TOWN OF MILFORD
NEW HAMPSHIRE

CYBER INCIDENT RESPONSE POLICY

Contents

Table of Contents

Introduction

Purpose

This document describes the Town of Milford's (hereinafter referred to as 'The Town') overall plan for preparing and responding to information security incidents, both physical and electronic. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The goal of this Cyber 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. Then, respond appropriately to that incident, communicate the results and risks to all stakeholders, and reduce the likelihood of an incident from occurring or reoccurring.

Scope

This plan applies to the electronic and physical components of the Town's information systems and networks, and any person or device that gains access to these systems or data. This applies only to the Town of Milford. The Milford School system is under alternative management and is not applicable under this plan.

Maintaining Currency

It is the responsibility of the IT Director to maintain and, if necessary, revise this policy annually, to ensure that it is always in a ready state.

Definitions

Event

An event is an exception to the normal operation of infrastructure, systems, or services. Not all events become incidents.

Incident

An incident is an event that, as assessed by the staff, violates the policies of the Town as related to Information Security, Physical Security of IT components, or Acceptable Use; other Town policy, standard, code of conduct; or threatens the confidentiality, integrity, or availability of information systems. Incidents are categorized according to their potential for the exposure of protected data or the criticality of the resource, using a four (4) level system of: 1- Low; 2 - Medium; 3 - High; 4 - Extreme.

Incidents can include:

1) Malware/viruses/Trojans
2) Ransomware
3) Successful Phishing Attack
4) Unauthorized electronic access to Town Information System hardware
5) Breach of information
6) Unusual, unexplained, or repeated loss of connectivity
7) Unauthorized physical access
8) Loss or destruction of physical files, etc.
9) Town email compromise

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 and return to operation is balanced by the need (if possible) 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

The Incident Response Life Cycle consists of a series of phases. There are distinct sets of activities that will assist in the handling of a security incident, from start to finish. These include Preparation, Detection and Analysis, Containment, Eradication, and Recovery, and Post-Incident Activity.

Preparation

Preparation includes those activities that enable the Town to respond to an incident. These include a variety of policies, procedures, tools, as well as governance and communications plans. The Town utilizes several mechanisms to prevent, as well as prepare to, respond to an incident.

- *Security Awareness Training:* The Town requires bi-monthly security awareness training provided through KnowBe4. This training covers phishing threats as they become known. New employees are required to complete training that covers phishing, social engineering, ransomware and other threats.
- *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.
- *Firewalls and Intrusion Prevention Devices (IPD):* Multiple firewalls and IPD are in place within the network to provide the necessary depth of defense. IT Department 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.
- *Physical Security Measures:* All locations within the Town that house information systems are secured. Access to these secured areas and information systems are a need-to-know/need- to- share basis and required agency authorized credentials for access and are under the direct control and management of the Town.
- *Event Logs:* Event logging is maintained at all applicable levels.
- *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 deemed out-of-compliance and replaced.

Staffing

The Town 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.

Training

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 Town staff will participate in initial security awareness training upon initial employment as well as on a bi-monthly basis via simulated phishing tests. Additional security awareness training on topics such as recognizing and reporting incidents, safety protocols and other topics is provided as needed. Procedures for reporting and handling incidents will be provided and post-incident findings may be incorporated into policy and procedure.

Detection and Analysis

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 determination of a security incident can arise from one or several circumstances simultaneously. Means by which detection can occur include:

- Trained personnel reviewing collected event data for evidence of compromise.
- Software applications analyzing events, trends, and patterns of behavior.
- Intrusion Protection/Intrusion Detection devices alerting to unusual network or port traffic.
- The observation of suspicious or anomalous activity within a Town facility or on a computer system.

Incidents detected by anyone other than the IT Department shall report the incident to the IT Department or his/her designee IMMEDIATELY, as a quick response to an incident is critical. Specific procedures are listed in Appendix C. The detection of an incident with a severity level of 2 or higher requires the immediate activation of the IRT as listed in Appendix B.

