City of Bexley, Ohio

Cyber Incident Response Plan

Table of Contents

Plan Version History

Version	Date	Description	Approved By
1.0	1.16.2023	Initial Policy Initiated	

Plan Mission & Objective:

The City of Bexley Incident Response Plan (IRP) documents the strategies, personnel, procedures, and resources required to respond to various cybersecurity incidents affecting the City of Bexley, Ohio's systems and data, in accordance with documentation set forth in the LEADS Security Policy for Law Enforcement Systems with access to Criminal Justice Information Services (CJIS), and as a part of the NIST Cybersecurity framework for the balance of the City of Bexley's systems.

A cyber incident is defined as "actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on the City's information systems and/or the information residing therein."

This plan will be reviewed and updated annually, or at any time a security incident indicates a change should be made to the IRP.

Scope:

This plan applies to all information systems, institutional data, and networks of The City of Bexley, Ohio and any person or device accessing these systems or data.

The Information Security Manager (ISM) acts on behalf of the City of Bexley, Ohio and will request cooperation and assistance in investigating incidents from City employees and other constituents as required. The ISM will also work closely with other City administrative groups such as Human Resources, General Counsel, Finance, and Public Safety in the investigation of incidents as appropriate and required by policy.

Balance of page intentionally left blank

Roles and Responsibilities Matrix:

The roles and responsibilities for various task assignments and deliverables throughout the incident response process are depicted in the table below. The following should be the members of the Incident Response Team:

Roles and Responsibilities of Incident Response Team

Roles	Filled By	Responsibilities
Information System Owner	Gary Lewis, Chief of Police	Annual review of documentation, and perform annual test of IRP. Ensure that Security Manager and The City systems administrators are properly trained, and have resources required to maintain an incident response capability.
Information Security Manager	Erik McGuinness, IT Manager	Oversee and prioritize actions during the detection, analysis, and containment of an incident. Work on annual IT response team tabletop sessions for response process validation and updates.
Agency Administrator	Gary Lewis, Chief of Police	Owner of the Information Systems of the Bexley Police Department
EOC Administrator	Lt Dawn Overly, Emergency Management Director	Director of Emergency Management Operations for the City of Bexley
LEADS Compliance Manager	Dispatcher Sara Holley, LEADS Terminal Agency Coordinator	Individual directly responsible to the Agency Administrator for the compliant operation of LEADS
Department Representatives – IT	Lt Dawn Overly, Police Natalie Mullin, Rec Jordan Cavallaro, Service Robin Shetler, Building Natalie Vawter, Mayor's Office	Work directly with Security Manager and Information Systems Owner throughout the six steps of Incident Response.
Executive Management	Ben Kessler, Mayor	Incident Response Team reports to Management during an Incident and approves actions to be taken for containment and remediation.
Human Resources	Emily Buckley, Human Resources Coordinator	Work directly with Security Manager and Information Systems Owner to create internal and external messaging and determine who should be communicated to in which fashion under what timelines.

Definitions

1. Event

An event is an occurrence not yet assessed that may affect the performance of an information system and/or network. Examples of events include an unplanned system reboot, a system crash, and packet flooding within a network. Events sometimes provide indication that an incident is occurring or has occurred.

2. Incident

An incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Examples of security incidents include penetration of computer systems, spillages, exploitation of technical or administrative vulnerabilities, and introduction of computer viruses or other forms of malicious code.

Types of Incidents

The term "incident" encompasses the following general categories of adverse events:

Malicious Code: Malicious code attacks include attacks by programs such as viruses, Trojan horse programs, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity. Malicious code is particularly troublesome in that it is typically written to masquerade its presence and, thus, is often difficult to detect. Self-replicating malicious code such as viruses and worms can replicate rapidly, thereby making containment an especially difficult problem.

- **Virus Attack:** A virus is a variation of a Trojan horse. It is propagated via a triggering mechanism (e.g., event time) with a mission (e.g., delete files, corrupt data, send data). Often self-replicating, the malicious program segment may be stand-alone or may attach itself to an application program or other executable system component in an attempt to leave no obvious signs of its presence.
- **Worm Attack:** A computer worm is an unwanted, self-replicating autonomous process (or set of processes) that penetrates computers using automated hacking techniques. A worm spreads using communication channels between hosts. It is an independent program that replicates from machine to machine across network connections, often clogging networks and computer systems.
- **Trojan Horse Attack:** A Trojan horse is a useful and innocent program containing additional hidden code that allows unauthorized Computer Network Exploitation (CNE), falsification, or destruction of data.
- **Cryptoware Attack:** A cryptoware attack is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Business Email Compromise: Business email compromise occurs when a malicious actor gains access to a user's email account for the purposes of stealing information, money, or leveraging that account to gain access to other accounts.

Note: These categories of incidents are not necessarily mutually exclusive.

