THE CITY OF BLUE ISLAND
COOK COUNTY, ILLINOIS

RESOLUTION
NUMBER 2022- 048

A RESOLUTION OF THE CITY OF BLUE ISLAND, COOK COUNTY, ILLINOIS, TO AUTHORIZE AND APPROVE CITY OF BLUE ISLAND COMPUTER AND NETWORK POLICIES AND PROCEDURES

FRED BILOTTO, Mayor
RAEANN CANTELO-ZYLMAN, City Clerk
JAIRO FRAUSTO, City Treasurer

DEXTER JOHNSON
LUIZ MONTOYA
NANCY RITA
BILL FAHRENWALD
GABRIEL McGEE
CANDACE CARR
JOSH ROLL

Alderman

Published in pamphlet form by authority of the Mayor and City Clerk of the City of Blue Island on 10/25/22
City of Blue Island – 13051 Greenwood Avenue, Blue Island, IL 60406

RESOLUTION NUMBER 2022-048

A RESOLUTION OF THE CITY OF BLUE ISLAND, COOK COUNTY, ILLINOIS, TO AUTHORIZE AND APPROVE CITY OF BLUE ISLAND COMPUTER AND NETWORK POLICIES AND PROCEDURES

WHEREAS, the City of Blue Island, Cook County, Illinois (the *"City"*) is a duly organized and existing City created under the provisions of the laws of the State of Illinois and operating under the provisions of the Illinois Municipal Code, and all laws amendatory thereof and supplementary thereto, with full powers to enact ordinances and adopt resolutions for the benefits of the residents of the City; and

WHEREAS, the City of Blue Island desires to implement policies and procedures for computer and network usage for City operations, a copy of which is attached hereto and made a part hereof as Exhibit A (the "*Policies*"); and

WHEREAS, the Mayor and Aldermen of the City deem it advisable and in the best interest of the health, safety and welfare of the residents of the City to implement the Policy.

NOW, THEREFORE, BE IT RESOLVED by the Mayor and the Aldermen of the City of Blue Island, Cook County, Illinois as follows:

Section 1. That the above recitals and legislative findings are found to be true and correct and are hereby incorporated herein and made a part hereof, as if fully set forth in their entirety.

Section 2. The Policies, which are attached hereto and made a part hereof as Exhibit A, are hereby approved in substantially the same form presented to the Mayor and Aldermen of the City with such necessary non-material changes as may be authorized by the Mayor and City Attorney.

Section 3. The officials and officers of the City are hereby authorized to undertake actions on the part of the City as contained in the Policies to complete satisfaction of the provisions, terms or conditions stated therein.

Section 4. If any section, paragraph, clause or provision of this Resolution shall be held invalid, the invalidity thereof shall not affect any other provision of this Resolution.

Section 5. All ordinances, resolutions, motions or orders in conflict with this Resolution are hereby repealed to the extent of such conflict.

Section 6. This Resolution shall be in full force and effect immediately upon its passage, approval, and publication as required by law.

(*Left intentionally blank*)

ADOPTED this **25th** day of **October, 2022,** pursuant to roll call as follows:

	YES	NO	ABSENT	PRESENT	ABSTAIN
Alderman JOHNSON			**X**		
Alderman FAHRENWALD	**X**				
Alderman RITA	**X**				
Alderman MONTOYA	**X**				
Alderman MCGEE			**X**		
Alderman CARR	**X**				
Alderman ROLL	**X**				
Mayor BILOTTO					
	5		**2**		

APPROVED by the Mayor on **October 25, 2022.**

FRED BILOTTO
MAYOR OF THE CITY OF BLUE ISLAND,
COUNTY OF COOK AND STATE OF ILLINOIS

ATTESTED and Filed in my office this
25th day of **OCTOBER, 2022.**

RAEANN CANTELO-ZYLMAN, CITY CLERK

STATE OF ILLINOIS)
) ss.
COUNTY OF COOK)

CERTIFICATION

I, RAEANN CANTELO-ZYLMAN, DO HEREBY CERTIFY THAT I am the duly elected City Clerk of the City of Blue Island, Illinois, as such City Clerk, I am the keeper of the minutes and records of the Proceedings of the City Council of the said City and have in my custody the RESOLUTIONS and BOOKS of the records of said City.