It is imperative in this phase:

- To detect whether a security incident has occurred.
- To determine the method of attack.
- To determine the impact of the incident to the mission, systems, and personnel involved in the incident.
- To obtain document information concerning regarding attack modes and methods.

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. For an electronic incident of level 3 or 4, Town will utilize NH Primex 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. NH Primex may be utilized for electronic incidents of level 2, depending on severity and circumstances.

Incident Categories

An incident will be categorized as one of four severity levels. Categorization is initially completed by IT Department, the IRT will either confirm or change the categorization at the earliest possible time. These severity levels are based on the impact to The Town and can be expressed in terms of financial impact, impact to trust by The Town's customers and citizens, impact to services and/or performance of mission functions, impact to The Town's image, etc. The below table provides a listing of the severity levels and a definition of each severity level.

Severity Level	Description
1 (Low)	Incident where the impact is minimal. Examples may be e-mail SPAM, isolated virus infections, etc.
2 (Medium)	Incident where the impact is significant. Examples may be a delayed or limited ability to provide services, inability to meet the Town's mission, delayed delivery of critical electronic mail or data transfers, etc.
3 (High)	Incident where the impact is severe. Examples may be a disruption to the services and/or performance of our mission functions, the Town's proprietary or confidential information has been compromised, a virus or worm has become widespread and is affecting over 10 percent of employees, Public Safety systems are unavailable.
4 (Extreme)	Incident where the impact is catastrophic. Examples may be a shutdown of all The Town's network services. The Town's proprietary or confidential information has been compromised and published in/on a public venue or site. Public safety systems are unavailable. Executive management may make a public statement if needed.

Containment, Eradication, and Recovery

Any time a suspected event occurs, day or night, immediately shut down the offending PC by either holding the power button in for 5 seconds or unplugging its power cord. The person discovering the incident shall then contact the IT Department. The IT Department will coordinate notification of the Town Administrator as well as NH Primex to file a cyber liability claim in the event the severity level is 2 or higher. If the IT Department is unavailable, the person will then notify his/her Department Head. The DH will attempt to first contact the IT Dept, secondly the Town Administrator. If both are still unavailable, the Department head shall contact NH Primex directly to file a cyber liability claim, regardless of severity level. NH Primex will aid in determining the applicable severity level and assist until IT Department is available. Once the incident has been contained and the offending system disconnected from the Town's network information systems, a security incident report will be completed and submitted to NH Primex and MS-ISAC for further analysis. Internal IT Department will work in partnership with NH Primex during the process until all known incidents have been resolved.

Containment

The IT Department, in tandem with NH Primex, is responsible for overseeing the containment and will document all containment activities during an incident. In the event that the IT Department is unavailable, the Dept head responsible will document as much information as possible.

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.

Eradication

The IT Department, in tandem with NH Primex, is responsible for overseeing the 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.

Recovery

The IT Department, in tandem with NH Primex, is responsible for overseeing the 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.

Post-Incident Activity

NH Primex and its IT Security sub-contractor are responsible for documenting and communicating post-incident activity.

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:

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

Escalation

The IT Department is responsible for recommending incident escalation as necessary at any point during an incident. When the IT Department determines that escalation is necessary and dependent on the current severity level, they shall notify the necessary members of the IRT, who will make the final determination concerning escalation. While the recommendation is under review by the IRT, the IT Department shall respond as if the recommendation to escalate has been approved. 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 in order 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	Response Team Member Involvement	Description
1 (Low)	• IT Department Staff and/or Contractor	Normal operations.
2 (Medium)	• IT Department Staff and/or Contractor • Involved Department Head • NH Primex	Reference Incident Category descriptions on page 5.
3 (High)	• IT Department Staff and/or Contractor • Department Head • Town Administrator • NH Primex	Reference Incident Category descriptions on page 5.
4 (Extreme)	• IT Department Staff and/or Contractor • Department Head • Town Administrator • Legal Contact • NH Primex	Reference Incident Category descriptions on page 5.

