and risks to all stakeholders, and reduce the likelihood of an incident from occurring or reoccurring.

## II. Scope and Authority

- A. This plan applies to the physical location, the information systems, all personally identifiable information (PII) data, and networks of the Village of Avoca and any person or device that gains access to these systems or data.
- B. This cyber incident response plan is managed by the Mayor or his / her designee. This plan has been endorsed by Board of Trustees who is responsible for ensuring that Village of Avoca has a dependable and secure ICT environment.
- C. It is the responsibility of the Mayor of the Village of Avoca to maintain and revise this policy to ensure that it is always in a ready state.

## III. Definitions

**Event** - An event is an exception to the normal operation of infrastructure, systems, or services. A cyber event has the potential to become, but is not confirmed to be, a cyber incident. Not all events become incidents.

Cyber events can include:

- A. Multiple failed sequential logons for a user
- B. A user has disabled the antivirus on their computer
- C. A user has deleted or modified system files
- D. A user restarted a server
- E. Unauthorised access to a server or system.

**Incident** - An incident is an event that, as assessed by the staff, violates the policies of the Village of Avoca as related to Information Security, Physical Security, or Acceptable Use; other Village of Avoca policy, standard, or code of conduct; or threatens the confidentiality, integrity, or availability of information systems or PII.

Incidents will be categorized according to their potential for the exposure of protected data or the criticality of the resource, using a four (4) level system of: 0 – Low; 1 – Medium; 2 – High; 3 – Catastrophic.

Incidents can include:

- A. Malware attacks (Viruses/ Trojans/ Spyware)
- B. Ransomware
- C. Phishing and Social Engineering
- D. Denial of Service and Distributed Denial of Service (DDoS) attack
- E. Data Breach
- F. Unauthorized electronic access
- G. Unusual, unexplained, or repeated loss of connectivity
- H. Unauthorized physical access
- I. Loss or destruction of systems or information

**Evidence Preservation** - The goal of any incident response is to reduce and contain the impact of an incident and ensure that information security related assets are returned to service in the timeliest manner possible. The need for a rapid response is balanced by the need to collect and preserve evidence in a manner consistent with state and federal laws, and to abide by legal and administrative requirements for documentation and chain-of-custody

**Incident Response** – Incident response is the process of preparing for, detecting, and responding to security incidents, data breaches, or cyber-attacks in order to mitigate the impact and minimize the damage caused by the incident. The primary goal of incident response is to identify and contain the incident as quickly as possible, and then restore normal operations as soon as possible.

An effective incident response plan typically involves several key steps, including:

1. **Preparation:** This involves identifying potential security threats, developing an incident response plan, and conducting regular security training and awareness programs for employees.
2. **Detection:** This involves monitoring networks, systems, and applications for signs of a security incident, such as suspicious activity or unusual traffic patterns.
3. **Containment:** Once a security incident has been detected, the next step is to contain the incident to prevent it from spreading or causing further damage. This may involve isolating affected systems, disabling compromised user accounts, or shutting down specific services or applications.
4. **Analysis:** This involves investigating the incident to determine the cause, scope, and impact of the incident. This may involve analyzing log files, conducting forensic analysis, or reviewing security policies and procedures.
5. **Response:** This involves developing a response plan to address the incident, such as restoring data from backups, patching vulnerabilities, or deploying additional security controls to prevent future incidents.
6. **Recovery:** Once the incident has been contained and the response plan has been executed, the final step is to restore normal operations and ensure that systems and data are secure.

**Personally Identifiable Information (PII)** - Any information that can be used to identify an individual or that can be linked to a specific individual. Examples of PII include a person's name, address, phone number, email address, date of birth, Social Security number, driver's license number, passport number, and biometric data such as fingerprints or facial recognition data.

Under various data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) in the United States, organizations must take

reasonable measures to protect PII and ensure that it is collected, processed, and stored in compliance with applicable laws and regulations. It's important for individuals to be aware of the risks associated with PII and take steps to protect their personal information, such as using strong passwords, avoiding sharing sensitive information online, and regularly monitoring their credit reports for signs of fraudulent activity.

#### **IV. Incident Response Plan**

In accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-61 rev. 2, the Incident Response Life Cycle consists of a series of phases—distinct sets of activities that will assist in the handling of a security incident, from start to finish. More information about this process is found in Appendix B.

