CITY OF CONCORD, NEW HAMPSHIRE

INFORMATION SECURITY POLICY

DEPARTMENT OF INFORMATION TECHNOLOGY

TABLE OF CONTENTS

I. PURPOSE OF POLICY

The purpose of the Information Security Policy (Policy) is to establish the appropriate use and protection of the City's information assets and technology. This Policy is intended to ensure that the City's information assets and technology are secure from unauthorized access, misuse or destruction.

II. APPLICABILITY

This Policy applies to the City of Concord's employees (including temporary employees), volunteers, interns, vendors, consultants, contractors and agents (collectively referred to as "Users") as set forth below:

- All new employees are required to receive and sign this Policy, which will be included in the new hire packet provided by the Human Resources Department.
- All employees, volunteers, interns, vendors, consultants, contractors and agents who have access to the City's secure network system shall be required upon logging in to the system to acknowledge that they have read this Policy and will abide by its terms.

All other individuals who use the City's information technology, but do not have access to the City's secure network, must abide by this Policy where applicable. For those individuals, a copy of this Policy will be publicly available on the City's website.

Any arrangements that extend the City's information from the City's secure network into a third parties' computing environments require the third party to abide by this Policy, as applicable, unless specific additional provisions have been established through contractual agreements. For example, a vendor that provides remote support and has access to the City's secure network system must abide by this policy.

This Policy does not create any rights, constitute a contract, or contain the terms of any employment contract or other contract between the City, any employee or applicant for employment, or any other person. Rather, this Policy details certain procedures and responsibilities with respect to the management of information assets. The City reserves the right to amend this Policy or any part or provision of it.

III. IT DEPARTMENT - RESPONSIBILITY FOR ORGANIZING INFORMATION SECURITY

The I.T. Department is responsible for designing, implementing and maintaining a City-wide information security program, and for assisting all City Departments in implementing and maintaining practices for information management.

The I.T. Director is responsible for the overall security of information assets and technology at the City. The Director may delegate specific responsibilities related to information security to others within the City based on their job function. The I.T. Director, or his or her designee, is designated as the security officer.

IV. DEFINITIONS

The following are some of the definitions of terms used in this Policy. Please also familiarize yourself with the common terms and definitions in Appendix A as part of your understanding of this Policy.

Term	Definition
City Secure Network System	The City's data network that allows computers and other mobile devices to securely exchange data for distributed applications.
Users	The City of Concord's employees (including temporary employees), volunteers, interns, vendors, consultants, contractors and agents who use the City's information technology as part of their job function.
Information Assets	Information and data created, developed, processed, or stored by the City that has value to the City's business or operations.
Information Technology or Network and Computer Resources	Computer hardware and software, mobile devices that connect to the network or Internet, network hardware and software, email, voice mail, video conferencing, facsimile transmission, telephone, remote access services, printers, copiers, and all other printed and electronic media.

V. CLASSIFICATIONS OF INFORMATION ASSETS

The City's information assets, whether in electronic or physical form, are categorized into three classifications. This Policy sets forth the manner in which the three classifications must be protected.

1. Confidential Information: Sensitive Personal Identifiable Information (PII) used for business purposes within the City which, if disclosed through unauthorized means, could adversely affect the City's personnel, including employees and constituents, and could have legal, statutory, or regulatory repercussions.

   Examples: Information protected from disclosure under the federal Health Insurance Portability and Accountability Act (HIPAA), other personnel information including Social Security numbers, and personal financial information including credit card data protected by the Payment Card Industry's Digital Security Standard (PCI DSS).

2. Internal Information: Information related to the City's business that if disclosed, accessed, modified or destroyed by unauthorized means, could have a financial or operational impact on the City.

Examples: Confidential contract negotiations, vendors' proprietary information and information protected by non-disclosure agreements. Other information related to the City's information technology that is considered Internal Information includes access point Internet Protocol (I.P.) addresses used for firewalls.

3. Public Information: Information intended for public disclosure in the course of the City's business.

Examples: Press releases, public marketing materials, and employment advertisements.

VI. OWNERSHIP OF INFORMATION ASSETS

All information assets stored and processed over the City's technology systems is the property of the City. Users of the system have no expectation of privacy associated with the information they store in or send through these systems.

VII. ACCEPTABLE AND UNACCEPTABLE USE OF IT RESOURCES

To effectively conduct the City's business and operations, the City makes available to authorized Users various information technology resources, including e-mail, the City's Intranet, the Internet, and other communication and productivity devices.