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

1) How widespread is the incident?
2) What is the impact to Town operations?
3) How difficult is it to contain the incident?
4) How fast is the incident propagating?
5) What is the estimated financial impact to the Town?
6) Will this negatively affect the Town's image?

Approved:

(Mark Bender), Town Administrator

8/23/22
Date

Appendix A: NH Primex Cybersecurity Incident Reporting Procedures

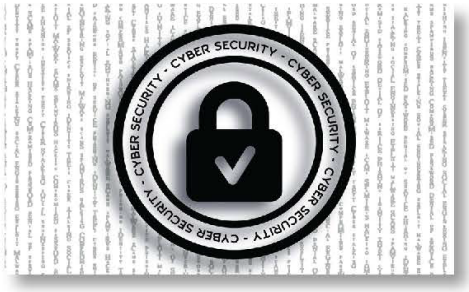
Primex³ NH Public Risk Management Exchange

Cybersecurity Incident Reporting Procedures

Cybersecurity breaches are very serious and continue to be on the rise. In the event you experience such an occurrence or suspect one, please follow the procedures outlined below.

Call Primex³ Immediately!

In the event of a **SUSPECTED** or **ACTUAL** attack, call as soon as possible to prevent further damage!



Our Claims Department stands ready to assist you. Primex³ will arrange for technical forensic, legal, communication, and negotiation response, if applicable, as part of your Property and Liability coverage. This can be accomplished 24/7 with one call to Primex³:

603-225-2841 or **1-800-698-2364**

Additional Notifications

- **LAW ENFORCEMENT:**

  The incident can be reported to your local police department, but for investigation of cybersecurity incidents with international jurisdictional realities federal law enforcement should be contacted:

  - **United States Secret Service, Manchester, New Hampshire Residence Office**

    Office: 603-626-7026 or Resident Agent in Charge, Timothy Benitez: 202-355-3037

  - **Federal Bureau of Investigation, Boston Field Office**

    Office: 857-386-2000

  In the event Criminal Justice Information (CJI) is involved:

  - **New Hampshire State Police - Justice Information Bureau**

    Office: 603-223-8701

- **STATE OF NEW HAMPSHIRE:**

  - **New Hampshire Cyber Integration Center (NHCIC)**

    Office: 603-271-7555 or After Hours: 603-271-7555 (Option 2), **nh-cic@doit.nh.gov** or **helpdesk@doit.nh.gov**

  - **Multi-State Information Sharing and Analysis Center (MS-ISAC)**

    Office: 866-787-4722, **soc@cisecurity.org**

*Law Enforcement and State of New Hampshire notifications are considered local policy decisions, some of which may be required. Consult with your local legal counsel **prior to** a suspected or actual cyber-attack and consider adding these organizations to your **Incident Response Plan** so you will know whether to call in case of an emergency.* Please call Primex³ or CLICK HERE should you require assistance with the creation of your Incident Response Plan.

Rev. 01/12/2021

800.698.2364
46 Donovan Street, Concord, NH 03301

Primex³ NH Public Risk Management Exchange

www.nhprimex.org
Trust. Excellence. Service.

Appendix B: Incident Response Team + Department Heads

Role	Leadership Members	eMail	phone
IT Director	Bruce Dickerson	bdickerson@milford.nh.gov	O: 603-249-0612 C: 603-783-6524
IT Assistant	Randy Ippolito	rippolito@milford.nh.gov	O: 603-249-0613 C: 603-520-2011
Town Administrator	Mark Bender	mbender@milford.nh.gov	O: 603-249-0602 C: 603-769-1286
Fire Dept Chief & Emergency Mgmt	Ken Flaherty	kflaherty@milford.nh.gov	O: 603-249-0681 C:603-732-6689
Police Chief	Mike Viola	mviola@milford.nh.gov	O: 603-249-0630
Ambulance Dir	Eric Schelberg	eschelberg@milford.nh.gov	O:603-249-0609 C:603-860-0939
Finance Director	Paul Calabria	pcalabria@milford.nh.gov	O: 603-249-0642 C: 603-582-0361
Community Media	Chris Gentry	cgentry@milford.nh.gov	O: 603-249-0670 C: 603-732-2985
Community Development	Lincoln Daley	ldaley@milford.nh.gov	O: 603-249-0621 C: 603-247-6983
Public Works	Leo Lessard	llessard@milfod.nh.gov	O: 603-249-0685 C: 603-801-2713
HR	Karen Blow	kblow@milford.nh.gov	O: 603-249-0605 C: 603-801-5885
Recreation	Arene Berry	aberry@milford.nh.gov	O: 603-249-0625 C: 603-732-7558
Town Clerk	Joan Dargie	joan.dargie@milford.nh.gov	O: 603-249-0650 C: 603-233-0788
Water Utilities	Jim Pouliot	jpouliot@milford.nh.gov	O: 603-249-0661 C: 603-365-1750