##### **A. Preparation**

1. Preparation includes those activities that enable the Village of Avoca to respond to an incident. These include a variety of policies, procedures, tools, as well as governance and communications plans.

The Village of Avoca utilizes several mechanisms to prevent, and prepare to respond to, an incident.

- a. Security Awareness Training: All personnel are required to take Cyber Awareness Training. The Village of Avoca requires annual security awareness training provided through NYCOM or an appropriate provider. Additionally, Village of Avoca seeks to have personnel participate stay up to date with cyber security news via webinars. The training covers additional ongoing threats to systems such as malware, phishing, social engineering, ransomware, and other threats as they become known.
- b. Malware/Antivirus/Spyware Protections: All information system terminals, as well as key information flow points on the network are protected by continuous defense against malware/antivirus/spyware and other known malicious attacks. These defense mechanisms are kept up to date without the need for end user intervention, and end users are restricted from accessing, modifying, disabling, or making other changes to the defense mechanisms.
- c. Firewalls and Intrusion Prevention Devices (IPD): Multiple firewalls and IPD are in place within the network to provide the necessary depth of defense. The Village of Avoca keeps all firewalls and IPD up to date with the latest security patches and other relevant upgrades, as well as maintain an active backup of the latest security configuration.
- d. Personnel Security Measures: All Village of Avoca personnel with access to PII or those areas in which CJI is accessed, stored, modified, transmitted, or maintained have been cleared to the required Personnel Security standards set forth by NYS.

- e. Physical Security Measures: All locations within the Village of Avoca that house PII or PII-related information systems are secured to the required. Access to these secured areas and information systems are a need-to-know/need to-share basis and authorized credentials for access are required and are under the direct control and management of the Village of Avoca.
- f. Event Logs: Event logging is maintained where applicable, capturing all the required events and content specified for PII, retained for the specified period, and reviewed as required.
- g. Patching/Updating: Systems shall be patched and updated as new security patches and hot fixes are released. Any software or hardware product that reaches the end of the manufacturers service and support life for patching will be reviewed and a plan will be made to address the product appropriately.

The Mayor or his or her designee, will strive to maintain adequate staff levels and third-party support to investigate each incident to completion and communicate its status to other parties while it continues to monitor the tools that detect new events.

No incident response capability can be effectively maintained over time without proper and ongoing training. The continuous improvement of incident handling processes implies that those processes are periodically reviewed, tested, and translated into recommendations for enhancements. All [municipal] staff will be trained on a periodic basis in security awareness, procedures for reporting and handling incidents to ensure a consistent and appropriate response to an incident, and that post incident findings are incorporated into policy and procedure.

## 2. Detection

Detection is the discovery of an event with security tools or through notification by an inside or outside party about a suspected incident. The detection of an incident requires the immediate activation of the IRT as listed in Appendix A. The determination of a security incident can arise from one or several circumstances simultaneously. Means by which detection can occur include:

Indicators	Examples
Reports of unusual or suspicious activity by staff, municipal departments/ facilities, or external	A staff member receives an email asking them to confirm their network credentials or to provide other personal or sensitive information.
	Multiple staff report being 'locked out' of their network accounts.
	An external stakeholder reports receiving spam or

stakeholders.	phishing emails from your organization.
	A member of the public approaches your organization to report the discovery (or exploitation) of a security vulnerability.
System(s)/service(s) not operating or functioning as expected	For example, one or more IT systems or services may cease functioning, or may not function as expected, and there is not a readily identifiable cause (such as a planned upgrade or outage).
	SSL Certificates broken; for example, customers complaining that your organization's website has a broken link.
Unusual activity	Network administrators observe many 'bounced' emails containing suspicious or unexpected content; or there is a substantial change in network traffic flows with no readily identifiable cause.
	Network or application logs show multiple failed login attempts from unfamiliar remote systems, such as overseas locations.
	Anti-virus alerts – a notification from your anti-virus service or a managed service provider that it has detected suspicious activity or files on your network, which require analysis and remediation.
	Service or admin accounts modifying permissions; admin accounts adding standard users to groups; service accounts logging into a workstation.
	A system administrator observes a filename with unusual characters, or expected files are no longer visible on the network.

