RESOLUTION NO. 2022- 14

A RESOLUTION OF THE CITY COUNCIL OF THE TOWN OF ASHLAND CITY AMENDING THE IT POLICY

WHEREAS, the City Council for the Town of Ashland City has established an IT Policy by Resolution 2021-30; and

WHEREAS, the IT Policy shall be amended with the attached changes.

NOW, THEREFORE BE IT RESOLVED BY THE MAYOR AND COUNCIL OF THE TOWN OF ASHLAND CITY, TENNESSEE, that the IT Policy updates and changes, attached hereto, is hereby approved and adopted and shall replace any previously adopted sections of the IT Policy and shall become effective immediately following passage of this resolution.

We, the undersigned City Council members, meeting in Regular Session on this 12th day of April, 2022 move the adoption of the above Resolution.

Councilmember _____ moved to adopt the Resolution.

Councilmember Jean Adkins seconded the motion.

Voting in Favor 6 Voting Against 0

Attest:

Steve W. Allen
Mayor Steve Allen

Alicia Martin
City Recorder Alicia Martin, CMFO

Information Technology (IT) Policy

Information Technology Citywide Technology Standards

This policy provides procedures, standards, and guidelines to plan for, acquire, implement, and manage the City's computer systems. To satisfy that intent, rules have been formulated to ensure that information resources fit together in a citywide system capable of providing ready access to information, computing, and communication resources. This policy and related information technology standards apply to hardware and software acquired and/or developed by all departments. While every attempt is made to respect the privacy of our users, general usage is monitored in order to detect unauthorized access and illegal activities. When illegal or inappropriate activities are suspected, users' files may be inspected. Anyone making use of this computer system expressly consents to such monitoring and is advised that evidence of criminal activity may be provided to law enforcement officials. The development of a citywide computer system requires the establishment of technical standards based upon international industry standards to the maximum extent possible. Information Technology is responsible for establishing, updating, and communicating the City's Information Technology Standards. The City's dependence on computer technology requires policies and procedures to provide adequate protection for these resources. For these reasons, internal procedures will address security for standalone and shared computer resources. All City Departments will apply the Information Technology adopted Information Technology Policies and standards to all procurement and application development projects to the maximum extent possible. Exemption Process Occasionally, departments may have special conditions or extraordinary requirements that prevent them from conforming to a standard. Department managers may request an exemption from the Information Technology Department.

IT Mission

To provide innovative and secure technology serving the city government and its residents.

IT Vision

Connecting employees and citizens using efficient, leading-edge technology to promote enhanced government services.

IT Values

- Accountability
- Teamwork & Coordination
- Confidentiality & Privacy
- Adaptability & Flexibility
- Achievement & Excellence

- Creativity & Innovation
- Respect
- Hard Work & Effort
- Customer – Focused

Responsibilities of the Department of Information Technology

- The information technology (IT) department shall be responsible for maintaining, installing, upgrading, and supporting all information technology hardware, software, and online systems; providing internet security; backing up data; researching and providing technical expertise for information technology-related issues.
- The IT department shall provide services to all departments of the city.

Powers and duties of the Department of Information Technology

- Manage and coordinate internal information technology systems and data processing functions.
- Coordinate the acquisition, development, and implementation of computer applications, and recommend changes and improvements to operations and programming.
- Direct the design, coordination, and operation of the local and wide area network and the evaluation and implementation of computers though out the city.
- Develop and operate automated information systems for the purpose of providing efficient data handling.
- Coordinate with departments, recommend and establish policies, procedures, and standards for the development of the City's technology operations, subject to the approval of the Council.
- To provide leadership to the city council, Mayor, and directors on the alignment of technology with city initiatives, planning priorities, policy, and strategic objectives.

Acquisition of Technology Resources

No City Department Head or employee shall acquire, through purchase, lease or any form of contract, any information technology resources for the City except through, in coordination with, or in accordance with, policies, guidelines, standards, and procedures established by the Technology Department and subject to approval by Council.

Guidelines for Technology Policy

- No one shall use any City computer or network facility for non-City business without proper authorization.
- No one shall connect any computers or equipment to City's network unless approved by Information Technology

- No one shall download, copy or install any software that violates copyright or licensing agreements.
- Games are prohibited on ALL City computers.
- No one shall use City E-mail for personal correspondence.
- No one shall give any passwords for any City computer to any unauthorized person, nor obtain any other person's password.
- No one shall misrepresent his or her identity or relationship to the city when on the Internet or E-mailing.
- City personnel may use the Internet for personal use while on breaks or as permitted by their Department Head.
- No one shall attempt to gain unauthorized access to other users' files or systems.
- Users shall not use any other e-mail services on City-owned computers other than those provided by Information Technology.

