Technology Policy and Forms

City of Lowell
Management Information Systems
375 Merrimack Street • Lowell, MA 01852
P: 978.674-4099 • F: 978.970.4004 • www.lowellma.gov

Mirán Fernandez
Chief Information Officer

John Meyers
MIS Director

This packet includes the following Technology Policies and MIS Forms, to be reviewed and completed as appropriate:

✓ **Technology Policy**, on pages 3 - 22
Use this form to acknowledge receipt/understanding of the City's various technology related policies. *This form must be signed by the computer user and submitted to MIS* ***within two (2) business days*** *after a new employee's start date*, or their account will be disabled until it is signed and submitted.

✓ **New User Request Form**, on pages 23 – 24
Use this form to request the creation of a new City network user account. This form must be completed by the Department Head, Manager, or Supervisor as completely as possible in order to ensure your employee has the appropriate resources available on the anticipated start date. *Please note that MIS* ***requires a two (2) week notice*** *prior to the employee's start date to schedule, configure, and setup a new computer user; more time may be necessary if there are specialized computing needs or the submission is incomplete. Requests submitted without two weeks' notice may result in delayed account activation.*

✓ **ID and Access Badge Request Form**, on pages 25 - 26
Use this form to request a City picture ID and/or Door Access Badge. This form must be completed by the Department Head, Manager, or Supervisor of the employee for whom an ID and/or Door Access Badge is being requested, and signed by the employee prior to contacting MIS to schedule the ID photo; ***NO photo will be taken without a completed and signed form*****.** Once the photo is taken and the ID/Badge is processed, MIS will contact the department to coordinate delivery.

General Notes:

- Please make sure to **PRINT CLEARLY**; illegible forms will be returned and may result in a delay; all forms are scanned for archiving.
- A **separate set of forms must be completed for each user**, and be submitted to the Help Desk separately, as each may be handled or prioritized separately.

! THIS ENTIRE PACKET DOES NOT NEED TO BE PRINTED !
However, if you choose to print it, please make sure to print it double-sided!

[This page intentionally left blank]

Technology Policy

City of Lowell
Management Information Systems
375 Merrimack Street • Lowell, MA 01852
P: 978.674-4099 • F: 978.970.4004 • www.lowellma.gov

Mirán Fernandez
Chief Information Officer

John Meyers
MIS Director

To: All City of Lowell Technology and Data Users

From: Thomas A. Golden, Jr., City Manager

Re: Computer Use and Technology Policies

Date: 08/17/2022

Since 1995, when the City of Lowell issued its first "Computer Usage Policy", technology has grown more powerful and complex, been further integrated into much of what we do, and the City has invested millions of dollars in its information systems and facilities. The power and complexity of the technology used to manage the City of Lowell's services, requires that standards and guidelines be in place in order to ensure that the taxpayer's technology investment is safe, secured, and available.

These policies are not intended to discourage you from using the City's technology or data in performing your job – rather, they are intended to ensure that the City's technology and data is used responsibly, and that it is adequately protected from events which may jeopardize City services, whether internal, external, deliberate, or accidental.

While definitive policies cannot be readily formulated for every possible scenario which may arise, these policies are intended to ensure that: (1) safe, responsible, and secured computing conditions are maintained, (2) a consistent, effective, and efficient delivery of the appropriate levels of service and support are provided, and (3) the cost effectiveness of the technology for the taxpayer is maximized.

[This page intentionally left blank]

Technology Policy

City of Lowell
Management Information Systems
375 Merrimack Street • Lowell, MA 01852
P: 978.674-4099 • F: 978.970.4004 • www.lowellma.gov

Mirán Fernandez
Chief Information Officer

John Meyers
MIS Director

Purpose

The City of Lowell's Technology Policies are intended to ensure that the City of Lowell's ("City") technology resources are available and utilized in an appropriate manner, in accordance with local, state, and federal laws, and the City's own various policies and procedures. The policies contained in this document are intended to work together comprehensively as a single City Technology Policy ("Policy"). The Policy is designed to (1) ensure safe, responsible, and secured computing conditions are maintained, (2) ensure a consistent, effective, and efficient delivery of the appropriate levels of service and support are provided, and (3) ensure that the cost effectiveness of the technology for the taxpayer is maximized.