Incident Response

The City shall follow the Incident Response and Reporting Procedures specified in this IRP. To assure preparedness for an Incident, a copy of this Plan, along with supporting Procedures which should be followed to respond to and resolve Incidents, should be printed and kept in an accessible location in the event an Incident leaves the City's systems inaccessible.

Upon learning of an Incident or a data spillage, the Security Manager will take immediate steps intended to minimize further damage and/or regain custody of the information, material or mitigate damage to program security. Both the Security Manager and Executive Management have the authority to declare an incident.

Incident response will follow the subsequent six steps:

1. Preparation – One of the most important elements to a response plan is knowing how to use it once it is in place. Knowing how to respond to an incident before it occurs can save valuable time and effort in the long run.
2. Identification – Identify whether or not an incident has occurred. If one has occurred, the response team can take the appropriate actions.
3. Containment – When an incident occurs actions must be taken immediately to limit the scope and magnitude. Due to the fact that so many incidents observed currently involve malicious code, incidents can spread rapidly. This can cause massive destruction and loss of information. As soon as an incident is recognized, immediately begin working on containment.
4. Eradication – Removing the cause of the incident can be a difficult process. It can involve virus removal, conviction of perpetrators, or dismissing employees.
5. Recovery – Restoring a system to its normal business status is essential. Once a restore has been performed, it is also important to verify that the restore operation was successful and that the system is back to its normal condition and not vulnerable to a breach.
6. Follow-up – Some incidents require considerable time and effort. It is little wonder, then, that once the incident appears to be terminated there is little interest in devoting further effort to the incident. Performing follow-up activity is, however, one of the most critical activities in the response procedure. This follow-up can support any efforts to prosecute those who have broken the law. Follow-up provides a root-cause analysis and may also include modifications to City policies, changes to configurations to mitigate future risk, and/or changes to System Security Structure, including the selection of additional or different technology.

INCIDENT RESPONSE WORKSHEET

SECURITY INCIDENT REPORT SECTION 1 – PoC Information		
Report No.:		
Report Date:	Report Type (initial, final, status):	
Report Generated By:	Date:	Time:
Title:	Phone:	E-mail:
Signature:		
SECTION 2 – Incident Notification		
Incident Reported By:	Date:	Time:
Location:	Phone:	E-mail:
Signature:		
Security Manager Notified	Date:	Time:
Signature:		
Method of Notification:		
Security Team Notified	Date:	Time:
SECTION 3 – Incident Information		
Incident Type:	Time of Incident:	Ongoing?
Department:	Location:	
Affected Computer Systems (Hardware and/or Software):		
Impact to City Systems/protected data:		
Classification of Affected Computer Systems:		
Physical Location of Affected Systems:		
Connections of Affected Systems to Other Systems:		
Type of Incident (Malicious Code, Business Email Compromise (BEC) – please identify):		
Suspected Method of Intrusion/Attack:		
Suspected Perpetrators or Possible Motivations:		
Apparent Source (e.g., IP address) of Intrusion/Attack:		
Apparent Target/Goal of Intrusion/Attack:		
Mission Impact:	Success/Failure of Intrusion/Attack:	
Attach incident/compromise narrative, including technical details of incident thus far. Include as much as possible about the Detection and Identification, Containment, Eradication, and Recovery – steps taken (with date/time stamps), persons involved, files saved for analysis, etc.		

LEADS SECURITY INCIDENT RESPONSE FORM

BASED ON FBI CJIS DIVISION
INFORMATION SECURITY MANAGER (ISM)
SECURITY INCIDENT REPORTING FORM

NAME OF PERSON REPORTING THE INCIDENT: ______________________________

DATE OF REPORT: ____________________________ (mm/dd/yyyy)

DATE OF INCIDENT: __________________________ (mm/dd/yyyy)

POINT(S) OF CONTACT (Include Phone/Extension/Email): _________________________
____

LOCATION(S) OF INCIDENT: ____

INCIDENT DESCRIPTION: ____
____

SYSTEM(S) AFFECTED: ____
____

SYSTEM(S) AFFECTED (e.g. CAD, RMS, file server, etc.): ________________________
____

METHOD OF DETECTION:
____

ACTIONS TAKEN/RESOLUTION: ____
____
____
____
____
____
____

Copies To:

LEADS Security
1970 West Broad Street
Columbus OH 43223

(614) 466-3055
LEADSSecurity@dps.ohio.gov

INCIDENT RESPONSE PROCEDURES:

Overview:

When an alert or a call is received that identifies a potential Cybersecurity Event that has occurred to a user's workstation or system device, The IT team at the city will enact a series of steps that follow appropriate measures to respond to a Cybersecurity Event.