I DO FURTHER CERTIFY that the attached and foregoing is a true and correct copy of the certain **RESOLUTION: A RESOLUTION OF THE CITY OF BLUE ISLAND, COOK COUNTY, ILLINOIS, TO AUTHORIZE AND APPROVE CITY OF BLUE ISLAND COMPUTER AND NETWORK POLICIES AND PROCEDURES.**

RESOLUTION NO. 2022-048 which was adopted at a regular meeting of the City Council of the City of Blue Island, Illinois held on the **25th day of October, 2022**; that at said meeting **5** Alderman were present; that at said meeting, on motion duly made and seconded that the Resolution did pass and on the roll being called the vote of each Aldermen present on the question of the passage of said Resolution was duly and separately taken by Ayes and Nays and their names and votes recorded in the minutes of **5** Alderman voted Aye and **0** Alderman voted Nay and **0** Alderman voted Abstain and **2** Alderman Absent.

I DO FURTHER CERTIFY that the original Resolution which the foregoing is a true copy, is entrusted to my care for safe keeping, and that I am the lawful keeper of the same.

IN WITNESS WHEREOF, I have hereunto set my hand and affixed the Corporate Seal of the City of Blue Island aforesaid, at the said City in the County and State aforesaid, this **25th** day of **October, 2022**.

CORPORATE SEAL

Raeann Cantelo Zylman

City Clerk

Exhibit A

Computer and Network Policies
(see attached)

CITY OF BLUE ISLAND

COMPUTER and NETWORK POLICIES AND PROCEDURES

OCTOBER 2022

- Network Security Policies and Procedures
- Appropriate use of Computer Network Resource policy
- Internet Content Filtering Policy
- Data Backup Policy
- Network Connection Policy
- New Software Request Policy
- Password Policy
- Incident Response Policy

CITY OF BLUE ISLAND

18 35

Information Technology

Network Security Policies and Procedures

Table of Contents

Intro

The City of Blue Island looks to enhance constituent support and service through a secure, reliable network of data systems. These systems are interconnected via network switches, routers, and firewalls that allow for proper access to City information stored on multiple file servers, in databases and in cloud storage entities. The goal is to maintain all of these components, including backup devices and supported client devices, utilizing a manner consistent with industry standards and best practices. Through employing industry best practices that are reinforced by processes, the Information Technology Department (IT) strives to support the availability of the City's data and technology resources.

Purpose

The purpose of this document is to establish policies, processes, and procedures for maintaining and securing data within enterprise network. These policies provide an enforceable governance model around how the City's network is managed and maintained to keep data secure and accessible.

This endeavor is truly a partnership, and we are all one team, as all parties involved have a significant stake and responsibility to comply with all agreed-upon policies and procedures to ensure the highest level of security. A single breach, whether from the largest server to an individual user, could compromise the confidential data or create a significant loss of information. Malicious applications, viruses, malware, and ransomware can be inadvertently or deliberately run on a device and cause the destruction or disruption of service to others on the network. The IT Department is constantly working to reinforce systems against such attacks, and to implement services to screen out viruses and other debilitating rogue software. However, it is still up to each individual user to comply with all revisions to published policies and procedures. All network users should follow the security mantra, "risk assumed by one is shared by all."

Scope

These policies and procedures cover all City of Blue Island network resources and associated data.

User Responsibility

Each employee is entirely responsible for their user ID and password and should not share them with anyone else. Employees should also use best practices in protecting their user ID and password. Storing ID's and password on sticky notes under keyboards, in desk drawers or tape to one's monitor is not acceptable.

Consequences for Non-Compliance

Any employee found to have violated any of these policies may be subject to disciplinary action, up to and including termination of employment.

Revision Process

Providing network security is an ongoing refinement process as situations change and new vulnerabilities develop. The IT Department will conduct a review of this document and make revisions, as necessary.

Acceptable Use Policy

Data Privacy

All electronic data, including communications, transmitted, or stored on City network systems remain the property of the City of Blue Island. The City retains the right to access, inspect, monitor, or disclose any material transmitted or received on its network systems, including information downloaded from the internet, or received or sent via email. This does include mobile devices owned by the City of Blue Island.

Incidental Personal Use

Incidental personal use of City computer resources is outlined in the City of Blue Island ***Appropriate Use of Computer Network Resources Policy*** outlines the guidelines for the use of computer resources for incidental personal use.

Internet and/or Email Usage

Internet and email usage is governed by the City of Blue Island ***Appropriate Use of Computer Network Resources Policy.***

All incoming email attachments will be scanned using virus scanning software and those that may be infected, or pose a threat of being infected, will be quarantined if caught.

Internet Content Filtering

The City of Blue Island ***Internet Content Filtering Policy*** outlines the internet filtering security protocols for the City network.

Ownership of Network, PC, and Data Resources

All hardware and software are the property of the City of Blue Island. All workstations, telephones, servers, and other networking devices must be approved by the IT Department, before being connected anywhere on the network.

Privacy Rights Waiver

Employees should not expect privacy with respect to information transmitted, received, or stored on the City's network resources. By accessing the City of Blue Island network, the employee authorizes the City to access, inspect, monitor, and disclose material. IT will never ask for employees' passwords.