Scope

This Policy applies to all users ("Users"). Users include, but are not limited to, all City and School employees, contractors, visitors, or any other personnel using, accessing, or otherwise interacting with the City's data, hardware, software, and other technology resources ("Resources"). Resources include, but are not limited to, all hardware and data (regardless of origination, destination, custody, funding source, or format), all media and the facilities containing them, all host or remote technology systems (e.g., workstations/PCs, mobile and handheld devices, telecommunication/radio devices, system software, application software, and data), and communications networks or systems which may be directly, indirectly, or remotely controlled, administered, accessed or otherwise interact with other City Resources. All Users having previously completed a Computer Usage Policy Acknowledgement Form are required to continue observing and abiding by these updated Policies which replaces the Computer Usage Policy originally issued in 1995, and which may be updated ad-hoc as technology continues to evolve. If any component of this Policy conflicts with any applicable collective bargaining agreement (CBA), the component shall be subject to the CBA, and the remaining non-conflicting features of this policy shall remain in effect.

Privacy Statement

USERS OF CITY RESOURCES HAVE NO PRIVACY RIGHTS. NO EXPECTATION OF PRIVACY IS MADE, GIVEN, SUGGESTED, RESERVED, IMPLIED, OR OTHERWISE ASSOCIATED WITH THE USE OF CITY RESOURCES. Passwords do not imply privacy; Users may not expect any privacy in the use of City Resources.

Compliance

Violations of this Policy may result in disciplinary actions as deemed applicable by City Management and/or the appropriate governing body. If violations of this Policy are discovered that consist of illegal activities, the City may notify the appropriate authorities. The City reserves the right to pursue appropriate legal actions to recover any financial losses suffered as a result of violations of this Policy.

General Use Policy

The City's Resources are owned, operated, administered, and managed by the City of Lowell, provided as a business tool to users in order to facilitate timely and efficient business use, and are to be used for business-purposes only. The appropriate use ("Appropriate Use") and protection of all City Resources is expected from all Users. Appropriate Use of these resources is defined as use which is City business-related; all other use is inappropriate.

General Use of City Resources is subject to the following:

- All City Resources are the property of the City.
- The City's MIS Department is responsible for establishing the rules and guidelines for the use of these Resources.
- The City reserves the right without notice, to limit, restrict, monitor, block, access, search, review, modify, or disclose the use of any and all City Resources, including but not limited to, any City Resources or materials ("Materials") including, but not limited to, data, applications, Internet access or emails.
- The term "personal computer" does not suggest that Users have the choice of what general City Resources are made available, or of what applications are installed or configured on City Resources assigned to Users; applications may be installed, modified, or removed without notice.
- The City retains ownership of all City Resources and Materials stored, maintained, deleted, added to, modified, received, sent, or otherwise accessible via the City's Resources unless otherwise copyrighted, trademarked, or agreed to through the City's Law Department.
- Any Materials sent to or from City Resources must comply with federal and state laws regarding the protection of personally identifiable ("PID") information (e.g., DOB, SSN, Name and Address information), and applicable Record Retention Laws. PID data should always be encrypted.
- All Users are expected to appropriately guard against the loss, theft, or corruption of the City's Resources. Data files and materials should not be stored on local device storage areas (e.g., hard drives, flash memory, etc.); all data files and materials should be stored on network drives, or otherwise be appropriately backed up to prevent against disaster and assist with recovery.
- All City Resources are subject to discovery; even if a User believes they have deleted Materials, they may be retained on other City Resources. Users should NOT generally delete Materials unless they are clearly considered trivial or irrelevant (e.g., an email about coffee/pizza being served somewhere), as they may be subject to Records Retention Laws.
- City Resources and Materials must not be taken off-site by Users without written approval.
- Only City-issued email addresses (e.g., *user*@lowellma.gov) are to be used for City-related business.
- Access to 3rd party email and/or messaging systems is generally not allowed and is subject to review and approval by the City Hall MIS Department.