It is critical in this phase:

- a. To detect whether a security incident has occurred.
- b. To determine the method of attack.
- c. To determine the impact of the incident to the mission, systems, and personnel involved in the incident.
- d. To obtain or create intelligence products regarding attack modes and methods.

### 3. Analysis

Analysis of the incident indicators will be performed in a manner consistent with the type of incident. In the event of a physical incident, appropriate steps will be taken to determine weaknesses in either the physical security of the facility, its monitoring tools, or its training programs to assess areas for process improvement or change is limited. For an electronic incident, Village of Avoca will utilize [define who is required] to perform static and dynamic analysis of malicious code, a review of information system boundary protections, determination of source code if applicable, the depth and breadth of the attack, if the attack has migrated to other systems on or off the network, and any other tasks appropriate to the type of incident experienced. These analyses can be performed either manually or utilizing automated tools dependent upon the situation, timeliness, and availability of resources.

There are several steps that are beneficial to confirming the presence of a cyber incident:

Action	Description
Updated Resources	Ensure you have access to the latest: Network diagrams IP addressing schemas Port lists Documentation that may include system designs/architecture, security plans, GPO configuration, etc.
Reviewing log entries and security alerts	Are there any unusual entries or signs of suspicious behavior on the network or applications?
Have Standard Operating Procedures (SOPs) for different operating systems	For Windows workstations, follow a SOP on what to look for or review (i.e. specific event log sources, the types of events to search for, etc.). The same applies for Linux and Unix Operating Systems.
Consult with network and application experts	Is there a legitimate explanation for the unusual or suspicious activity that has been observed?
Conduct research	Research and review any open-source materials (including via internet search engines) relating to the unusual or suspicious activity that is observed (for example, consider performing a search on any unusual filenames that are observed on the network).
Watch list / monitor list	Develop a list where suspected accounts or IPs can be added to monitor their ongoing activity.
<b>IMPORTANT</b>	Do not 'ping' or try to communicate with a suspected IP address or URL from your own network, as you

Action	Description
	may tip off the attacker that you have detected their activity. This should be conducted by a third party that is able to conduct this activity securely and anonymously.

#### 4. Categorization

An incident will be categorized as one of four severity levels. These severity levels are based on the impact to Village of Avoca and can be expressed in terms of financial impact, impact to services and/or performance of our mission functions, impact to Village of Avoca's image, impact to trust by Village of Avoca's customers and citizens, impact to wellbeing of Village of Avoca's residents (illness, death) etc. The below table provides a listing of the severity levels and a definition of each severity level.

Severity Level	Description
0 (Low)	Incident where the impact is minimal. Examples may be e-mail SPAM, isolated virus infections, etc.
1 (Medium)	Incident where the impact is significant. Examples may be a delayed or limited ability to provide services, meet Village of Avoca's mission, delayed delivery of critical electronic mail or data transfers, etc.
2 (High)	Incident where the impact is severe. Examples may be a disruption to the services and/or performance of our mission functions. Village of Avoca's proprietary or confidential information has been compromised, a virus or worm has become widespread and is affecting over 1% of employees, Public Safety systems are unavailable, or Village of Avoca's Executive management has been notified.
3 (Catastrophic)	Incident where the impact is catastrophic. Village of Avoca is severely impacted, where there is a potential threat to loss of life and/ or extensive damage to property, infrastructure or the environment. Examples may be a shutdown of all Village of Avoca's network services. Village of Avoca's proprietary or confidential information has been compromised or published in/on a public venue or site. Public safety systems are unavailable. The Board must make a public statement.



## 5. Incident Reporting

If an incident involves or is suspected of involving PII, the Mayor of his / her designee will be contacted and the IRT will be activated. \*Smaller incidents may be manageable without full activation of an IRT.

## 6. Incident Notification

It is important to notify relevant stakeholders that a cyber incident has occurred or is occurring. The scope, impact, and severity of the incident should determine the extent of stakeholder notifications. More serious incidents will likely require engagement with a broader range of stakeholders.

Key stakeholders to notify include:

- a. The Mayor and the (4) elected Board of Trustees;
- b. The Village of Avoca in-house IT contact and paid IT contact;
- c. If needed, the County of Steuben or the State of New York;
- d. Your cyber insurance provider, Aaron Benton

The IRT, typically via the Incident Manager or communications lead, is responsible for managing these notifications on behalf of the Village of Avoca.