Those steps include:

1. Preparation
2. Identification
3. Containment

Then:

4. Eradication
5. Recovery

And as needed:

6. Follow-up

Malicious Code/Virus Attack Response Procedure

Identification and Initial Containment:

If an attack has been detected by a user on the system, or a user on the system suspects a virus attack, they should follow this procedure:

- Immediately remove network cable from system thought to be infected and/or turn off Wi-Fi access to the device.
- DO NOT Turn off the device.
- Notify the IT Department immediately by their Mobile phone at: (614) 657-4832.
- If contact is not able to be made to IT directly, notify the Helpdesk at (877) 490-2663

If an attack or suspected attack has been identified by the IT department's automated systems, the IT Department should be immediately notified via alerting. The IT Department should respond immediately as per the process below:

Containment Validation and Eradication Action Planning:

The IT Department will follow this procedure:

- **Follow the Respond To Malware | Virus Infection Procedure in the IT Runbook**
- Ensure the user has removed the affected device from the internet and network.
- Contact the reporting user to assess actions leading up to the attack.
- Send a text message to the Security Manager notifying them of the incident and its nature.
- Review all Security Support Structure for any evidence of the attack being more widespread.
- Scan the affected devices with approved Security Software.
- Take a backup of affected systems
- Change user passwords in all accounts across all platforms, not just the one affected.
- Review data systems to assure data is still intact.
- Report to the Security Manager and Information System Owner findings and action plan.
- Security Manager and Human Resources Department should meet to create messaging out to Organizational Partners, and potentially the Public, and determine if such communication is necessary, and if so, to whom, and under what timelines

Eradication and Recovery:

Depending on the nature of the attack and the number of systems effected, recovery procedures will vary. The IT Department, Security Manager, and Information System Owner should agree on a course of action and take action to recover swiftly. Documentation of actions taken is critical.

The response team will follow guidelines in the IT Operations run book for Incident Response - Eradication and Recovery.

In cases where a virus attack is widespread, or there is an incident of cryptoware, messaging to City Employees, Organizational Partners, and potentially the Public must be taken into consideration and prompt communication out to these stakeholders is vital during this time.

BEST PRACTICES IN RECOVERY:

- Thorough scans and manual assessment of the attack (attack TTP) should be assessed to determine point of entry, if there is a way to mitigate this risk in the future, and if it's possible there may be a latent compromise or persistent threat.

- Oftentimes, wiping and reinstalling the system and/or restoring from clean backups is a better way to assure the malicious actor has not left malware buried and undetected in the system.

- If a system connected to CJIS Information is involved in the Incident, notify the Incident to LEADS Control within 24 hours, complete, and return a LEADS Security Incident Response Form to the LEADS Security Team within 3 days' time.
  - Also consider: Reporting the incident within 72 hours through the Defense Industrial Base Cybersecurity Incident Reporting Portal (DIB-CS) https://dibnet.dod.mil/
  - Reporting the incident to the IC3 (Internet Crime Complaint Center) at https://www.ic3.gov

- In cases where the loss is high, notify the insurer that issued the Cyber Liability or Cyber Crime Policy.

- Ransomware incidents incurring losses over $50,000 should immediately be reported to the FBI.

Business Email Compromise Response Procedure

Identification and Initial Containment:

Business Email Compromise is sometimes identified by the affected user, but more often than not this attack is identified by internal or external users who receive a phishing message from the compromised account.

If an attack has been detected by a user on the system, the user on the system suspects an attack, or if anyone in the organization is alerted by an internal or external contact that there may be a business email compromise, they should follow this procedure:

Notify the IT Department immediately by phone at (614) 657-4832. If contact is not able to be made at this number, notify the Helpdesk at (877) 490-2663

Containment Validation and Eradication Action Planning:

The IT Department will follow this procedure:

- Send a text message to the Incident Response Team notifying them of the incident and its nature.
- Contact the reporting user to assess actions leading up to the attack.
- Review all Security Support Structure for any evidence of the attack being more widespread.
- Contact users whose email accounts may be compromised to notify them of actions to be taken.
- Follow the SOP on Evicting A Cyber Actor From Email Account.
- Change user passwords across all accounts, on all platforms, not just the affected one.
- Assess user access levels on the systems of the affected users to determine if there are vectors to leverage into additional services, accounts or data.
- Review data systems to assure data is still intact.
- Report to the Security Manager and Information System Owner findings and action.
- Security Manager and Human Resources Department should meet to create messaging out to Clients and Vendors and determine if such communication is necessary, and if so, to whom, and under what timelines.

Eradication and Recovery:

Depending on the nature of the attack and the number of accounts affected, recovery procedures will vary. The IT Department, Security Manager, and Information System Owner should agree on a course of action and take action to recover swiftly. Documentation of actions taken is critical.

The response team will follow guidelines in the IT Operations run book for the City of Bexley Incident Response – Malware Remediation.

Messaging City Employees, Organizational Partners, and potentially the Public must be taken into consideration and prompt communication out to these stakeholders is vital during this time.

BEST PRACTICES IN RECOVERY:

- Thorough scans and manual assessment of the attack (attack TTP) should be assessed to determine point of entry, if there is a way to mitigate this risk in the future, and if it's possible there may be a latent compromise or persistent threat.