- City Resources may be configured with remote management tools to assist with loading additional applications and software. Users shall not remove, disable, or otherwise modify any applications or software installed by the City Hall MIS Department. The City Hall MIS Department will only assist with the installation of additional applications or software deemed necessary and appropriate for City-related business use.

Computing Ethics Policy

With so many Users sharing City Resources, misuse by even a few Users has the potential to disrupt the City's business, interrupt the work of others, and create an unwelcome or unsafe environment. All Users are therefore required to exhibit and exercise responsible, prudent, and ethical behavior when using City Resources.

Ethical Use of City Resources is subject to the following:

- The use of City Resources and Materials should always be conducted in a truthful and accurate manner; Users should never misrepresent themselves in order to gain access to any City Resources or Materials, or in order to deceive anyone interacting with City Resources or Materials.
- Users should make every effort to keep their communications and correspondence professional and appropriately personable.
- Users must make every prudent and reasonable effort to protect against the theft, loss, or damage of City Resources and Materials.
- Users must only access City Resources and Materials as expressly authorized by City administration and management ("Management"), must not attempt to bypass or defeat any City Resources, security, or firewall restrictions, and must not disable, hinder, render inoperable, or otherwise tamper with City Resources or Materials.
- Users may not authorize anyone to use their City Resource accounts for any reason, are responsible for properly locking down access to systems when they are away from them, and are responsible for any Materials transmitted, accessed, or otherwise entered or modified from systems/accounts Users are logged into.
- Users must not use any City Resources recklessly, negligently, irresponsibly, carelessly, excessively, or in any way that might needlessly interfere with the work of others directly or indirectly, impact other City Resources, cause offense to others, or waste City Resources. This includes, but is not limited to:
    - Using City Resources for any private, personal, unlawful, unethical, commercial, political campaigning, monetary gain, or legally questionable activity ;
    - Accessing inappropriate sites including adult content, online gambling, and dating sites;
    - Using encryption technology that has not been approved for use by the City's MIS Department;
    - Using personally owned technology (or technology which is owned by another organization or business) for conducting City business, where official City records are created but not maintained by the City;
    - Accessing sites that distribute security exploits (hacking sites), or using security exploit tools (hacking tools) to attempt to elevate user privileges or to otherwise obtain unauthorized resources.
    - Intentionally intercepting, accessing, altering, copying, distributing, moving or removing City Resources or Materials without Management permission;

  - Accessing City Resources related to other Users, constituents, businesses, or anyone else, without a City-related business purpose requiring you to do so;
  - Creating unnecessary network traffic, system processing load, congestion, disruption, disablement, alteration, impairment, or monopolizing of Resources.
  - Establishing any remote control, remote access, or remote monitoring services without the written permission of the City MIS Department or for any non business-related purposes;
  - Loading software or data from untrustworthy sources (e.g., freeware, or shareware), or without ensuring that all files are properly scanned for viruses or other malicious software code prior to introduction to City Resources;
  - Connecting, installing, introducing, or otherwise initiating unauthorized technology into the City;
  - Transmitting or making accessible offensive, fraudulent, sexually explicit, profane, obscene, harassing, intimidating, threatening, or defamatory Materials;
  - Using online shopping sites, social network sites, or media sites for personal and non business-related use; and
  - Using City Resources in a manner which may subject the City to any liability claim.
- Users must abide by copyright law and intellectual property rights; downloading non business-related Materials (e.g., games, music files, videos, etc.) is prohibited.