## 7. IRT Documentation

Upon establishment, the IRT should immediately begin documenting information about the incident. This documentation includes situation updates and the incident log (Appendix C & D).

Situation updates should contain the following information:

- a. Incident date and time (usually the date and time the incident was confirmed)
- b. The status of the incident – for example, new / in progress / resolved
- c. Incident type and classification – for example, malware / ransomware / DDoS etc.
- d. Scope – details of affected networks, systems and/or applications
- e. Impact – details of entities affected by the incident, and how they are affected
- f. Severity – details of the impact of the incident on the municipality (for example, what services are impacted?)
- g. Contact details for the incident manager and key IRT personnel.

Situation updates should be prepared and disseminated to Village of Avoca internal stakeholders at regular intervals. It is important to be proactive with the

development and dissemination of your situation reports, to reduce the need for stakeholders to approach you with various questions about the incident.

The incident log should be maintained by a member of the IRT (or a delegate). The incident log should capture minutes from each IRT meeting, details of all critical decisions (including the rationale for a decision), operational actions taken, action items and future meeting dates and times. Each entry to the incident log should include date, time and author details.

## **B. Containment and Eradication**

### **1. Containment**

The Mayor or his / her designee is responsible for containment and will document all containment activities during an incident. Containment activities for security incidents involve decision-making and the application of strategies to help control attacks and damage, cease attack activities, or reduce the impact or damage caused by the incident. This requires intelligence gathered by the detection and analysis phases of the incident – for example, identification of affected hosts, identification of attacking hosts or attackers, identification of malware and its capabilities, and identification and monitoring of attacker communication channels. In most cases, it is important to introduce containment solutions all at once, as attackers may escalate their attack activity if deployment of the strategy is delayed.

### **2. Eradication**

The Mayor or his / her designee is responsible for eradication and will document all eradication activities during an incident.

Eradication efforts for a security incident involve removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

## **C. Analysis**

1. The IRT should develop a Resolution Action Plan for resolving the incident. The Resolution Action Plan should consider the immediate and future steps required for containing the incident and eradicating any threats that might exist; and the future steps required for restoring systems and services. The Resolution Action Plan should be reviewed throughout the process as it may change depending on what evidence is acquired during the detection and analysis steps.

The key elements of the Resolution Action Plan are:

- a. Containment actions – what are you doing now to contain and the incident/threat and prevent the spread of the situation?

- b. Eradication actions – what are you doing to remove the incident/threat from your environment?
  - c. Capability and capacity requirements – what resources do you require for the plan to be successful?
  - d. Communications actions – what messages are you communicating, to whom, when and how?
2. The details of the Resolution Action Plan will vary depending on the type of incident that you experience. There is no ‘one size fits all’ approach.

When developing the Resolution Action Plan, it is important to consider:

- a. How long will it take to resolve the incident?
- b. What resources are required to resolve the incident (if not already included in the IMT)?
- c. What systems/services will be affected during the resolution process? What services are impacted?

#### **D. Response**

##### **1. Evidence Preservation**

The IRT will collect and record evidence about the cyber incident to support detailed forensic investigations, including law enforcement efforts to identify and prosecute potential cyber-attackers.

To the best of its ability, and where relevant to the incident, the IRT should collect and record the following evidence:

- a. Hard drive images and raw images
- b. RAM images
- c. IP addresses
- d. Network packet captures and flows
- e. Network diagrams
- f. Log and configuration files
- g. Databases
- h. IR/investigation notes
- i. Screenshots
- j. Social media posts
- k. CCTV, video and audio recordings

1. Documents detailing the monetary cost of remediation or loss of business activity.
2. When gathering evidence, it is important to consider the following steps:
  - a. Nominate a member of the IRT to be responsible for collating, recording, and storing all evidence that is collected.
  - b. The IRT will create and maintain a log of all evidence collected, detailing the date and time evidence was collected, who it was collected by, and details of each item collected.
  - c. Ensure that all evidence is securely stored and handled only by the nominated IRT member, with limited access provided to other staff.
  - d. Any access to evidence should be clearly recorded in the evidence log, including the rationale for access. This is important in maintaining the 'chain of custody' for collected evidence.
  - e. Minimise the number of times evidence is transferred between staff. Record details of any evidence transfer between staff.
3. Communications and Engagement

Beyond the regular situation reports, it may be necessary to brief employees of Village of Avoca about a cyber incident. This is important if municipal IT networks, systems or applications no longer operate as expected, or if the situation has potential to generate media or public interest.