- Oftentimes, wiping and reinstalling the system and/or restoring from clean backups is a better way to assure the malicious actor has not left malware buried and undetected in the system.

- If CJIS Information is involved in the Incident, notify the Incident to LEADS Control within 24 hours and complete and return a LEADS Security Incident Response Form to the LEADS Security Team within 3 days' time.
  - Also consider: Reporting the incident within 72 hours through the Defense Industrial Base Cybersecurity Incident Reporting Portal (DIB-CS) https://dibnet.dod.mil/
  - Reporting the incident to the IC3 (Internet Crime Complaint Center) at https://www.ic3.gov

- In cases where the loss is high, notify the insurer that issued the Cyber Liability or Cyber Crime Policy.

- Ransomware incidents incurring losses over $50,000 should immediately be reported to the FBI.

INCIDENT COMMUNICATION PLAN:

Initial Notification Process – Email Example

From: Affiliated Helpdesk <HelpDesk@aresgrp.com>
Sent: Monday, June 19, 2023 11:51 AM
To: Affiliated Helpdesk <HelpDesk@aresgrp.com>; Erik McGuiness
Cc:
Subject: RE: Severity 1 Notification: <City of Bexley> - <P&R Office Offline> Ticket #754202

Hi all,

According to IT Support incident notification procedures – We are sending out this notification of a severity one incident.

No response is required on your part – this is informational.

- Department
  - Parks & Recreation
- Incident Number - 754202
  - Assigned Resources
    - Erik McGuiness
    - Peter McCann
    - Jon Lynch
- Incident Description
  - Affiliated received notifications that the Parks and Rec office was reporting issues with locked files and workstations at 9:05 this morning.
- Next Steps
  - Initial work from support team identified potential security event/incident.
  - User has disconnected affected workstation form the internet (confirmed at 9:20).
  - Affiliated has engaged our security vendor (SP Partners)
  - An Affiliated engineer (Jon) is also scheduled to meet with Erik to address eradication planning at 9:45 .
  - **The network scans find only single user workstation involved – no PII affected.**
  - Jon is enroute now and should arrive shortly to finalize recovery plan for device and check results again for any other issues (11:35). Will update Erik when he arrives on site
- Next Update
  - An update will be provided once on-site diagnostics have been completed.

KC Fry

Service Manager

Internal Staff Communication Plan

Refer to Communication Plan Document

External Communication Plan

Refer to Communication Plan Document

Response Team Communication Plan

Refer to Communication Plan Document

Breach Notification Plan

Refer to Communication Plan Document

Incident Response Report

- Malware/Ransomware
- Business Email Compromise

Incident Response Plan Team & Contacts

Roles & Assigned	Contact Information		
Information Systems Owner	City of Bexley	559 N Cassingham Rd Bexley, OH 43209	(614) 559-4459
Gary Lewis, Chief of Police	(614) 551-4963	mayor@bexley.org	
Security Manager	City of Bexley	2242 E Main St Bexley, OH 43209	(614) 559-4285
Erik McGuinness, IT Manager	(614) 657-4832	it@bexley.org	
IT Department Representative	City of Bexley	2242 E Main St Bexley, OH 43209	(614) 559-4285
Erik McGuinness, IT Manager	(614) 657-4832	it@bexley.org	
IT Services Partner	Affiliated	5700 Perimeter drive Dublin, Ohio	(614) 339-0388
24/7/365 Helpdesk	(877) 490-2663	helpdesk@aresgrp.com	
Management	City of Bexley	2242 E Main St Bexley, OH 43209	(614) 559-4200
Ben Kessler, Mayor	(614) 397-3554	glewis@bexley.org	
Human Resources	City of Bexley	2242 E Main St Bexley, OH 43209	(614) 559-4255
Emily Buckley	(641) 521-7282	ebuckley@bexley.org	
Communications	City of Bexley	2242 E Main St Bexley, OH 43209	(614) 559-4210
Ben Kessler, Mayor	(614) 397-3554	mayor@bexley.org	
LEADS TAC	Bexley Police Department	559 N Cassingham Rd Bexley, OH 43209	(614) 559-4444
Sara Holley		bhanna@bexley.org	
Insurance Broker/Carrier	USI Insurance Services	5455 Rings Road, Suite 250 Dublin, OH 43017	(614) 340-6155
Joey Machuga, Commercial Lines Account Manager	(330) 718-9176	joey.machuga@usi.com	[POLICY #]
Joshua Furci, Vice President	(614) 530-2720	josh.furci@usi.com	[POLICY #]

Local FBI Office	Federal Bureau of Investigation	2012 Ronald Reagan Drive Cincinnati, OH 45236	(513) 421-4310

ASSETS/SYSTEMS TO BE PROTECTED

Please refer to Datto RMM list of IT Assets

Appendix A - IT SECURITY AND OPERATIONS POLICIES

The City has implemented a series of polices and procedures to protect the City's data and systems from unauthorized access and malicious activities. The following is a partial list of some of the policies implemented. Procedures created to address the IT Security and Operations Polices are maintained in the IT Department Operations Run Book.