- Use of these resources is intended for business purposes in accordance with Users' work functions and responsibilities, with limited personal use permitted only in accordance with other applicable City policies, personnel rules, and this Policy.
- The use of information technology resources is not permissible if it creates more than a negligible expense to the City, consumes excessive time, or violates a City or departmental policy.
- The privilege of limited personal use may be revoked or limited at any time by the City or department officials.

The following rules apply to the use of I.T. Resources:

1. Users must not allow any consultant, visitor, friend, family member, customer, vendor or other unauthorized person to use their network account, e-mail address or other City-provided computer facilities. Users are responsible for the activities performed by and associated with the accounts assigned to them by the City

2. No User may use the City's secure network or Confidential or Internal City information to solicit or conduct any personal commercial activity or for personal gain or profit or non-City approved solicitation. The City's secure network does not include Internet provided through the public network or guest access.

3. Users must not disclose Confidential or Internal City information outside of the organization unless expressly authorized by their Department Management.

4. Users must protect Confidential or Internal information being transmitted across the Internet or public networks in a manner that ensures its confidentiality and integrity between a sender and a recipient.

❖ Confidential information such as Social Security numbers, credit card numbers, and electronic Protected Health Information (ePHI) must be transmitted using encryption software.

5. Internal information must not be posted to any external information source, listed in telephone directories, placed on business cards, or otherwise made available to third parties without the prior express written permission of the User's Department Management.

6. Users must not install software on the City's network and computer resources without prior express permission from the I.T. Department.

7. Users may not access the City's secure network from any device that allows Peer-to-Peer (P2P) applications without explicit approval from the I.T. Department. A P2P application is designed to exchange digital media such as music, movies, videos or other files, and includes but is not limited to networks such as Napster, BitTorrent and LimeWire. For more information, please see the definition in Appendix A.
8. Users must not copy, alter, modify, disassemble, or reverse engineer the City's authorized software or other intellectual property in violation of licenses provided to or by the City, Additionally, Users must not download, upload, or share files in violation of U.S. patent, trademark, or copyright laws. Intellectual property that is created for the City by its employees, vendors, consultants and others is property of the City unless otherwise agreed upon by means of third-party agreements or contracts.

9. All Users must abide by the City of Concord Internet/E-Mail Policy and Social Media Policy.

VIII. COMMUNICATIONS AND OPERATIONS MANAGEMENT

A. Protection Against Malicious Code

It is the City's policy to conduct virus scanning of its technology resources to protect them from the threat of malicious code. The City will intercept and/or quarantine any networking and computer resource that poses a virus threat to its information assets.

All servers and workstations (networked and stand-alone) must have the City's approved antivirus protection software installed, properly configured, and functioning at all times. Additionally, systems that have not been issued by the City but that are used to access the City's secure network must also be protected by antivirus software.

❖ Users are responsible for ensuring that software, files, and data downloaded onto the City's workstations from any external source are properly scanned for viruses. The Department of Information Technology will provide information on the current scanning processes to ensure security.

B. Back-Up

The City will perform certain backups of User files stored on the City's file servers and storage media that are centrally managed by the Department of Information Technology. This process will be coordinated in conjunction with the City's Departments based on their business needs.

C. Media Handling — Disposal of Media

Except as otherwise provided by law or court order, electronic information maintained in a department's office may be destroyed by department staff or the I.T. Department when the retention period expires, in compliance with the City's implementation of the State of N.H.'s Disposition of Municipal Records RSA's.

D. Monitoring System Use

Users should have no expectation of privacy in their use of Internet services when using computers or other mobile devices provided by the City. The City reserves the right to monitor for unauthorized activity the information sent, received, processed or stored on City-provided network and computer resources, without the consent of the creator(s) or recipient(s). This includes all use of the City's secure network including but not limited to the Internet, City's email and instant messaging systems.

Audits may be conducted by the I.T. Department to:

- Ensure integrity, confidentiality and availability of Information and resources.
- Investigate possible security incidents.
- Ensure conformance with the City's security policies.
- Monitor user or system activity where appropriate.

All employees of the I.T. Department who by the nature of their assignments have privileged access to networks or computer systems must obtain approval from the Director of Technology to monitor activity.

E. Clock Synchronization

All server clocks shall be synchronized in the manner approved by the I.T. Department to provide for timely administration and accurate auditing of systems. Users are prohibited from modifying such clocks.

IX. ACCESS CONTROL

A. User Access Management

- User accounts that have not been used for 90 days may be disabled without warning. After 180 days of inactivity, these accounts may be deleted without warning
- Departments must use the Intranet form (new user, user termination), to notify the I.T. Department of a change in employment status (such as when a User takes a leave of absence, transfers departments, or is terminated). The account of a User on a leave of absence can be retained, suspended, or deleted at the discretion of the User's department
- When a User leaves the City, all Information Assets remain the property of the City. A User must not take away Confidential or Internal Information or take away a copy of Confidential or Internal Information when he or she leaves the City without the prior express written permission of the Department Head.