Usage Prohibitions and Restrictions

Computer resource usage prohibitions and restrictions are outlined in the City of Blue Island ***Appropriate Use of Computer Network Resources Policy***.

Network Infrastructure

Backup Systems

The City of Blue Island ***Backup Systems Policy*** outlines the standards of backing up files on the network for the purpose to be able to restore information in the event of a disaster or incident.

File Storage

Files that need to be shared by multiple employees or with other City agencies, or need to be stored in a secure, disaster resistant environment, should be written to one of our network file servers. Usually, these file servers are annotated by a drive letter of "F:" or higher.

A "user" directory will be maintained for each user account on a network file server and access to this directory will be exclusive to the user.

On each file server resides a common directory as an ideal place to temporarily store files that need to be shared between departments. Full rights to all employees have been granted for this directory, so it is important that no sensitive information is stored in this directory at any time.

All sensitive information should be stored in a secure area of the file server for which only those employees who are authorized have access. If an area does not already exist on the network that is suitable to store this sensitive information, the department authorized contact (Department Head) may request to have this structure created through the Help Desk.

Virtual Private Network (VPN)

Approved City employees and authorized third parties (e.g., vendors, etc.) may utilize the benefits of VPNs, which are classified as an "IT Department - managed" service. With approval from City Administration & Department Head, IT may install the VPN Software on only City issued devices. Further details may be found in the City of Blue Island ***Network Connection Policy***.

Additionally, the following should be noted on VPNs:

- It is the responsibility of employees to ensure that unauthorized users are not allowed access to City internal networks.
- When actively connected to the City of Blue Island network, VPNs will force all traffic to and from the PC over the VPN tunnel. All other traffic will be dropped.
- Gateways will be set up and managed by the IT Department.
- All computers must use up-to-date anti-virus software.
- All computers must have the most current operating system security patches applied.

- All City employees must use a City-owned laptop and have a business need to access the City's internal network via VPN.
- Only City-approved VPN clients may be used.

Wireless Communication

Includes all wireless communication devices capable of transmitting packet data (e.g., personal computers, wireless phones, smart phones, etc.) connected to any of the City's internal networks. Wireless devices and/or networks without any connectivity to the City's networks do not fall under the purview of this policy.

All point-to-point (building-to-building) wireless devices must use City-approved vendor products and security configurations. A data encryption method, which meets or exceeds the IT standard, is required.

All wireless access points and base stations must be registered and approved by IT. All wireless network interface cards (NIC) (i.e., PC cards) used in City devices must be registered and approved by IT. If a mobile device contains both a LAN NIC and wireless NIC, the wireless NIC must be disabled while the device is connected to the internal network via the LAN NIC.

Workstations

Only workstations approved and setup by IT may be connected to the City network. The Help Desk is responsible for deploying patches to workstations on a monthly basis. All workstations must comply, at a minimum, with standard workstation types and configurations established by IT.

All software running on City workstations must be properly licensed, and any new software must follow the ***New Software Request Policy Procedure***.

Network Security

Formal IT Permissions Approval

Written approval from an authorized department head must be attained and approved by the City Administrator to add new network accounts and/or devices, grant network file rights, search archived emails, or install new application software on a work device.

Physical Security

Every City employee is responsible for maintaining physical security in City offices. While the need for physical security is obvious for locations such as the network operation centers, other areas are just as sensitive. There is valuable equipment on desks and other storage areas, and there is sensitive business information on desks and laptops. Even how we handle disposing of sensitive materials has an effect on our physical security. Employees also carry valuable information and equipment with them – laptops, smart phones, and customer hardware.

City-owned work areas

- When stepping away from your computer workstation (either in a City office or elsewhere), lock the console of your workstation.

Conference rooms

Wireless access points in all conference rooms will be located on a network separate from the internal City network, but still behind a firewall. If City employees need to access the internal network from a conference network connection, they must use the private (not public) network. In the event you have guests, vendors, etc... IT will provide guest credentials for just internet connectivity outside of the internal network.

Portable devices

City employees traveling with computer hardware – laptops, smart phones, tablets – should take steps to minimize the likelihood of theft or loss. For example: encryption software and hardware must be used to secure sensitive data on traveling computers. Always keep your bags with you.

Primary and secondary Network Operations Centers

- No food or beverages are allowed in any of the Network Operations Centers.
- All doors to the Network Operations / Server Room must remain closed and locked.
- Access to any of the Network Operations / Server Room is restricted to authorized personnel only.
- All Network Operation / Server Room must be kept in an orderly and professional manner.