Key messages to consider when communicating with employees include:

- a. What happened and why did it happen?
- b. What will happen in the immediate future?
- c. What are employees expected to do?
- d. Who can employees contact if they have questions?

All internal communications must be reviewed and approved by the Mayor or his / her designee prior to release.

Depending on the impact and severity of a cyber incident, it may be necessary to communicate with external stakeholders (including residents, other municipalities, state/ federal agencies, and the media). This is particularly important if the incident affects IT networks, systems or applications relied upon by third parties, such as public facing websites or services.

Key messages to consider when communicating with external stakeholders include:

- a. What happened and why did it happen?
- b. What systems/services are affected?
- c. What steps are being taken to resolve the situation?
- d. Is it possible to say when the situation will be resolved?
- e. What are external stakeholders expected to do?

- f. Who can external stakeholders contact if they have questions/concerns?

All external communications must be reviewed and approved by the Mayor of his / her designee prior to release. Village of Avoca should seek guidance from state and federal agencies as well as consult insurers and regulators to ensure the right information is being conveyed in the right way.

## **E. Recovery**

The Mayor or his / her designee is responsible for recovery and will document all recovery activities during an incident.

Recovery efforts for incidents will involve the restoration of affected systems to normal operation. This is dependent upon the type of incident experienced but may include actions such as restoring systems from backups, rebuilding systems from an agency approved baseline, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host-based security.

The IRT should develop a plan for recovering from the cyber incident.

The recovery plan should detail the approach to recovering IT networks, systems and applications once containment and eradication is complete. Depending on the type and severity of an incident, the IRT may need to develop this plan in conjunction with business continuity and IT services advisors.

The recovery plan should include the following elements:

- a. A plan to restore systems to normal operation
- b. A process of continual monitoring to confirm that the affected systems are functioning normally
- c. A plan (if applicable) to remediate vulnerabilities to prevent similar incidents.

It is important to consider that, in some circumstances, a recovery plan may include the finalisation of a related criminal investigation (including forensic evidence collection), which may need to occur before recovery is possible.

Following the implementation and execution of an agreed recovery plan, the Incident Manager should advise the IRT that it is acceptable to stand down. The Incident Manager should gather copies of all notes taken during the response effort to assist with a Post Incident Review.

## **F. Post Incident Activities**

The Mayor or his / her designee is responsible for documenting and communicating post incident activity.

1. Post-incident activities will occur after the detection, analysis, containment, eradication, and recovery from a security incident. One of the most important phases of incident response, post-incident activities involve the reflection,

compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident, including the incident response team. Important items to be reviewed and considered for documentation are:

- a. Exactly what happened, and at what times?
- b. How well did staff and management perform in dealing with the incident?
- c. What information was needed sooner?
- d. Were any steps or actions taken that might have inhibited the recovery?
- e. What should be done differently the next time a similar incident occurs?
- f. How could information sharing with other organizations have been improved?
- g. What corrective actions can prevent similar actions in the future?
- h. What precursors or indicators should be watched for in the future to detect similar incidents?
- i. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Post-incident activities will be incorporated into future training opportunities for all parties involved in the incident, from victims to system administration personnel, to incident responders.

## 2. Escalation

The escalation process will be initiated to involve other appropriate resources as the incident increases in scope and impact. Incidents should be handled at the lowest escalation level that can respond to the incident with as few resources as possible to reduce the total impact and maintain limits on cyber-incident knowledge. The table below defines the escalation levels with the associated team members involvement.

Severity Level	Coordination and Response Team Involvement	Description
0 (Low)	<ul style="list-style-type: none"> <li>- IT Technical Support Staff or Vendor.</li> <li>- Local Municipal Security Officer (IT Director, CSO, CISO, Cybersecurity Officer).</li> </ul>	Normal operations.
1 (Medium)	<ul style="list-style-type: none"> <li>- IT Technical Support Staff or Vendor.</li> <li>- Local Municipal Security Officer (IT Director, CSO, CISO, Cybersecurity</li> </ul>	Village of Avoca is aware of a potential or actual threat and is responding to that threat.