Reference Appendix A for additional NH Primex contact & information.

Additional Numbers / Contacts

Appendix C: Incident Response Process Tree

This document discusses the steps taken during an incident response plan.

1) The person who discovers the incident will contact The IT Department at any time. If the IT Dept is unavailable, the person will contact the their Dept Head. The Dept Head will attempt to contact the IT Dept. If the IT Dept is unavailable, the Dept Head will contact NH Primex directly. In the event of a legitimate incident where The IT Department and the Dept Head are unavailable, the person discovering the incident will contact NH Primex to initiate a cyber liability claim. Sources requiring contact information are found in Appendix B:
    a) IT Dept
    b) Department Heads.
    c) NH Primex
2) The IT Department, or (if the IT Dept is unavailable), the Dept Head or Incident Person will log:
    a) The name of the person reporting the incident.
    b) Time of the call.
    c) Contact information about the caller.
    d) The nature of the incident.
    e) When the event was first noticed, supporting the idea that the incident occurred.
    f) Is the system affected business critical?
    g) What is the severity of the potential impact?
    h) (When possible) The name of system being targeted, along with operating system, Internet Protocol (IP) address, and location.
    i) (When Possible) the IP address and any information about the origin of the attack.
3) Review: Contacted members of the response team will meet or discuss the situation in person and/or electronically and develop a response strategy. In the event that the IRT cannot be assembled in a timely manner such determinations shall be accomplished by the IT Department
    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(s) are targeted, where are they located physically and on the network?
    f) Is the incident inside the internal staff network?
    g) Is the response urgent (severity level)?
    h) Can the incident be quickly contained?
    i) Will the response alert the attacker?
    j) What type of incident is this? Example: virus, worm, intrusion, abuse, damage, data exfiltration, ransomware, Town email compromise.
4) Categorize: An incident ticket will be created by The IT Department. The IRT will categorize the incident into the highest applicable level of one of the following categories:
    a) Severity Level 1 (Low) - Minimal impact on operations.
    b) Severity Level 2 (Medium) -A threat to sensitive data.
    c) Severity Level 3 (High) - A threat to computer systems.
    d) Severity Level 4 (Extreme) - A disruption of services.
6) Response: Team members will develop procedures specifically related to the type of incident. The team may create additional procedures which are not foreseen in this document. If there is no applicable procedure in place, the team must document what was done.

Post Incident Activity

7) Team members will use forensic techniques, including reviewing system logs and interviewing all involved parties to determine how the incident was caused. Only IT authorized personnel shall perform interviews or authorize examination of evidence.
8) Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.
9) Upon management review and approval, the changes will be implemented.
10) Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:
    a) Reinstall the affected system(s) from scratch and restore data from uninfected backups if necessary and able
    b) Make users change passwords if passwords may have been compromised.
    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.
11) **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?
12) **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.
13) Notify proper external agencies-notify the police and other appropriate agencies if prosecution of the intruder is possible. Reference Appendix A for contact information.
14) Assess damage and cost-assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
15) Review response and update policies-plan and take preventative steps so the intrusion cannot 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 reinfection? Have all systems been patched, systems locked down, passwords changed, antivirus 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?