User IDs and Passwords

Individual user accounts and passwords are issued to create security for the systems and data belonging to the City. The purpose of a user ID and password is to secure against unauthorized access to the City's network systems or confidential data. User IDs and passwords must conform to the following criteria:

- Every customer must use a unique user ID that is associated with their name alone (i.e., no generic/shared user IDs are allowed).
- Network user IDs must follow the City's standard naming conventions for network login names.
- City staff should not share their password with anyone. If an instance arises where someone requires access to another person's files, an authorized contact in the owner agency should contact the Help Desk to request a change in access rights for the account.
    - If an employee forgets their password, they should contact the Help Desk to request that a new, temporary password be assigned. The Help Desk will assign a new short-term password that will expire upon the user's next network login and prompt the user to change their password.

- Passwords must meet or exceed the following rules in accordance with the City of Blue Island's Password Policy:
    1. Must be at least 7 characters.
    2. Must have a minimum of (1) uppercase letter.
    3. Must have a minimum of (1) lowercase letter
    4. Must have a minimum of (1) number
    5. Must have a minimum of (1) special character (E.g. !@#$%).

Password Reset

Password will expire every (42) days.
All password reset requests must be initiated by supervisor/manager via email to Help Desk.
After receiving temporary password user will be required to reset password upon initial login.

CITY OF BLUE ISLAND

Appropriate Use of Computer Network Resources Policy

Purpose: The City of Blue Island computer network provides mission critical application, telephone, data, and storage services to first responders and all other City agencies. These network resources have become an invaluable asset which must be protected and managed to ensure that they are secure, reliable, maintainable, and supportable. The following Procedure outlines the appropriate use of City of Blue Island computer network resources.

Policy: The use of computer network resources including the Internet and/or email, whether internally or externally, for any of the following purposes is **strictly prohibited**:

1. To create or transmit material which is designed or likely to threaten, disturb, intimidate, or otherwise annoy or offend another, including, but not limited to, broadcasting unsolicited messages, or sending unwanted mail after being advised it is unwanted.
2. To create or transmit defamatory material.
3. Using the Enterprise City of Blue Island email system to transmit material to "all email users" or mass distribution of non-work related material without prior approval from a department or division head.
4. To gain unauthorized access, including the use of hacking or packet sniffing software, to facilities or services on the City of Blue Island network or to use such facilities or services in an unauthorized manner.
5. To conduct business or engage in any for-profit communications or activities unrelated to the City of Blue Island.
6. To access, view or obtain any adult entertainment, pornographic or obscene material, unless it is for work-related investigatory purposes and with the approval of the department head.
7. For political campaign purposes, including, but not limited to, using e-mail to circulate advertising for political candidates or relating to political campaign issues.
8. Sharing your network credentials (login ID and password) with anyone.
9. Downloading and/or installing software to City of Blue Island devices without authorization from Information Technology.
10. Using one's City of Blue Island email address on any Internet service for non-business purposes. If an employee becomes aware that their City-issued email address is on a non-business related service, the employee must promptly request that it be removed and/or unsubscribe.
11. Opening attachments or clicking on embedded links contained in an email from unknown sources.
12. To gain commercial or personal profit or advantage, including, but not limited to, selling lists of names, addresses, telephone numbers, or other information generated from City files.
13. To create or transmit harassing and/or discriminatory material.
14. To represent oneself directly or indirectly as conducting City business when using such equipment for incidental personal purposes.
15. Creation of web pages, without the approval of IT, that purports to officially represent the City of Blue Island, personal or otherwise, regardless upon what server they may reside.
16. To print lengthy documents unrelated to City business.

17. Use of City devices for the purpose of listening to audio or viewing video unless it is for City business.

18. The attachment of any device, except via the City's public wireless network, to the City network including servers, laptops, computers, monitors, printers, multi-function devices, scanners, cell phones/smartphones, mobile computing devices, surveillance cameras, wireless routers, switches, hubs, or any other networking devices without the formal approval of IT.

19. Affix non-business related political and/or decorative stickers, banners, or substances of any nature to the surfaces of any City-owned computer network resources.

20. The inappropriate use of social media

21. Unauthorized distribution of confidential or sensitive information, including the use of non-City Cloud-based storage facilities, personal computing devices, external storage media, or cameras to take pictures or make copies of sensitive materials.

22. Unauthorized use or viewing of City-owned surveillance cameras

23. Use of a cellular phone, Mobile Device while operating a City vehicle (exclusion: Police, Fire & EMS

24. For any other purpose which would be a violation of any City work rules, City ordinance, state law or federal law.

Guidelines:

Purchasing Guidelines: All IT-related equipment, hardware, and software purchases, including software used as a service, and unified communications used as a service must be approved by the IT Department & City Administration. Software to be installed or used on the City of Blue Island network must be properly licensed and proof of this licensing must be available.