LEADS System Use and Management Policy

The Bexley Police Department utilizes the LEADS system to support Law Enforcement in the City of Bexley. The City will maintain and manage access to and management of systems utilizing LEADS data. Systems that access, store, and manage from LEADS will act in accordance with specific set of policies defined as the LEADS policies and procedures that are adopted and enforced by the City's Police Department and IT department. Specific details are managed in the Bexley Police Department Manual, Policy 807.

Annual Assessment Of Risk

Policy: The City of Bexley will perform (using a 3rd party**) a**n Annual Risk Analysis/Assessment of our Information Systems and IT assets that involves identifying risk and vulnerabilities in our Information Systems. To do this we will conduct an accurate and thorough assessment of the potential threats and vulnerabilities to the confidentiality, integrity and availability of systems and data at our facilities, stored in the cloud, and used by our staff.

After an analysis of our Annual Risk Assessment, we will reduce the risks and vulnerabilities to an appropriate and reasonable level or to the greatest extent possible through ongoing management. The Risk Analysis will be performed following industry best practice standards as described in the NIST Cybersecurity framework and other appropriate industry or state mandated frameworks.

In addition, an abbreviated form of the Risk Assessment called a Risk Profile will be performed quarterly to identify and prioritize risks to data breaches and threats from unauthorized access that could negatively impact our productivity. This will occur on an ongoing basis using automated tools and checked by the Security Officer regularly.

Risk Management Strategy Plan

Policy: Once The City has completed the Risk Analysis/Assessment process for the IT systems and assets, the next step is Risk Management. Risk Management includes the implementation of security measures designed to reduce risk to reasonable and appropriate levels to, among other things, ensure the confidentiality, availability and integrity of our data and protect against any reasonably anticipated threats, hazards, or disruptions of access or availability of our systems by our staff for the performance of their duties.

The first step in the Risk Management process should be to develop and implement a Risk Management Plan. The purpose of a Risk Management Plan is to provide structure for the evaluation, prioritization, and implementation of risk-reducing measures and controls. The risk prioritization and mitigation decisions will be determined by answering which controls and measures should be implemented and the priority in which they should be addressed based upon their risk score.

The implementation component of the Risk Management Plan may vary based on the circumstance. Compliance with the security policy rules created and implemented requires financial resources, management commitment, and staff involvement. Cost is one of the factors we must consider when determining measures and controls to mitigate a vulnerability. However, cost alone is not a valid reason for choosing not to implement security measures that are reasonable and appropriate. The output of this step is a Risk Management Plan that contains prioritized risks, options for mitigation of those risks, and a plan for implementation. The plan will guide our actual implementation of security measures to reduce risks to our systems and data (“our systems”) to reasonable and appropriate levels.

The final step in the Risk Management process is to continue evaluating and monitoring the risk mitigation measures implemented. Risk Analysis and Risk Management are not one-time activities. Risk Analysis and Risk Management are ongoing, dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The Risk Analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated Risk Analysis will be an input to the Risk Management processes to reduce newly identified or updated risk levels to reasonable and appropriate levels.

Access Controls

Policy: The City of Bexley will implement access controls to protect access to the City’s systems, applications, and data.

The Controls will be Policies that will at a minimum, cover:

1. Unique User Id’s for each user and privileged account
2. A Password and Password Management Policy/Process
3. Multi-Factor Authentication as a second layer of validation for accessing the City’s systems
4. The Policy of Least Access – providing users with access to only the systems they need access to use to perform their duties.
5. A Termination Policy to ensure that when a staff member leaves the City’s employment, their access is deactivated in a complete and timely manner.

Password And Password Management

Policy: The City Of Bexley will require the use of passwords to access all the City’s IT systems. The policy in put in place to ensure access to all systems, including those maintained in the cloud are protected and tracked. The following password and credential management:

- All passwords must be changed at least once every 90 days.
- All production system-level passwords must be part of the Security Officer’s administered global password management database.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

Users must select strong passwords. Further, systems that authenticate must require passwords of users and must block access to accounts if more than three unsuccessful attempts are made.

City employees are also required to follow specific guidelines for the creation and use of their passwords; those guidelines will be managed and provided by the IT department and Information Security Manager.

Multi-Factor Authentication

Policy: The City of Bexley requires several controls over access to the systems used in the City of Bexley technology stack. An additional level of access control will be to require Multi-factor Authentication (MFA) procedures for each user for system access, access to their cloud-based email systems, and for IT administration of systems and devices in our technology environment.