City computers and network facilities comprise all computers owned or administered by the Town of Ashland City that are connected to the City's communication facilities, including departmental computers, mobile devices, and voice over IP telephones, and also the City's computer network facilities accessed by anyone from anywhere. Some exclusions apply to the City's guest network as it is open to everyone.

Violations of these policies incur the same types of disciplinary measures as violations of other City policies or state or federal laws, including criminal prosecution in serious cases.

(A) No one shall use any City computer or network facility without proper authorization. No one shall assist in, encourage, or conceal from authorities any unauthorized use, or attempt at unauthorized use, of any of the City's computers or network facilities. Comment: Computers and networks are just like any other City facilities – they are to be used only by people who have permission. Using a computer without permission is theft of services and is illegal under state and federal laws.

(B) No one shall knowingly endanger the security of any City Computer or network facility, nor willfully interfere with others' authorized computer usage. Comment: Many of the other regulations given here deal with specific acts of this kind. You should not assume that other malicious acts or deliberate security violations are permissible merely because there is no specific rule against them.

(C) No one shall use the City's communication facilities to attempt unauthorized use, nor to interfere with others' legitimate use, of any computer or network facility anywhere. Comments: State and federal laws forbid malicious disruption of computers. Town of Ashland City does not tolerate individuals who invade others' privacy, steal computer services, or commit misrepresentation or fraud; nor pranksters who attempt to disrupt computers or network facilities for any other purpose. The mere lack of security measures does not mean that a computer is open to anyone who wishes to use it. The same goes for unauthorized use of communication paths.

(D) No one shall connect any computer or device to any of the City's networks unless it meets technical and security standards and is specifically approved by Information Technology. Comments: The applicable requirements depend on what kind of connection is being made. For example, connecting to the citywide network requires special authorization, because one improperly configured machine on a network can cause widespread disruption.

(E) All users shall share computing resources in accordance with policies set for the computers involved, giving priority to more important work and cooperating with other users of the same equipment. Comments: If you need an unusual amount of disk space, CPU time, or other resources, check with the administrators in charge of the computer rather than risk disrupting others' work. When resources are tight, work that is necessary to the City's mission must take priority over computing that is done to pursue personal interest or self-training on side topics. Also, no matter how important your work may be, you are only entitled to one person's fair share of the machine unless additional resources are available and appropriate permission has been granted. Priorities for any particular machine are set by the administrators in charge of it in consultation with the user community. Obtaining extra computer resources through any form of deception (e.g., secretly opening multiple accounts, misrepresenting the nature of your work, or the like) is strictly prohibited.

(F) No one without specific authorization shall use any City Computer or network facility for noncity business. Comments: By law, the city can only provide computer services for its own work, not for private use. In this respect the City's computers are different from those owned by colleges or corporations. It is improper to use the City's computers for political campaigns, fund-raising, commercial enterprises, mass mailings, or other outside activities that have not been granted the use of the City's facilities. Do not store personal files, including but not limited to, pictures, documents, and music on City computers. The Information Technology Department reserves the right to remove personal files from City computers. You should be aware that the ability to use a computer and/or service does not constitute permission or authorization. If you have questions, contact your supervisor or someone from the Information Technology Department.

(G) No one shall give any password for any City computer or network facility to any unauthorized person, nor obtain any other person's password by any unauthorized means whatsoever. No one except the System or LAN Administrators in charge of a computer is authorized to issue passwords for that computer. Comments: Giving your password to an unauthorized person can be a crime under Tennessee law. The criterion is not whether you trust them, but whether the city has authorized them. Passwords protect the City's network, not just the individual machines to which they apply. The city insists that each account be used only by the person to whom it belongs, so that if problems are detected or abuse is alleged, the responsible person can be identified. If a department cannot keep passwords secure, it cannot connect its machines to the citywide network. In general, you should never share your password with anyone else. Likewise, you must never use or disclose a password that was given to you improperly. Do not store the password for one computer in another computer. It is easy for anyone to walk up to your personal computer and retrieve passwords that are stored in it or written on paper around the computer. Passwords must