Personal Use of Network Guidelines: Use of computer resources for incidental personal purposes is a privilege and can be withdrawn by a supervisor at any time. Employees may not use IT resources in any way that:

- Directly or indirectly interferes with City operations of network facilities or email services.
- Is contrary to or damages the City's interest.
- Interferes with the employee's work duties, performance, or other obligations to the City of Blue Island. Examples include, but are not limited to, excessive use of games, personal internet usage, Social Media Browsing, etc.

Additional Guidelines: All network hardware and software are the property of the City of Blue Island.

Employees are required to follow all Network Security Policies and Procedures outlined in the Network Security Policies and Procedures Manual.

Consequences for Noncompliance: Failure by a City employee to comply with these policies may result in disciplinary action up to, and including, termination of employment.

Authority: The IT Department and City Administration shall maintain and interpret this document.

CITY OF BLUE ISLAND

Data Backup Policy

Policy

Full Backups

Backup of all files on the network.

- Occurs quarterly; on weekends during non-peak network utilization times: 6:00pm Friday - 7:00am Monday.
- Retained for three (3) years.

Incremental Backups

Backup files that have been modified since the last backup.

- Occurs daily during non-peak utilization times: 6:00pm – 7:00am.
- Retained for three (3) years.

Restoring Files

- To restore archived data, backup media devices, servers, and software will be kept as long as archived data exists for that media.
- Requests to restore data (i.e., spreadsheets, word processing documents, email, application data, etc.) must be within three (3) years or less from the date of the request This can be accomplished by submitting an email or phone request to the IT Help Desk.

CITY OF
18 35 BLUE
ISLAND

Internet Content Filtering Policy

Purpose: The City of Blue Island Internet Filtering Policy is put in place to protect the City's network from malicious viruses, trojan horses, ransomware and or other random threats to the network from the internet. It also enables the ability to filter out inappropriate content.

Policy: The City employs an industry leading firewall to scan, flag, and block malicious websites. Access to a website will be blocked if it poses a security risk to the City network. Websites are organized into categories based on similar topic and general description as determined by the vendor. Specific categories are blocked based on vendor recommendations.

Exceptions: Requests for exceptions need to be submitted to the Help Desk. The IT Department will not grant any exceptions that pose a security risk.

CITY OF BLUE ISLAND

Network Connection Policy

Purpose: The City of Blue Island Network Connection Policy is put in place to protect the City's network from malicious viruses, trojan horses, ransomware and or other random threats to the network from devices that are not part of the technology environment.

Policy: The Network Connection Policy states that only City of Blue Island devices are permitted to be plugged into or wirelessly connected to the overall data network. If the device has not been issued by the City of Blue Island, the IT Department & City Administration needs to approve or otherwise will be prohibited. After approval, validation of the device is required to ensure the device is clean from malware, viruses, etc.. Protecting the technology environment is most important and best practice. This allows the City to protect the integrity of its data. The Network Connection Policy is oversight on all devices connected through physical, wireless, and remote (VPN) abilities.

New Software Request

New Software Request Process

The New Software Request Process applies to all software and online services, including **free** software. Information Technology approval is required for all software, including downloaded, web-based and equipment embedded with software on City of Blue Island-owned devices, regardless of price.

The purchasing guidelines apply to all software purchases and must be followed. City Attorney and Risk review are required because software and online services come with a set of legal terms (sometimes known as an End User License Agreement or EULA). The EULA is a contract. City staff are **not** authorized to sign, click, or agree to any legal terms, even for free software.

Requesting New Software

1. **Authorized Contact Approval**

   Request software approval via email from your department's authorized contact. This approval email must be attached to your New Software Request form. Your request will be denied without proper documentation of authorized contact approval.

2. **Submit a New Software Request form**

   Submit a New Software Request form to begin the review process. Please contact the IT Department for the new user request form.

3. **Approval Status**

   Once your New Software request has been reviewed by each of the key departments, an IT Execution Planning meeting needs to be scheduled.

4. **Purchase**

   If your New Software request has been approved, you may purchase the software. Work with the administration office for PO information and or other necessities with the purchase.

5. **Installing Approved Software**

   When you are ready to have your new software scheduled to be installed, please email the Help Desk to have a service ticket created. Please include the following information in your email.

   - Staff names and machine IDs that need access to the software
   - Link to the software installation package
   - Serial number and license information of the software
   - Help Desk will assist with clicking through required terms and conditions and installing the software.

The Review Process

1. **Finance Review**

   Finance will review your New Software Request for budgetary notes.

2. **Information Technology Review**

   The IT Department & VCIO will review all New Software requests.