"Least Access" Rules For Access

Policy: The City of Bexley will implement technical policies and procedures that allow only authorized persons to access the City's systems, applications, and data. These access controls will include:

1. ***Unique user identification.*** The City's IT department must assign a unique user name for identifying and tracking each employee's user identity in the City's systems.
2. ***Access control and validation procedures.*** The City's IT department will implement procedures to control and validate a staff member's access to systems, applications, and data based on their role or function, and control of access to software programs for testing and revision.

Process For Termination of Staff Access

Policy: It is important that any termination of a City employee member immediately results in both the Human Resources (HR) and the Information Technology (IT) departments quickly coordinating their activities to ensure:

a. Access to all systems and applications is revoked
b. The staff member is removed from any systems or applications (including all cloud and phone systems)
c. All digital certificates are revoked
d. Any tokens or smart cards issued to the staff member are returned
e. Any keys and IDs provided to the staff member during their employment are returned
f. HR must conduct an exit interview and document any issues or concerns related to the staff member.

Validation should be performed monthly to ensure only active employees have access to the City's IT systems and facilities.

Protection Against Malicious Code/Virus Software

Policy: The City of Bexley will deploy malicious software/virus checking programs at the perimeter (edge) of the network and on individual end-user systems and servers. We will subscribe to receiving and deploying updates to malicious software checking programs as those updates are released by the tool vendor.

The City will require installation of operating system and third-party application updates (patches) and keep them current or both standard and security patches. The City will maintain a detailed set of procedures for the application, management, and validation that the security patches are applied to devices (workstations and servers) within a specific, timely manner.

Backup Management For Systems And Data

Policy: The City of Bexley, to be prepared for emergencies and to ensure smooth recovery from emergencies, will implement a backup process to protect their systems – including Operating Systems, Applications, and Data for the City's servers. The City IT department will evaluate, test, and update backup, as needed. Expectations of Plan include at least a daily backup of all contents of the City's servers to be used for IT operations restoration; an offsite encrypted copy of all contents of the City's servers, stored for up to 365 days of backups. These backups will also have regular test restores and validation to ensure the information is available when needed. Details of the Backup process will be defined and maintained in the IT department's IT Operations Run Book.

Data Protection

Policy: The City of Bexley will implement reasonable and appropriate measures to guard against unauthorized access to and protect the integrity and confidentiality of Protected Information that is transmitted over an electronic communications network. Such measures will ensure Protected Information has not been modified without authorization, or corrupted, without detection during transmission.

Measures to Ensure Protected Information is Not Improperly Modified Without Detection Until Disposed of:

1. The City of Bexley will ensure that wired and wireless transmission of Protected Information will utilize secure protocols (encryption).
2. The City of Bexley will require that all remote access to Protected Information be by secure means only.
3. The City of Bexley will prohibit sending of unprotected Protected Information by unencrypted email.
4. The City of Bexley will consider the mandating of Virtual Private Network (VPN) for all remote users.
5. The City of Bexley will ensure that employees delete or redact Protected Information from the body of received email before replying to it.

Appendix B – INCIDENT RESPONSE TRAINING

All City employees who have a role in Incident Response will receive incident response training at least annually, and a record of the training will be maintained. This training can be integrated into the overall program-specific annual security awareness training. One of the most impactful methods of training on incident response is through Tabletop Exercises.

Tabletop Exercises

Tabletop exercises are discussion-based events where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation.

Tabletop exercises are conducted in an informal environment, with a facilitator guiding participants through a discussion designed to meet pre-defined objectives. One or more scenarios may be discussed during a single tabletop exercise. Tabletop exercises are cost-effective tools designed to validate the content of IT plans, such as contingency plans and incident response plans, and to ensure that plan content is viable and implementable in an emergency situation.

This section provides a list of general questions that apply to virtually all scenarios.

Results of tabletop exercises may be used to amend response procedures. Once changes have been approved, all members of the Incident Response Team should be updated on them. Tabletop exercises, discussion and outcomes should be documented on the Tabletop Exercise Worksheet.

Incident Handling Scenarios

[reproduced and adapted here from NIST SP 800-62r2]

Incident handling scenarios provide an inexpensive and effective way to build incident response skills and identify potential issues with incident response processes. The incident response team members are presented with a scenario and a list of related questions.

The team then discusses each question and determines the most likely answer. The goal is to determine what the team would really do and to compare that with policies, procedures, and generally recommended practices to identify discrepancies or deficiencies.

For example, the answer to one question may indicate that the response would be delayed because the team lacks a piece of software or because another team does not provide off-hours support.

Scenario Questions

Preparation:

- Would the City consider this activity to be an incident? If so, which of The City's policies does this activity violate?
- What measures are in place to attempt to prevent this type of incident from occurring or to limit its impact?