	Officer).	
2 (High)	<ul style="list-style-type: none"> <li>- IT Technical Support Staff or Vendor.</li> <li>- Local Municipal Security Officer (IT Director, CSO, CISO, Cybersecurity Officer).</li> <li>- Municipal Administrator/Controller.</li> <li>- Government Agencies (FBI, DHS)</li> <li>- Cyber Insurance Provider</li> </ul>	An obvious threat has impacted business operations. Determine course of action for containment and eradication. Message staff of required actions and operational impacts if necessary.
3 (Catastrophic)	<ul style="list-style-type: none"> <li>- IT Technical Support Staff or Vendor.</li> <li>- Local Municipal Security Officer (IT Director, CSO, CISO, Cybersecurity Officer).</li> <li>- Municipal Administrator/Controller.</li> <li>- Finance Director.</li> <li>- Legal Contact.</li> <li>- Cyber Insurance Provider</li> <li>- [Spokesperson Title]</li> <li>- Government Agencies (FBI, DHS)</li> </ul>	Threat is wide spread with significant impact. Determine course of action for containment, mitigation, and eradication. Message staff and officials. Prepare for legal action. Prepare for a public statement

The IRT will consider several characteristics of the incident before escalating the response to a higher level. They are:

- How widespread is the incident?
- What is the impact to business operations?
- How difficult is it to contain the incident?
- How fast is the incident propagating?
- What is the estimated financial impact to Village of Avoca?
- Will this negatively affect Village of Avoca's image?
- Will this impact the wellbeing of residents of the Village of Avoca?

## V. Threat Scenarios

Some examples of threat scenarios that Village of Avoca could face include:

### 1. Ransomware attacks:

A ransomware attack is a type of malware attack that encrypts critical data on a victim's computer or network, making it inaccessible to the user until a ransom is paid. This type of attack is becoming increasingly common and sophisticated and can cause severe disruption and financial loss to municipal governments.

In a ransomware attack, the attacker typically gains access to a system through a vulnerability or social engineering tactic, such as a phishing email. Once inside, the attacker can encrypt data on the victim's system, making it unusable. The attacker then demands payment, often in cryptocurrency, in exchange for the decryption key.

Municipal governments may be targeted by ransomware attacks due to the sensitive nature of their data and operations. For example, a ransomware attack on a municipal government's network could cause severe disruption to essential services such as utilities, emergency services, and transportation.

### 2. Phishing attacks:

Phishing attacks are a type of social engineering attack where attackers use emails or other messages to trick victims into providing sensitive information, such as login credentials, financial information, or personal information. Municipal governments may be targeted by phishing attacks in an attempt to gain access to sensitive data or credentials.

In a typical phishing attack, the attacker poses as a legitimate entity, such as a bank or government agency, and sends an email or message to the victim. The message may contain a link to a fake website or a file attachment that contains malware. Once the victim clicks on the link or opens the attachment, the attacker can gain access to sensitive data or systems.

Phishing attacks can be highly effective and difficult to detect, as attackers may use sophisticated techniques to create convincing messages that appear legitimate. Municipal governments may be targeted by phishing attacks in an attempt to gain access to sensitive data, such as financial information or personally identifiable information (PII), or to plant malware that can be used in future attacks.

### 3. Distributed Denial of Service (DDoS) attacks:

A Distributed Denial of Service (DDoS) attack is a type of cyber-attack that involves flooding a website or network with traffic in an attempt to overwhelm and disable it. DDoS attacks are often carried out by botnets, which are networks of compromised devices that can be controlled remotely by an attacker.



Municipal governments may be targeted by DDoS attacks by hacktivist groups or other actors seeking to disrupt operations or make a political statement. For example, a DDoS attack on a municipal government's website could disrupt access to essential services or cause public relations problems.

4. Insider threats:

An insider threat is a type of cyber threat that involves a trusted employee or contractor abusing their access to information or systems for malicious purposes. Insider threats can be particularly challenging to detect and prevent, as the attacker already has legitimate access to the victim's systems.