- Requests to access to Confidential and Internal data on another User's work station that is not otherwise available to the requester must be made using a formal written request through the helpdesk system.

B. User Responsibilities

1 Password Use

a. All e-mail, network, domain accounts must be password protected. All new accounts will be created with a temporary password. The temporary password must be changed upon first use.

b. Mobile devices must be password protected; this includes but is not limited to smart phones, laptops, handhelds (e.g. iPhones, Androids, iPads) and off-site desktops.

c. Passwords used on the City's systems that are authorized for use must have the following characteristics unless otherwise approved by the I.T. Department:

i. Passwords must be a minimum of 12 characters in length

ii. Passwords must contain three out of four of the following characteristics: Uppercase, lowercase, numeric (0-9) and special characters @ # $ % * ( )

iii. Passwords must not be the same as the username

iv. Password cannot be one of the previous 10 passwords

v. Passwords must be changed at minimum every 90 days

vi. Passwords used for production systems must not be the same as those used for corresponding non-production system such as the password used during training, unless it is active directory synced.

d. Passwords must not be disclosed to anyone. All passwords are to be treated as Confidential information.

e. Do not use the same password for the City of Concord secure network as for other non-City access (e.g., personal internet access, stock accounts, banking, etc.). Where possible, do not use the same password for various City access (use separate passwords for software access, and the network).

2. Screen Savers

Use of password-protected screen savers are required to prohibit unauthorized system access. Screen savers should initiate after 15 minutes of inactivity. Password protected screen savers are required on workstations that access Confidential Information. An exception is allowed for a limited number of Public Safety workstations (identified by the I.T. department) located in a secure location.

C. Mobile Computing and Remote Access

1. Laptops, off-site computers, and other mobile computing devices (which includes flash drives) that contain Confidential Information must be encrypted using an encryption technique approved by the I.T. Department. Laptops, off-site computers, and other mobile computing devices that contain Internal Information must be protected using an encryption technique approved by the I.T. Department, a password, or restricted physical access in order to protect the data.

2. Personal mobile devices (for example, smartphones, iPods, iPads) must not be used as peripheral devices plugged into City-issued workstations, unless approved by the Department of Information Technology. Any charging of these devices shall be performed through a wall charging unit.

3. Remote access is provided by the City as an information conduit to assist in the accomplishment of municipal duties and goals. Any other use is strictly prohibited. Requests for remote access must have a valid business reason and be approved by the Department of Information Technology.

4. All remote access connections must be approved by the City. Authorized remote access connections must be properly configured and secured according to City approved standards including the City's password policy. All remote desktop protocol implementations must be authorized by the Department of Information Technology. Remote access through unapproved entry points will be terminated when discovered.

5. Non-City owned computer equipment used for remote access must have up to date Antivirus, and comply with the City's standards. The City will not be responsible for maintenance, repair, upgrades or other support of non-City owned computer equipment used to access the City's network and computer resources through remote access services,

X. INFORMATION SECURITY INCIDENT MANAGEMENT

A. Reporting Information Security Events and Weaknesses

1. Violations of this Policy must be immediately reported to a Department Head, Director of the I.T. Department or City Manager.
2. Users must also ensure that a Help Desk representative is notified immediately whenever a security incident occurs. Examples of security incidents include a virus outbreak, defacement of a website, interception of email, blocking of firewall ports, and theft of physical files or documents.
3. All reports of alleged violations of this Policy, or any part or provision hereof, will be investigated by the appropriate authority. During the course of an investigation, access privileges may be suspended. Any violation of this Policy, or any part or provision hereof, may result in disciplinary or other legal action, including termination of employment or service, civil action and/or criminal prosecution.

XI. COMPLIANCE WITH LEGAL REQUIREMENTS

A. Intellectual Property Rights

Intellectual Property that is created for the City by its employees is property of the City unless otherwise agreed upon by means of third-party agreements or contracts.

No User may transmit to, or disseminate from, the Internet any material that is protected by copyright, patent, trademark, service mark, or trade secret, unless such disclosure is properly authorized and bears the appropriate notations.

B. Prevention of Misuse of City's Information Assets, Technology, Network and Computer Resources

Users are prohibited from using the City's information assets, technology, network and/or computer resources in any way that violates this Policy, and federal, state, or municipal law, including, but not limited to, the City's Municipal Code and Personnel Rules.