Detection and Analysis:

- What precursors of the incident, if any, might The City detect? Would any precursors cause the City to respond before the incident occurred?
- What indicators of the incident might The City detect? Which indicators would cause someone to think that an incident might have occurred?
- What additional tools might be needed to detect this incident?
- How would the incident response team analyze and validate this incident? What personnel would be involved in the analysis and validation process?
- To which people and groups within the City would the team report the incident?
- How would the team prioritize the handling of this incident?

Containment, Eradication, and Recovery:

- What strategy should the City take to contain the incident? Why is this strategy preferable to others?
- What could have happened if the incident were not contained?
- What additional tools might be needed to respond to this incident?
- Which personnel would be involved in the containment, eradication, and/or recovery processes?
- What sources of evidence, if any, should the City acquire? How would the evidence be acquired? Where would it be stored? How long should it be retained?

Post-Incident Activity:

- Who would attend the 'lessons learned' meeting regarding this incident?
- What could be done to prevent similar incidents from occurring in the future?
- What could be done to improve detection of similar incidents?

General Questions:

- How many incident response team members would participate in handling this incident?
- Besides the incident response team, what groups within the City would be involved in handling this incident?
- To which external parties would the team report the incident? When would each report occur? How would each report be made? What information would you report or not report, and why?
- What other communications with external parties may occur?
- What tools and resources would the team use in handling this incident?
- What aspects of the handling would have been different if the incident had occurred at a different day and time (on-hours versus off-hours)?
- What aspects of the handling would have been different if the incident had occurred at a different physical location (onsite versus offsite)?

Scenarios

Scenario 1: Worm and Distributed Denial of Service (DDoS) Agent Infestation

On a Tuesday morning, a new worm is released; it spreads itself through removable media, and it can copy itself to open Windows shares. When the worm infects a host, it installs a DDoS agent. The City has already incurred widespread infections before antivirus signatures become available several hours after the worm started to spread.

The following are additional questions for this scenario:

- How would the incident response team identify all infected hosts?
- How would the City attempt to prevent the worm from entering the network before antivirus signatures were released?
- How would the City attempt to prevent the worm from being spread by infected hosts before antivirus signatures were released?
- Would the City attempt to patch all vulnerable machines? If so, how would this be done?
- How would the handling of this incident change if infected hosts that had received the DDoS agent had been configured to attack another organization's website the next morning?
- How would the handling of this incident change if one or more of the infected hosts contained sensitive personally identifiable information regarding City employees?
- How would the incident response team keep The City users informed about the status of the incident?
- What additional measures would the team perform for hosts that are not currently connected to the network (e.g., staff members on vacation, offsite employees who connect occasionally)?

Scenario 2: Stolen Documents

On a Monday morning, the City's legal department receives a call from the Federal Bureau of Investigation (FBI) regarding some suspicious activity involving City systems. Later that day, an FBI agent meets with members of management and the legal department to discuss the activity. The FBI has been investigating activity involving public posting of sensitive government documents, and some of the documents reportedly belong to the City. The agent asks for the City's assistance, and management asks for the incident response team's assistance in acquiring the necessary evidence to determine if these documents are legitimate and how they might have been leaked.

The following are additional questions for this scenario:

- From what sources might the incident response team gather evidence?
- What would the team do to keep the investigation confidential?
- How would the handling of this incident change if the team identified an internal host responsible for the leaks?
- How would the handling of this incident change if the team found a rootkit installed on the internal host responsible for the leaks?

Scenario 3: Compromised Database Server

On a Tuesday night, a database administrator performs some off-hours maintenance on several production database servers. The administrator notices some unfamiliar and unusual directory names on one of the servers. After reviewing the directory listings and viewing some of the files, the administrator concludes that the server has been attacked and calls the incident response team for assistance. The team's investigation determines that the attacker successfully gained root access to the server six weeks ago.

The following are additional questions for this scenario:

- What sources might the team use to determine when the compromise occurred?
- How would the handling of this incident change if the team found that the database server had been running a packet sniffer and capturing passwords from the network?
- How would the handling of this incident change if the team found that the server was running a process that would copy a database containing sensitive customer information (including personally identifiable information) each night and transfer it to an external address?
- How would the handling of this incident change if the team discovered a rootkit on the server?

Scenario 4: Unknown Exfiltration

On a Sunday night, one of the City's network intrusion detection sensors alerts on anomalous outbound network activity involving large file transfers. The intrusion analyst reviews the alerts; it appears that thousands of .RAR files are being copied from an internal host to an external host, and the external host is located in another country. The analyst contacts the incident response team so that it can investigate the activity further. The team is unable to see what the .RAR files hold because their contents are encrypted. Analysis of the internal host containing the .RAR files shows signs of a bot installation.

The following are additional questions for this scenario:

- How would the team determine what was most likely inside the .RAR files? Which other teams might assist the incident response team?
- If the incident response team determined that the initial compromise had been performed through a wireless network card in the internal host, how would the team further investigate this activity?
- If the incident response team determined that the internal host was being used to stage sensitive files from other hosts within the enterprise, how would the team further investigate this activity?