3. **City Attorney & Risk Management Review (City Executive Management/City Council/City Administration)**

   City Attorney and Risk Management review the legal terms and conditions of the software license or service agreement on behalf of the City of Blue Island.

4. **Final Information Technology Review**

   Once your New Software request has been reviewed by each department, Information Technology will work with you for timeline of execution & deployment.

CITY OF BLUE ISLAND

18 35

City of Blue Island New Software Request Form

Department: _____

Department Head: _____

Software Name: _____

Use Case or Purpose for Software: _____

Software Cost: _____

Infrastructure Type: **Local** ☐ **Server** ☐ **Cloud Based** ☐ **Mobile** ☐

Software Technical Requirements Obtained from Vendor: ☐

IT Notified ☐

IT Review Date: _____

CITY OF BLUE ISLAND

Computer Incident Response Plan & Policy

1 Purpose

The purpose of this Computer Incident Response Plan (CIRP) is to provide the City with a plan that addresses the dynamics of a computer security incident. A computer security incident is one that threatens confidentiality, integrity or availability of city information assets with high impact, high threat involving high risk and great vulnerability. A security incident includes unintentional disclosure of sensitive or protected information such as Social Security Number or other protected information. The CIRP defines the roles and responsibilities for incident response team members, defines incident severity levels, outlines a process flow for incident management, and includes methodologies for conducting response activities.

The CIRP may be used simultaneously during certain disasters to address information security and production computer/network continuity.

2 Scope

This CIRP applies to all computer systems and networks connected to The City of Blue Island's network. The CIRP contains actions required to assure the protection of The City of Blue Island's reputation, information assets and the city's, and staff's information assets that reside under the City of Blue Island control.

Definitions and Acronyms

- **CIRT** – Computer Incident Response Team
- **VCIO** - Virtual Chief IT Officer, VCISO - Virtual Chief Information Security Officer (Chief or designee)
- **IT** - IT Staff
- **CA** - City Administrator
- **PC** - Police Chief
- **FC** - Fire Chief

Policy for Technology Services

Computer security incidents will occur that require full participation of IT technical personnel as well as divisional leadership to properly manage the outcome. IT will

establish computer incident response procedures that will ensure that appropriate leadership and technical resources are involved to

1. Assess the seriousness of an incident,
2. Assess the extent of damage,
3. Identify the vulnerability created,
4. Estimate what additional resources – if any – are required to mitigate the incident,
5. Mitigate the incident,
6. Perform proper follow-up reporting
7. Adjust procedures so that responses to future incidents are improved.

3 Role and Responsibilities

Within this section, the roles and responsibilities for the VCIO, CIRT, and Supporting Groups are defined. In addition, this section addresses the various Technology Services functional areas within the City and their CIRT responsibilities.

3.1 VCIO - Chief IT Officer

The VCIO will either involve or inform as the needs of the incident dictate. Communication of information during an incident will follow this flow to eliminate confusion and misinformation between groups.

The VCIO is responsible for executing or delegating the following:

- Setting priorities
- Notifying the City Administrator of an incident declaration
- Disaster Declaration
- Participating with IT in forensic investigation decisions
- Designating an Assistant VCISO or an alternate to cover the responsibilities of the VCIO role
- Notifying City Communications as appropriate for internal and external communication
- Owning of the IT incident work plan(s)
- Defining and issuing 'gag' orders within Technology Services for particularly sensitive issues; the default guideline for communicating about a computer security incident is on a need to know basis
- Chairing the Post Mortem – Closeout Phase Beginning a case file for the incident. Used to ensure information is properly collected and documented
- Managing incident resources
- Determining if an incident is at a Critical Level and declaring it to be so
- Maintaining communications between CIRT and the VCIO
- Notifying Administration as appropriate
- Notifying Legal as appropriate
- Reminding staff that communication is on a need to know basis or if the VCIO has defined a 'gag order' informing team members of the nature of the 'gag'
- Communicating to the Technology Services Leadership Team that a critical incident has been declared and a CIRT has been formed

- Activating the CIRT and notifying the team of meeting locations and call-in telephone numbers
- Developing containment procedures
- Establishing a Post Mortem Team to determine the root cause and root effect of the incident
- Working closely with the VCIO and General Counsel during forensic investigations
- Managing the incident work plan(s) and task assignments
- Raising dependency issues as they arise
- Coordinating hand-off meetings between shifts, and developing work plans that address tasks completed and outstanding
- Certifying that all systems are returned to operational quality with the cause rectified
- The secure destruction/retention of all materials at the end of an incident
- Identifying external personnel/resources as needed

3.2 Computer Incident Response Team (CIRT)

During an incident the ISO will assemble a team. Members will vary depending on the skill sets required to assist during an incident. Teams will vary in size depending on the need. This team will remain active until the incident is closed. This team will be responsible for both response and recovery. The core membership of the CIRT is defined in section 6.