Municipal governments may face insider threats from disgruntled employees, contractors, or other insiders with access to sensitive information or systems. For example, an insider may steal data for personal gain or for use in a future attack or may attempt to disrupt operations or sabotage systems.

5. Advanced persistent threats (APTs):

An Advanced Persistent Threat (APT) is a sophisticated, targeted attack that involves a combination of social engineering, malware, and other tactics to gain access to sensitive information or systems. APTs are often carried out by nation-state actors or other highly motivated attackers with specific targets in mind.

Municipal governments may be targeted by APTs seeking to steal sensitive data, disrupt operations, or carry out other malicious activities. APTs can be highly sophisticated and difficult to detect, as they may use a variety of techniques to evade detection and gain access

## Appendix A

Village of Avoca Incident Response Team (IRT) is responsible for managing responses to cyber incidents. The members of the IRT are identified below:

Title/ Role	Name	Contact Info	Responsibilities
Technology Coordinator /IT Director/ CSO/ CISO			<ul style="list-style-type: none"> <li>- Planning and operations</li> <li>- Intelligence and analysis</li> <li>- Technical advice</li> </ul>
Technical Support Staff			<ul style="list-style-type: none"> <li>- Intelligence and analysis</li> <li>- Technical advice</li> </ul>
Communications Coordinator/ Spokesperson			<ul style="list-style-type: none"> <li>- Information and warnings</li> <li>- Internal communications</li> <li>- Media and community liaison</li> </ul>
Internal Audit Coordinator			<ul style="list-style-type: none"> <li>- Advisory services (e.g., regulatory compliance)</li> </ul>
Internal/ External Legal Counsel			<ul style="list-style-type: none"> <li>- Legal advisory services (e.g., regulatory compliance, insurance)</li> </ul>
Responsible Elected Official			
Human Resources			
First Responders (NYS DHS/ FBI/ Local Law Enforcement)			<ul style="list-style-type: none"> <li>- Technical/forensic investigations and communications support</li> </ul>
Insurance Provider			<ul style="list-style-type: none"> <li>- Intelligence and analysis</li> <li>- Technical advice</li> <li>- Advisory services</li> <li>- Facilities and finance support</li> </ul>
Finance/ Procurement			<ul style="list-style-type: none"> <li>- Facilities and finance support</li> </ul>
Operations Officer – Business Continuity			<ul style="list-style-type: none"> <li>- Facilities support</li> <li>- Business and community consequence analysis / management</li> </ul>

## Appendix B

This document discusses the steps taken during an incident response plan. To create the plan, the steps in the following example should be replaced with contact information and specific courses of action for your municipality.

1. The person who discovers the incident will call the Village Clerk's Office. List possible sources of those who may discover the incident. The known sources should be provided with a contact procedure and contact list. Sources requiring contact information may be:

- a. The Maintenance Supervisor;
- b. The Fire Chief;
- c. The Mayor;
- d. Trustees;
- e. IT Administrator;
- f. An outside source.

List all sources and check off whether they have contact information and procedures. Those in the IT department may have different contact procedures than those outside the IT department.

2. If the person discovering the incident is a member of the IT department or affected department, they will proceed to step 5.
3. If the person discovering the incident is not a member of the IT department or affected department, they will call the Mayor.
4. The Mayor will refer to the IT emergency contact list or effected department contact list and call the designated numbers in order on the list. The Clerk's Office will maintain the incident documentation to include:
  - a. The name of the caller.
  - b. Time of the call.
  - c. Contact information about the caller.
  - d. The nature of the incident.
  - e. What equipment or persons were involved?
  - f. Location of equipment or persons involved.
  - g. How the incident was detected.
  - h. When the event was first noticed that supported the idea that the incident occurred.
5. The IT staff member or Mayor who receives the call (or discovered the incident) will refer to their contact list for the Board of Trustees to be contacted and incident response members to be contacted. The Mayor will call those designated on the list.