Password Policy

No one is immune from cyber risk, but there are steps you can take to minimize your chances of a cyber-incident. When coupled with frequently changing your password, creating a strong password is an essential step to protecting yourself online; using long and complex passwords is one of the easiest ways to defend yourself from cybercrime.

- Passwords do not imply privacy; Users may not expect any privacy in the use of City Resources.
- Passwords should not be generally shared with anyone, written down or posted in your work area, or otherwise stored on non-MIS authorized devices.
- Management reserves the right to request password information related to 3rd party systems; please check with MIS for additional information.
- All Technology Users are required to change their passwords every three (3) months or ninety (90) days at a minimum.
- All network passwords are required to meet strong-password guidelines, are subject to lockout-based failed login attempts, and will require contacting the MIS Help Desk in order to be re-enabled.
- Multifactor authentication devices ("MFAs") are issued for controlled access to a variety of the City's Technology, and may be used in combination with passwords.
- Simple tips to creating strong passwords include:
  - Make your password eight characters or longer, combining letters, numbers, and symbols.
  - Use a long passphrase, such as a news headline or even the title of the last book you read; then add some punctuation and capitalization.
  - Don't make passwords easy to guess. Do not include personal information in your password such as your name or pets' name. This information is often easy to find on social media, making it easier for cybercriminals to hack your accounts.
  - Avoid using common words in your password. Instead, substitute letters with numbers and punctuation marks or symbols. For example, @ can replace the letter "A" and an exclamation point (!) can replace the letters "I" or "L".

Cybersecurity Policy

Cybersecurity is a shared responsibility and each one of us is entrusted with protecting our public assets and helping to ensure the continuity of government services.

- Educational opportunities about this topic are mandated per the City Manager, including CyberStrength Assessments, Training Assignments, and Mock Phishing Emails. These educational opportunities are intended to help you improve the City's overall cybersecurity posture, and the skills you learn through this program will also be beneficial in protecting you and your family's cybersecurity at home.
- The City participates in the Federal Government's "Stop. Think. Click." program, encouraging users to carefully assess websites and emails before clicking on them. For additional details, please contact the Help Desk.
- No one from within the City will ever email or call anyone asking that you confirm your password or other personally identifiable information.
- All Users are required to demonstrate due diligence when accessing websites and reviewing emails.
- The City uses a variety of tools to block potentially malicious websites and emails; questions about blocked websites and emails should be directed to the MIS Department.
- From time to time, City Hall MIS may broadcast alerts regarding significant technology-related events we want everyone to be aware of. Emails of this type will originate from either "Help, MIS", or from a member of the MIS Department.
- E-mail messages which do not originate from "Help, MIS", and which do any of the following are most likely hoax emails intended to either frighten or mislead you, and fall into the "chain letter", "SPAM" and/or "hoax" category:
    - Signed by "Lowellma Email Exchange", "System Administrator", "Help Desk", "Information Desk", "IT Help Desk", "Your Support Team", or some other similar generic name.
    - Requesting your network or email login credentials (e.g., account/email and password, etc.).
    - Requesting general technology information (e.g., make/model, etc.) on computer systems, printers, or phones in your office.
    - Indicating that you have to re-synchronize your email by clicking on a button, alerting you of a new "virus that will destroy your computer", notifying you of a "safety warning", or indicating that you are "the winner" of some sort of promotion.
    - Trying to impart a sense of urgency "or else", containing an "important warning that everyone needs to know about immediately/confidentially", rushing you to complete a task immediately, or asking you to "forward this to everyone you know".
    - Attempts to intimidate you by claiming to know what you are "doing" or otherwise "watching" you via your computer's camera.

If you receive one of these “chain letter”, “SPAM”, or “hoax” e-mails please forward it to the MIS Help Desk (help@lowellma.gov) by (1) opening a new email message, (2) dragging the email you are concerned about into it as an attachment, and then (3) deleting the original email message. This retains the “header” information within the original email, and allows us to better diagnose it.