Response Phase: The response duties of the team are to conduct a triage of the incident, assist in containment of the incident, collect evidence for the post mortem report and if necessary, conduct or assist in a forensic investigation.

Assisting in the collection of evidence during an incident investigation

Making recommendations to the VCIO on remedial action on affected systems
The CIRT may be called up 24 hours a day, 7 days a week, 365 days a year during a critical incident

Recovery Phase: The response aspects of the team are centered on damage assessment, return to normal operations, rebuilding servers and systems, etc.

- Determining whether affected systems can be restored from backup tapes, or must be reinstalled
- Scrubbing all data before making it ready for reinstall
- Determining what data is lost and cannot be recovered or restored
- Reloading data on affected systems
- Restoring normal operations

Follow-up Phase:

- Sending final incident reports to parties with a need-to-know
- Discussing procedural changes and updates
- Discussing configuration issues
- Deciding whether to conduct an investigation to determine the root cause and root effects of the incident

- Discussing any task that were not completed

3.3 Public Safety

- Assist in interviews when necessary
- Assist VCIO during policy violations
- Coordinate with external law enforcement as required
- Liaison to Federal Bureau of Investigation (FBI) as requested by General Counsel

3.4 General Counsel

- Provides guidance to the VCIO regarding legal and regulatory aspects of the incident and its public disclosure
- Advises Administration regarding investigations involving employees
- Advises the VCIO and/or CA regarding decision to simply protect its operations or to pursue civil or criminal actions
- Consults with the VCIO regarding involvement with law enforcement
- Advises the VCIO and/or CA regarding involvement with regulatory agencies
- Reviews communications drafted by the City Administrator as required
- Liaison to external counsel

3.5 CA (City Administrator)

- Advises VCIO on personnel matters
- Initiates employee related investigations along with City General Counsel
- Participates in investigation interviews and furnishes legally permissible personal information as necessary
- Alerts the CIRT of any unusual employee behavior patterns during a critical incident or investigation
- Manages internal concerns and questions from the employee base that are not associated with an incident
- Coordinates internal employee communications along with City General Counsel, as necessary

4 Incident Defined

A computer security incident is any adverse event that threatens the confidentiality, integrity, or availability of city information assets, information systems, and the networks that deliver the information. Any violation of computer security policies, acceptable use policies, or standard computer security practices is an incident.

Adverse events may include unauthorized access to systems and information, denial-of-service attacks, loss of accountability, or damage to any part of the system. If an incident has happened or there is suspicion of an incident, the VCIO must be notified to help determine the level of the incident and next steps in response as defined in this document.

4.1 Incident Levels

Incident levels are defined here for clarity although with any potential incident the VCIO must be notified to help determine next steps. As part of the initial incident response process, the VCIO will need to make an assessment of the incident's impact and assign an appropriate severity level. This severity level will be based upon the potential impact to the operations or reputation of the City of Blue Island, and/or staff.

An incident's severity level dictates the initial response and management activities associated with the event. As incident management activities continue, further assessment may effect a reassignment to a higher or lower severity level.

Critical Incident: Any unexpected or unauthorized change, disclosure or interruption to the City of Blue Island's information resources that could be severely damaging to our students, staff, faculty, and/or reputation. These incidents impact on the City's ability to meet its mission objectives.

High Level: Successful penetration or denial-of-service attack(s) detected with significant impact on operations. These incidents are: very successful; difficult to control or counteract; compromise large number of systems; cause significant loss of confidential data, loss of mission-critical systems or applications; compromise admin/root, user account; result in illegal file server share access; and cause significant risk of negative financial or public relations impact.

Medium Level: Penetration or denial-of-service attack(s) detected with limited impact on operations. These incidents are: minimally successful, easy to control or counteract, compromise small number of systems, result in little or no loss of confidential data and no loss of mission-critical systems or applications. This includes widespread instances of a new computer virus or worm that cannot be handled by deployed anti-virus software that may require corporate-wide activations of CIRT and/or site-administrators. Also includes illegal mirrors and unapproved content (e.g. games, pornography, multi-media servers on corporate networks). These incidents have small risk of negative financial or public relations impact.

Low Level: These incidents involve: a significant level of network probes, scans and similar activities detected indicating a pattern of concentrated reconnaissance; intelligence received concerning threats to which systems may be vulnerable; penetration or DoS attacks attempted with no impact on operations; isolated instances of a new computer virus; or work that cannot be handled by deployed anti-virus software.