be changed every 90 days. You are responsible for choosing a secure password. Don't use names, nicknames, phone numbers, or recognizable words in any language, because some people guess passwords by automatically trying every word in a large dictionary. A strong password should include upper- and lower-case letters, numbers, and/or symbols. Also, a phrase such as "57ityMwb" is a good password, and it's easy to remember because it stands for "57 is the year Michael was born." Your password is secret. System or LAN administrators will not typically ask you for it. The computer will never ask you to type it unless you are logging in or changing your password. Beware of computer programs that ask you to "log in again" or type your password at any other time; they are likely to be scams. (There are rare exceptions on some computers; check with your system manager. If anything, that you don't understand ever happens after you type your password, then change your password immediately.) In some situations, the city authorizes more than one person to a single account, but this is seldom the best way to conduct collaborative work. Instead, use file sharing, groups, and related features of the system you are using. Email can be redirected automatically to an assistant, who can then forward it to you using a separate mailbox.

(H) No one shall misrepresent his or her identity or relationship to the City when obtaining or using City computer or network privileges. Comments: Naturally, you must not claim to be someone else, nor claim to have a different relationship to the city than you actually do, when obtaining a computer account or access to a lab. You must not falsify your name, address, email address, or affiliation when sending email or other messages from a city computer. Doing so can be illegal as well as being an unacceptable use of the City's facilities. On some systems, there are ways to post messages without revealing your name and address. Anonymous communication is permissible when there is a legitimate need for additional privacy. It is not a cover for fraudulent or obnoxious behavior, and in cases of abuse, anonymous messages may be traced to their source. Deceptive communication, in which you claim to be some other specific person, is never permitted. You can create confusion, and possibly violate trademark law, by using someone else's trademark as your name on the internet.

(I) No one without specific authorization shall read, alter, or delete any other person's computer files or electronic mail. This rule applies regardless of whether the operating system of the computer permits these acts. Comments: Do not try to guess or steal other people's passwords, or read their files, even if the computer permits this.

(J) No one shall download, copy, install, or use any software or data files in violation of applicable copyrights or licensing agreements. Comments: This rule forbids making unauthorized copies, for use elsewhere, of software residing on the City's computers. It also forbids installing or downloading ANY games or using pirated software on City computers. Unauthorized copying is usually a violation of federal copyright law. Some software is "site licensed" and can be used on any City computer. (The terms of various site licenses differ.) Some software is genuinely free; the author allows everyone to use it free of charge. Before copying software, be sure what you are doing is legal, and consult people who have full information. If strangers show up at your computer site saying they are there to check software licenses, you should immediately contact Information Technology and

your administrative superiors. Software licenses do not normally authorize these surprise inspections, and there is a substantial risk that the "inspectors" are not legitimate.

(K) No one shall create, install, or knowingly distribute a computer virus, "Trojan Horse," or other surreptitiously destructive program on any City computer or network facility, regardless of whether any demonstrable harm results. Comments: A virus is a hidden computer program that secretly copies itself onto users' disks, often damaging data. A Trojan horse is a program with a hidden, destructive function, or a program designed to trick users into revealing confidential information such as passwords. Even when the harm done by programs of these types is not readily evident, they confuse beginning computer users, degrade CPU performance, and waste the time of system managers who must remove them.

(L) No one without proper authorization shall modify or reconfigure the software or hardware of any City computer or network facility. Comments: Do not modify the hardware, operating system, or application software of a city computer unless someone has given you explicit permission to do so from Information Technology. The other users with whom you share the machine, and the technician on whom you rely for support, are expecting to find it set up exactly the way they left it. City personnel shall adhere to the software license agreement provided with each software product purchased. Only city owned software shall reside on City owned computers. Authorized evaluation software may be permitted for a fixed period of time. Software is copyright protected in the same manner as other media such as records, books, and film. The fact that software is so easy to copy does not legitimize its duplication. The City will purchase and track the requisite number of licenses and use all commercial software in accordance with licensing agreements.