Social Networks and Social Media Policy

Social networks consist of social media content within online communities of people or organizations that share interests and/or activities and use a wide variety of Internet technology to make the interaction a rich and robust experience. Social media may facilitate discussion on City issues, operations, and services by providing members of the public the opportunity to participate in a variety of ways via the Internet. Examples of social networks and social media ("Social Media") include, but are not limited to, Facebook, Blogs, My Space, RSS, YouTube, Second Life, Twitter, LinkedIn, Delicious, Flicker, various 3rd party email accounts, instant messaging tools and general websites.

The City views Social Media positively, recognizes that these tools may significantly influence reputation, and understands that Social Media is the basis for much wider changes taking place in online media that may increasingly affect City services delivered to constituents. Because of this, the City has an overriding interest and expectation in deciding "what is said" on behalf of the City on Social Media, and how the City is portrayed. The use of Social Media must be tempered with common sense, good judgment, discretion, and responsible use in order to maximize the benefits of these resources and minimize potential liability.

Use of Social Media is subject to the following:

- The City's uses of Social Media must meet one of the following three categories:
  - As a channel for disseminating time-sensitive information as quickly as possible;
  - As a channel for enhancing communications with constituents, businesses, and stakeholder organizations related to conducting business with the City; and
  - As a channel for marketing, promoting, or otherwise furthering the City's goals and objectives by publishing news and articles, facilitating discussions, and communicating information related to City accomplishments, promotions, or other marketing events.
- The City's website (lowellma.gov) will remain the City's official, primary and predominant Internet presence.
- Wherever possible, content posted to City Social Media will also be available on the City's primary sites.
- Wherever possible, content posted to City Social Media should contain links directing users back to the City's official websites for in-depth information, forms, documents, or online services necessary to conduct business with the City.
- The City reserves the right at its sole discretion to determine which Social Media sites and tools are appropriate and applicable to best represent the City, as well as which Users may access Social Media tools, or post on behalf of the City.
- Users may not create (or have created for them) any Social Media site on behalf of, for, designed to represent, or otherwise intended to officially promote the City in any official capacity, without first obtaining written permission from the City MIS Department.

- Ownership of any Social Media sites created on behalf of, for, designed to represent, or otherwise intended to promote the City in any official capacity, must be transferred to the City prior to going live online; the City retains ownership of all Materials posted on City-owned Social Media sites.
- All Social Media sites must be registered with the City MIS Department. Registration must include the department coordinating the Social Media, any email associated with the account, administrative account and password credentials, and must identify which Users may be accessing/managing the Social Media site for updates and commentary approval. The City MIS Department must be updated with any changes to any registration information as applicable.
- Wherever possible, City Social Media sites shall comply with all appropriate City policies and standards, and shall include information on or links to existing City privacy policies, terms of use, accessibility policies, social media policies, terms of comment, information on third party providers, information on personal information collected by third parties, and/or intellectual property disclaimers, as applicable; please see the City MIS Department for links or templates.
- Users and visitors to City Social Media sites shall be notified that the intended purpose of the site is to serve as a mechanism for communication between City departments and members of the public. City Social media site articles and comments containing any of the following forms of content shall not be allowed:
    - Comments not topically related to the particular social medium article being commented upon;
    - Comments in support of or opposition to political campaigns or ballot measures;
    - Profane language or content;
    - Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, marital status, status with regard to public assistance, national origin, physical or mental disability, sexual orientation, or gender identity;
    - Sexual content or links to sexual content;
    - Solicitations of commerce;
    - Conduct or encouragement of illegal activity;
    - Information that may tend to compromise the safety or security of the public or public systems; or
    - Content that violates a legal ownership interest of another party.
    - Any content removed based on these guidelines must be retained, including the time, date and identity of the poster when available.
- The City reserves the right to restrict or remove any content that is deemed in violation of this Social Media policy or any applicable law.
- Submission of comments by members of the public to City Social Media constitutes participation in a limited public forum, and is subject to record retention laws.
- Commentary on Social Media shall be moderated, and anonymous posting should be disabled or otherwise not allowed. Enrollment of public commentators shall be accompanied by valid contact information, including name, address and email address, as applicable.