5 Escalation levels and Roles and Responsibilities

The roles and responsibilities of each of the teams involved in incident response vary with the particular escalation level that is active at any particular point in time. These roles & responsibilities are described below.

5.1 Low Level Incident

Normal system operations coupled with periodic and real time monitoring of the City's information assets.

System/Network Administrator

- Monitor all known sources for alerts or notification of a threat.

5.2 Medium Level Incident

The monitoring processes have detected early indications of an incident.

System/Network Administrator

- Analyze monitoring data and determine early defensive action with notification to and input from VCIO.
- Notify the local IT Director (where applicable) and Head of Division
- If users are affected, communication message via VP for Administrative Services.

Director / Manager

- Receive and track reported incident event information from System/Network Administrator.
- Escalate incident response to the next level if event information points to a genuine threat.
- Alert relevant business unit head and VCIO of the threat (as appropriate).
- If users are affected, communication message via the City Administrator.

5.3 High Level Incident

A threat has manifested itself.

IT Staff:

- Identify countermeasures for containment of the incident.
- Provide on-going threat status to Director.

VCIO

- Notify City Administrator if appropriate
- Notify CIRT of the manifestation of the threat.
- Report incident details and supporting system logs, audit records, etc. to CIRT.
- Start logging of events for possible disciplinary / legal proceedings.
- If users are affected, communication message via VP for Administrative Services.
- Report continuously to relevant business/academic units.

CIRT

- Assume responsibility for directing the incident handling activities.
- Determine whether further escalation to the VCIO is required.
- Determine if countermeasures have reduced the risks to an acceptable level.
- Receive technical information from relevant system administrators.
- Take required actions.
- Provide feedback to VCIO of department (where applicable).

5.4 Critical Level Incident

The threat has become wide spread or is of high severity level.

IT Staff

- Support the CIRT
- Continue reporting status to VCIO and CA
- Continue to monitor all event sources for alerts and notification of threats
- Monitor effectiveness of the countermeasures in reducing the threats

VCIO

- Continue monitoring the incident
- Report continuously to the CA, PC, FC or equivalent management

CIRT

- Set up command center
- Alert City General Counsel and City Administrator
- Alert vendors/suppliers/external service providers (as appropriate)
- Determine if the countermeasures have reduced the risks to an acceptable level.
- Take required actions
- Provide feedback to VCIO (where applicable)

5.5 Post Incident

The threat has been removed. Full recovery is made. Normal operations have commenced.

CIRT

- For high and critical level incidents, prepare incident report to be reviewed by VCIO and others as appropriate. The report should include:
- Incident log including findings of Technical work that can be used as evidence.
- Estimate of damage / impact
- Details of action taken during the incident
- Follow on efforts needed to eliminate or mitigate the vulnerability
- List of policies or procedures that require updating
- Details of efforts taken to minimize liabilities or negative exposure
- Recommendations for legal/disciplinary action against intruders.
- Document lessons learnt and take corrective action to prevent recurrence.

General Counsel

- As necessary, initiate disciplinary action or legal proceedings against internal / external threat source.

VCIO

- Should perform follow up to ensure any identified corrective action is implemented within a reasonable timeframe.
- Communicate final notice of completion of remediation to affected unit heads.

5.6 Incident Review Report Template

Preparation/Documentation

- Were controls applicable to the specific incident working properly?
- What conditions allowed the incident to occur?
- Could more education of users or administrators have prevented the incident?
- Were all of the people necessary to respond to the incident familiar with the incident response plan?
- Were any actions that required management approval clear to participants throughout the incident?

Identification/Detection

- How soon after the incident started was it detected?
- Could different or better logging have enabled earlier detection of the incident?
- Is the exact time the incident started known?
- How effective was the process of invoking the incident response plan?
- Were appropriate individuals outside of the CIRT notified?
- How well was the CIRP followed?
- Were the appropriate people available when the response team was called?
- Should there have been communication to other inside and outside parties at this time; and if so, was it done?
- Did all communication flow from the appropriate source?

Containment

- How well was the incident contained?
- Did the available staff have sufficient skills to do an effective job of containment?
- If there were decisions on whether to disrupt service to internal or external customers, were they made by the appropriate people?
- Are there changes that could be made to the environment that would have made containment easier or faster?
- Did technical staff document all of their activities?

Removal and Recovery

- Was the recovery complete — was any data permanently lost?
- If the recovery involved multiple servers, users, networks, etc., how were decisions made on the relative priorities, and did the decision process follow the incident response plan?
- Were the technical processes used during these phases effective?
- Was staff available with the necessary background and skills?

6 CIRT Core Team

- VCIO
- City Administrator
- IT Staff
- Police Chief
- Fire Chief