Scenario 5: Unauthorized Access to Payroll Records

On a Wednesday evening, the City's Police Department receives a call from a payroll administrator who saw an unknown person leave their office, run down the hallway, and exit the building. The administrator had left her workstation unlocked and unattended for only a few minutes. The payroll program is still logged in and on the main menu, as it was when she left it, but the administrator notices that the mouse appears to have been moved. The incident response team has been asked to acquire evidence related to the incident and to determine what actions were performed.

The following are additional questions for this scenario:

- How would the team determine what actions had been performed?
- How would the handling of this incident differ if the payroll administrator had recognized the person leaving her office as a former payroll department employee?
- How would the handling of this incident differ if the team had reason to believe that the person was a current employee?
- How would the handling of this incident differ if the physical security team determined that the person had used social engineering techniques to gain physical access to the building?
- How would the handling of this incident differ if logs from the previous week showed an unusually large number of failed remote login attempts using the payroll administrator's user ID?
- How would the handling of this incident differ if the incident response team discovered that a keystroke logger was installed on the computer two weeks earlier?

Scenario 6: Disappearing Host

On a Thursday afternoon, a network intrusion detection sensor records vulnerability scanning activity directed at internal hosts that is being generated by an internal IP address. Because the intrusion detection analyst is unaware of any authorized, scheduled vulnerability scanning activity, she reports the activity to the incident response team. When the team begins the analysis, it discovers that the activity has stopped and that there is no longer a host using the IP address.

The following are additional questions for this scenario:

- What data sources might contain information regarding the identity of the vulnerability scanning host?
- How would the team identify who had been performing the vulnerability scans?
- How would the handling of this incident differ if the vulnerability scanning were directed at the City's most critical hosts?
- How would the handling of this incident differ if the vulnerability scanning were directed at external hosts?
- How would the handling of this incident differ if the internal IP address was associated with the City's wireless guest network?
- How would the handling of this incident differ if the physical security staff discovered that someone had broken into the facility half an hour before the vulnerability scanning occurred?

Scenario 7: Remote Worker Compromise

On a Saturday night, network intrusion detection software records an inbound connection originating from a watchlist IP address. The intrusion detection analyst determines that the connection is being made to the City's VPN service and contacts the incident response team. The team reviews the intrusion detection, firewall, and VPN service logs and identifies the user ID that was authenticated for the session and the name of the user associated with the user ID.

The following are additional questions for this scenario:

- What should the team's next step be (e.g., calling the user at home, disabling the user ID, disconnecting the VPN session)? Why should this step be performed first? What step should be performed second?

- How would the handling of this incident differ if the external IP address belonged to an open proxy?
- How would the handling of this incident differ if the ID had been used to initiate VPN connections from several external IP addresses without the knowledge of the user?
- Suppose that the identified user's computer had become compromised by a game containing a Trojan horse that was downloaded by a family member. How would this affect the team's analysis of the incident? How would this affect evidence gathering and handling? What should the team do in terms of eradicating the incident from the user's computer?
- Suppose that the user installed antivirus software and determined that the Trojan horse had included a keystroke logger. How would this affect the handling of the incident? How would this affect the handling of the incident if the user were a system administrator? How would this affect the handling of the incident if the user were a high-ranking executive at The City?

Scenario 8: Anonymous Threat

On a Thursday afternoon, The City's physical security team receives a call from an IT manager, reporting that two of their employees just received anonymous threats against The City systems. Based on an investigation, the physical security team believes that the threats should be taken seriously and notifies the appropriate internal teams, including the incident response team.

The following are additional questions for this scenario:

What should the incident response team do differently, if anything, in response to the notification of the threats?

What impact could heightened physical security controls have on the team's responses to incidents?

Scenario 9: Unknown Wireless Access Point

On a Monday morning, The City's IT department receives calls from three users on the same floor of a building who state that they are having problems with their wireless access. A network administrator who is asked to assist in resolving the problem brings a laptop with wireless access to the users' floor. As he views his wireless networking configuration, he notices that there is a new access point listed as being available. He checks with his teammates and determines that this access point was not deployed by his team, so it is most likely a rogue wireless access with an unidentifiable owner.

The following are additional questions for this scenario:

- How do we determine if the access point is internal and connected to the network, being broadcast from inside the facility but not connected to the network, or being broadcast outside the facility with range inside the facility?
- What should be the first major step in handling this incident (e.g., physically finding the rogue access point, logically attaching to the access point)?
- What is the fastest way to locate the access point? What is the most covert way to locate the access point?
- How would the handling of this incident differ if the access point had been deployed by an external party (e.g., contractor) temporarily working at The City offices?
- How would the handling of this incident differ if an intrusion detection analyst reported

signs of suspicious activity involving some of the workstations on the same floor of the building?

- How would the handling of this incident differ if the access point had been removed while the team was still attempting to physically locate it.