C. Compliance with Relevant Laws and Regulations

By virtue of the City's services to its constituents and the nature of its legal status, the City is covered by certain laws and regulations dealing with security and privacy of information, most notably the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry's Digital Security Standard (PCI DSS). These laws and regulations, in some circumstances, may require additional safeguards for protection the City's information beyond the stipulations of this Policy. Users with access to Protected Health Information (PHI) must abide by HIPAA and Users with access to credit/debit card information must abide by PCI, as applicable.

Dated: Sept. 26, 2022 Signed: Thomas J. Aspell Jr.

Thomas J. Aspell, Jr., City Manager

Appendix A
Common Terms and Definitions

1. Computer Resources - All related peripherals, components, disk space, system memory and other items necessary to run computer systems.

2. Credit Card Data - The Primary Account Number (PAN), Card Verification Value (CVV--the 3-4 digit code on the signature block on the back of a Credit Card), track data (the data read directly from the magnetic stripe of a Credit Card) and PIN Block data (also read from the magnetic stripe). The PCI DSS can be found at https://www.pcisecuritystandards.org.

3. Department Management - A supervisor, manager or employee of the City designated to be responsible for implementation of this Policy by his/her City board, commission or department

4. Electronic Mail (E-mail) - The transmission of messages through electronic means in a body or attachment using the City's network or other information technology.

5. Information Assets - Information and data created, developed, processed, or stored by the City that has value to the City's business or operations.

6. Information Technology or Network and Computer Resources - Computer hardware and software, mobile devices that connect to the network or Internet network hardware and software, e-mail, voice mail, video conferencing, facsimile transmission, telephone, remote access services, printers, copiers, and all other printed and electronic media.

7. Intranet - The suite of browser-based applications and HTML pages that are available for use only with access to the City's internal network.

8. Internet - The worldwide network of networks connected to each other using the I.P. protocol and other similar protocols. The Internet enables a variety of information management services, including, but not limited to, e-mail, instant messaging, file transfers, file uploads, file downloads, news, and other services.

9. Internet Services - Any service in which its primary means of communication is the Internet. For example, e-mail, web browsing and file transfers,

10. Mobile Computing Devices - Mobile devices and mobile media. Mobile data processing devices are used as business productivity tools. Examples include: laptops, personal digital assistants (PDAs), smart phones, handhelds, and off-site desktops. Mobile media are devices typically used to transport data. Examples include: flash drives, DVDs, CDs, and external hard drives.

11. Network - The linking of multiple computers or computer systems over wired or wireless connections.

12. P2P - Peer-to-Peer network. A network where nodes simultaneously function as both client and server to other nodes on the network, P2P may be used for a variety of uses, but it is typically used to share files such as audio files. Examples of P2P networks include Napster, BitTorrent, and LimeWire. If a node is not properly configured, any file on the device may potentially be accessed by anyone on the network.

13. Protected Health Information - Individually identifiable health information about an individual that relates to the past, present, or future physical or mental health or condition, provision of health care, or payment for health care.

14. Remote Access Services - A service that enables off-site access to the City information technology and assets. Examples include the City's telephone exchanges, internal phone switches, wireless access points (WAP), and Virtual Private Network (VPN) connections. Remote access includes, but is not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems.

15. Secure Network System - The City's data network that allows computers and other media devices to securely exchange data for distributed applications.

16. Security Incident - An event that has an adverse impact on the confidentiality, integrity, and availability of computer systems, computer networks, electronic information assets, or physical information assets.

17. Users - The City of Concord's employees (including temporary employees), volunteers, interns, vendors, consultants, contractors and agents who use the City's information technology as part of their job function

16. World Wide Web (WWW) - Browser-based applications and HTML pages that are available for access and use across the Internet.

Appendix B

FOR USE OF THE HUMAN RESOURCES DEPARTMENT (INCLUDE IN NEW HIRE PACKET)

City of Concord

Statement of Adherence to the Written Information Security Policy

The City has created a policy that has been prepared for your understanding of the City's policies and practices related to the City's technology resources and private information. Please read the document carefully and upon completion, sign the statement below. For all employees and paid interns, please return the form to the Human Resources Department. For all volunteers, unpaid interns, vendors, consultants, contractors and agents, please return the form to the Department Management responsible for retaining or hiring you.

I,_____have received and read a copy of the City's written information security policy that details my responsibilities for implementing appropriate administrative, technical and physical safeguards to maintain the security and confidentiality of private information.

I have familiarized myself with this document. I acknowledge, understand, accept and agree to comply with the information contained in the City's written information security policy provided to me by the City of Concord.

_____

(Signature) (Date)

_____

(Print Name)