- City Users who participate or otherwise engage in City Social Media must:
  - Identify themselves as a City Employee;
  - Conduct themselves in an appropriate manner, and keeping in mind that Material they post may be viewed by others as representing the City;
  - Add value to the City through your interaction, by providing worthwhile information and perspective;
  - Avoid comments or topics that may be considered objectionable or inflammatory;
  - Frame comments or opposing views in a positive manner;
  - Protect your privacy, the privacy of citizens, and other City information; ensure to follow all privacy protection laws;
  - Distinguish between personal commentary "when speaking for yourself", and not in their City capacity; and
  - Correct any mistakes or mistaken information that may be communicated, but not alter any previous posts without indicating that you have done so.
- City Users who participate in non-City Social Media are encouraged to:
  - Make it clear that they are speaking for themselves, and not on behalf of the City, through the use of a disclaimer along the lines of "The postings on this site are my own and do not represent the City's position(s) or opinion(s)."; and
  - To avoid using the City of Lowell seal, tagline, or other marketing related material in your Social Media to avoid confusing visitors, or suggesting the appearance that your Social Media posts are representative of the City's position, opinion, or view.

City Issued Device Policy

Advances in technology and cellular telephony services have enabled fast communication, email integration, remote wireless connectivity, and more productive mobile employees. The City may issue devices ("Devices") to Users to assist them with conducting City business-related activities. Devices include, but are not limited to, laptop computers, cell phones and pagers, tablets and GPS systems, and radio and wireless equipment.

Use of City issued Devices is subject to the following:

- City Devices must be properly recorded, inventoried, asset tagged, and registered as appropriate.
- City Devices do not include any accessories beyond what is factory shipped. If Users wish to add any accessories, it must be either funded by the User or through the User's department.
- It is the User's responsibility to ensure that City issued Devices are kept in a safe, functioning and reasonable condition. Equipment must remain free of any writing, drawing, stickers, or labels that are not the property of the City. It is the Department's responsibility to fund, acquire, and install cases designed to minimize damage to Devices. Users should contact the City MIS Department with any questions about how to maintain City issued Devices, cases for them, or training on them.
- No data, including but not limited to confidential information, should be permanently stored on City Devices; to maintain the integrity of City Materials, frequent data backups and transfers must be maintained between City Resources and City Devices.
- City Devices should not be left unattended in public places, or in places where they may be subject to harsh environmental conditions.
- City Devices which are damaged, lost, or stolen must be reported to Management as soon as possible; Users may be responsible for damages or replacement, as determined by Management. The City may, at its own discretion, choose to remotely wipe or reset lost or stolen Devices, and Users agree to assist with Device recovery as applicable.
- City Devices must be returned upon separation of employment. Users are responsible for ensuring that City Materials are properly transferred prior to being returned, and that Devices are completely unlocked and ready for redeployment as appropriate.
- The loss or theft of a City Device must be reported to the City MIS Department immediately, along with a summary of the data and/or any PID information which may have been on the City Device.

Personal Device Use Policy

The City recognizes that Users may have privately owned or personal Devices (“Personal Devices”) which they are interested in (1) using for City business-related purposes, (2) using for personal use while leveraging the City’s Resources (e.g., City or public Internet connectivity), or (3) using for purely personal use while leveraging their own private Internet connectivity (e.g., personal cellular connectivity).