- The following procedures shall be followed to ensure adherence to software licensing agreements:
    1. Software may be loaded onto City computers only if (1) it is licensed by the City, or (2) it is licensed to an employee of the City and IT, or Department Head has approved its use.
    2. Users are responsible for ensuring that backups of critical data files are made. Users may contact Information Technology for assistance with backups.
    3. Configuration of each workstation shall be determined first by citywide policy and then departmental policy. Only within those parameters is personal preference to be exercised. Information Technology personnel may reconfigure systems and delete unauthorized software and data. Any exceptions, which have been authorized, should be noted in a file.
    4. Computers or terminals shall not be left unattended in a state, which affords unauthorized access to records that compromises security.

(M) Users shall not place confidential information in computers without protecting it appropriately. The city cannot guarantee the privacy of computer files, electronic mail, or other information stored or transmitted by computer unless special arrangements are made. Comments: Due to the nature of most e-mail systems, the physical security of

messages cannot be guaranteed. As with voice mail and fax, e-mail systems transmit information through wires or through the airwaves. Because there is a security risk in the use of e-mail, it is suggested that care be taken when transmitting sensitive and non-public data through e-mail. Depending on the content, there may be times when e-mail is not the appropriate vehicle to send a message. The contents of the message determine whether the message is public or non-public. Remember that public data is accessible to the public.

Example uses of e-mail that will not be tolerated:

- Illegal activities
- Wagering, betting, or selling chances
- Harassment
- Fundraising, except for agency-sanctioned activities
- Commercial activities
- Other unethical activities

Since the e-mail messages are City records, you should be aware that department heads have the right to access them at any time with the assistance of the Information Technology department. However, the content of e-mail messages is not routinely monitored or disclosed. Monitoring or disclosure may occur under subpoena or other legal actions, in connection with charges of improper or illegal actions by an individual, unexpected absence of an employee, disciplinary proceedings against an employee, and other appropriate business or technical reasons. Problems or issues regarding agency e-mail should be directed to the Information Technology Director and/or department heads. Ordinary electronic mail is not private. Do not use it to transmit computer passwords, credit card numbers, personally identifiable information (PII) or information that would be damaging if made public. Bear in mind that some records are required by law and by City policy, to be kept confidential. It is also necessary to protect confidential information about employees. The city will normally respect your privacy but cannot guarantee it absolutely. There are many ways a normally private file can end up being read by others. If email is misaddressed, it may go to one or more recipients who will read it and try to correct the address. For your own protection, system administrators will often look at unusual activity to make sure your account hasn't fallen victim to an attack. Encryption is available for portable devices and email. Contact the Information Technology department for more information. The Tennessee Open Record Act applies to information stored in computers. This act gives citizens the right to obtain copies of "public records" as defined by state law. Requests for public records must be made through proper administrative channels. If you are using personal email to conduct City business, your personal email would become subject to public record requests. If you have a concern regarding any possible violation of the above rules by anyone, please forward the message with your complaint to Amartin@ashlandcitytn.gov.

(N) Users shall take full responsibility for messages that they transmit through the City's computers and network facilities. No one shall use the City's computers to transmit fraudulent, defamatory, harassing, obscene, or threating messages, or any communications prohibited by law. Comments: Electronic mail (e-mail) is an authorized and recommended method of inter and intradepartmental communications. All City personnel who are assigned an individual e-mail address shall become proficient in the use of the e-mail system. Personnel that have been assigned an individual email address should check incoming messages in a timely manner each workday. All personnel should respond to e-mail, which requires a response, in a timely manner. Any use of technology provided by the