The employee will contact the incident response manager using both email and phone messages while being sure other appropriate and backup personnel and designated contacts. The Village Clerk will log the information received in the same format as the Mayor's office in the previous step. The employee could possibly add the following:

- a. Is the equipment affected business critical?
  - b. What is the severity of the potential impact?
  - c. Name of system being targeted, along with operating system, IP address, and location.
  - d. IP address and any information about the origin of the attack.
6. Contacted members of the Board of Trustees will meet or discuss the situation to determine a response strategy.
  - a. Is the incident real or perceived?
  - b. Is the incident still in progress?
  - c. What data or property is threatened and how critical is it?
  - d. What is the impact on the business should the attack succeed? Minimal, serious, or critical?
  - e. What system or systems are targeted, where are they located physically and on the network?
  - f. Is the incident inside the trusted network?
  - g. Is the response urgent?
  - h. Can the incident be quickly contained?
  - i. Will the response alert the attacker, and do we care?
  - j. What type of incident is this? Example: virus, worm, intrusion, abuse, damage.
7. An official report will be created. The incident will be categorized into the highest applicable level of one of the following categories:
  - a. Category one - A threat to public safety or life.
  - b. Category two - A threat to sensitive data
  - c. Category three - A threat to computer systems
  - d. Category four - A disruption of services
8. IT members will establish and follow one of the following procedures basing their response on the incident assessment:
  - a. Worm response procedure
  - b. Virus response procedure
  - c. System failure procedure

- d. Active intrusion response procedure - Is critical data at risk?
- e. Inactive Intrusion response procedure
- f. System abuse procedure
- g. Property theft response procedure
- h. Website denial of service response procedure
- i. Database or file denial of service response procedure
- j. Spyware response procedure.

The Board of Trustees may create additional procedures which are not foreseen in this document. If there is no applicable procedure in place, the Board must document what was done and later establish a procedure for the incident.

- 9. IT members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization. *As a municipality, you may rely solely on contracted IT personnel so be sure to make note of that.*
- 10. IT members will recommend changes to prevent the occurrence from happening again or infecting other systems.
- 11. Upon the Board of Trustees approval, the changes will be implemented.
- 12. IT members will restore the affected system(s) to the uninfected state. They may do any or more of the following:
  - a. Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
  - b. Make users change passwords if passwords may have been sniffed.
  - c. Be sure the system has been hardened by turning off or uninstalling unused services.
  - d. Be sure the system is fully patched.
  - e. Be sure real time virus protection and intrusion detection is running.
  - f. Be sure the system is logging the correct events and to the proper level.
- 13. Documentation—the following shall be documented:
  - a. How the incident was discovered.
  - b. The category of the incident.
  - c. How the incident occurred, whether through email, firewall, etc.
  - d. Where the attack came from, such as IP addresses and other related information about the attacker.
  - e. What the response plan was.

- f. What was done in response?
  - g. Whether the response was effective.
14. Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.
  15. Notify proper external agencies—notify the police and other appropriate agencies.
  16. Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
  17. Review response and update policies—plan and take preventative steps so the intrusion can't happen again.
    - a. Consider whether an additional policy could have prevented the intrusion.
    - b. Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
    - c. Was the incident response appropriate? How could it be improved?
    - d. Was every appropriate party informed in a timely manner?
    - e. Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
    - f. Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
    - g. Have changes been made to prevent a new and similar infection?
    - h. Should any security policies be updated?
    - i. What lessons have been learned from this experience?

## Appendix C

<b>DATE OF ENTRY:</b>	<b>TIME OF ENTRY:</b>	<b>AUTHOR:</b>
<b>DATE AND TIME INCIDENT DETECTED</b>		
<b>CURRENT STATUS</b>	New / In Progress / Resolved	
<b>INCIDENT TYPE</b>	Malware/ Ransomware/ Phishing/ Denial of Service/ Unauthorized Access	
<b>INCIDENT CLASSIFICATION</b>	Event/ Low Impact/ Medium Impact/ High Impact/ Catastrophic	
<b>SCOPE</b> – list the affected networks, systems and/or applications; highlight any change to scope since the previous log entry		
<b>IMPACT</b> – list the affected stakeholder(s); highlight any change in impact since the previous log entry		
<b>SEVERITY</b> – outline the impact of the incident on the stakeholder(s); highlight any change to severity since the previous log entry		
<b>NOTIFICATIONS ACTIONED/PENDING</b>		
<b>ADDITIONAL NOTES</b>		
<b>CONTACT DETAILS FOR INCIDENT MANAGER</b>		
<b>DATE AND TIME OF NEXT UPDATE</b>		

## Appendix D

[illegible]