Use of Personal Devices is subject to the following:

- All Personal Devices which use City Resources are subject to the City Technology Policy.
- The use of Personal Devices being used for purely personal use while on City property or otherwise representing the City, must be conducted in a manner that doesn’t needlessly interfere with their own work, the work of others directly or indirectly, cause offense to others, violate any applicable laws, or otherwise violate any City policies (e.g., sexual harassment, etc.).
- The City will not be responsible for any Personal Devices, or any damage or loss that might arise from using Personal Devices to remotely connect to, interface with, integrate with, or interact with City Resources, regardless of whether it is being used for City business-related purposes or personal use.
- Integration of Personal Devices with the City’s Resources (e.g., for access to email) must be authorized by Management in advance.
- Only ActiveSync compatible Personal Devices or Personal Devices which can run the Microsoft Outlook application are allowed to synchronize directly with the City’s Email systems. By using ActiveSync to synchronize your Personal Device with the City’s Email system Users agree to allow their Personal Device to be remotely wiped or reset in the event that the Personal Device is lost or stolen, in order to protect access to the City’s Resources and any PID information which may be on the Personal Device.
- The City will neither integrate nor support 3rd party applications on Personal Devices into City systems.
- Technical support for Personal Devices is limited to instructional support only; any support beyond instructional support (e.g., hands on support, or installation/configuration support) must be handled in a manner independent of the City (e.g., using support options available through the manufacturer).
- The use of non-Personal Devices (e.g., equipment owned by another organization or business, etc.), are not supported in any capacity, and are not allowed to connect into the City’s networks or technology.

ID & Access Badge/Credentials Policy

The City may choose to issue Users an ID & Access Badge/Credentials ("ID") in order to (1) identify themselves when working with other employees, citizens, or businesses while representing the City, and (2) for controlled access to authorized areas.

Use of City issued IDs is subject to the following:

- IDs are to be used for identification purposes and for controlled access to authorized areas.
- IDs require the Users' photograph, name, employee number, and job title.
- IDs are assigned to specific Users, and should not be shared.
- Users are responsible for all activity conducted through the use of their ID.
- Photographs taken for use with IDs become the property of the City of Lowell, and may be incorporated into other City systems, as deemed appropriate.
- IDs should not be defaced in any way – do not write on it, place labels on it, or punch holes in it.
- IDs should be displayed or otherwise available whenever conducting City business, or otherwise representing the City.
- IDs must be presented for review when requested.
- Lost, stolen or otherwise misplaced IDs, it must to be reported to MIS immediately so that they may be deactivated, and another issued as appropriate.
- IDs are the property of the City of Lowell, and must be surrendered upon demand.

Duty To Care For And Responsibility To Maintain City Technology And Materials

Throughout the course of employment with the City, Users may create and work with a variety of Materials, and acquire and work with a variety of Technology. **All City Materials (whether hard copy or electronic) are subject to Commonwealth of Massachusetts' records retention laws, and All City Technology should be properly inventoried and taken care of to avoid compromise, damage, or loss.**

All Users have a duty to care for and a responsibility to maintain City Technology and Materials in accessible and good working condition at all times, and to prevent them from events which may jeopardize City services, whether internal, external, deliberate, or accidental. This includes but is not limited to City issued laptops, monitors, smart phones, IDs, multifactor authentication devices, etc. All technology purchases must be presented to MIS within 30 days of receipt for review, asset tagging, registration, and recording into the City's inventory and technology management system(s).

Leading up to and upon separation from the City, Users are responsible for ensuring that any City Materials which they have created or otherwise worked with are neither modified, deleted, removed, or otherwise impacted, accordingly. Likewise, Users are responsible for ensuring that any City Technology which may have been assigned to them is in working condition, accessible, and unlocked (e.g., passwords removed, or logged with MIS accordingly, etc.).

If an employee is separating from the City, it is critical that neither emails nor data files be deleted or otherwise removed. Generally speaking: (1) Emails should NOT be deleted or otherwise purged from the City's systems; (2) Data files should NOT be deleted or otherwise purged from Devices or the Network; and (3) Neither Emails nor Data files should be released or otherwise shared with unauthorized personnel.

[This page intentionally left blank]