City is considered to be public record and may be subject to public disclosure and/or review by authorized city managers in accordance with applicable law. Personnel should understand that they have no legitimate expectation of privacy with regard to any use of technology provided for their use by the city (including but not limited to email, text messaging, internet usage, and telephone/cell phone usage). Never send or keep anything that you would mind seeing on the evening news or being subject to public disclosure. Routine back up of electronic mail will occur as part of the system maintenance. You have exactly the same responsibilities on the computer network as when using other forms of communication. You must obey laws against fraud, defamation, harassment, obscenity, solicitation of illegal acts, threatening or inciting violence, and the like. Bear in mind that uninvited amorous or sexual messages are likely to be construed as harassment. If you are bothered by uninvited email, ask the sender to stop, and then, if necessary, consult your system administrator. Use of the computers to circulate chain letters and pyramid schemes is not permitted. If someone says, "Forward a copy of this to everyone you know on the Internet," don't. Such messages often contain misunderstood or outdated information, or even outright hoaxes. Even when the information is legitimate, chain forwarding is a needlessly expensive way to distribute it. Never participate in schemes to deliberately flood a computer with excessive amounts of email. "Mail bombing" can incapacitate a whole computer or even a whole subnetwork, not just the intended victim. It is considered good practice to use your real name, rather than a nickname or pseudonym, in the headers of all outgoing communications. Use of nicknames is often interpreted as a sign of immaturity or an indication that you are not taking full responsibility for what you are sending out. All users should be aware that there is no guarantee that electronic mail actually came from the person or site indicated in it. Deceptive electronic mail is easy to fake, including the technical information in the header. Doing so is of course prohibited and is in many cases against the law. Hoaxes, pranks, and con games are common on the Internet. Be on the lookout for misguided "warnings" (about computer viruses, impending legislation, etc.) and false appeals for charity (usually involving dying children). If you get a message that spurs you to take immediate action, it is very likely to be a hoax, even if the person who passed it along to you was perfectly sincere. Also, genuine appeals that are several years old are still circulating as if they were current. Rather than spreading the appeal or "warning", post a question to the Information Technology department. Use prudent caution when sending out any messages that appears to be an official communication from the city. If the header identifies your message as coming from an administrative office or from the office of someone other than yourself (e.g., "City Clerk"), recipients will presume that you are speaking for that office or person. It is important to distinguish actions taken to punish a person from actions taken to protect a system. If your account appears to have been misused or broken into, your system administrator will inactivate it and contact you or wait to hear from you. This is done to stop the misuse and does not presume that you are the guilty person; you can expect to have your privileges reinstated right away, with new password, as soon as you identify yourself and indicate willingness to follow the rules. Thus, you can resume using the computer while investigation of the incident continues.

(O) Those who publish World Wide Web pages or similar information resources on City computers shall take full responsibility for what they publish; shall respect the acceptable-use conditions for the computer on which the material resides; shall obey all applicable laws; and shall not publish commercial advertisements. References and links to commercial sites, advertisements, and especially paid advertisements, are not permitted. Users shall not accept payments, discounts, free merchandise or services, or any other remuneration in return for placing anything on their web pages or similar facilities. Comments: All Internet users are expected to be responsible cyber-citizens. That means

knowing the tools, rules and etiquette and behaving accordingly. This includes the selection of materials to post; posts should reflect well on the City and not violate anyone's trust or copyright laws. The viewing, downloading or printing of pornography is strictly prohibited. Any personnel caught viewing, downloading or printing pornography may be subject to MAJOR disciplinary action. Personnel are encouraged to use Internet for research, education, and communications, provided it is for City related business. Personnel shall not use the Internet for non-city business use while on City time. City personnel are not permitted to use the Internet or wide area network services for any illegal purpose. This includes unauthorized access to protected resources for the city. Transmitting unprofessional communications or using City resources for unsolicited advertising for personal gain is strictly prohibited. The information technology department uses network equipment to block access to specific parts of the Internet that by definition have no valid use normally here at the Town of Ashland City. Examples of these areas include pornography, gambling and streaming media. If you find that in the course of your job that you need access to these web sites, your department manager should submit a request to human resources to request access. Human Resources will approve the request and submit a help desk ticket to information technology to grant the requested access. Web pages on the City's network are subject to the same rules as other uses of the same facilities. Different City computers are set up for different purposes; System administrators can advise about what is permitted at any particular site. Only Town of Ashland City Departments are allowed to have pages hosted on the City's computer systems. Furthermore, only links to government agencies will be allowed on the City's web page(s) unless other links are specifically approved by Information Technology. When you publish something on the World Wide Web, you are putting it before a potential audience of millions. You have the same responsibilities as if you were publishing a newspaper. If the content is libelous or deceptive, people can sue you and you can be held personally liable. Since there are laws against distributing obscene material (not just creating it), a link to an obscene web site can be a violation of the law. This is true regardless of the status of the Communications Decency Act or other new laws that specifically mention computers. You are not allowed to view any material that is sexually explicit or obscene. Additionally, the City's sexual harassment policy prohibits you from displaying sexually explicit material, which interferes with anyone's work or personal performance or creates an intimidating, hostile, or offensive environment. If you want to reproduce copyrighted pictures, cartoons, or comic strips on your web page, you must have the copyright owner's permission. It is not sufficient to reproduce the owner's copyright notice; you must actually obtain permission for yourself. Brief textual quotations do not always require permission as long as the source is acknowledged and you are not reproducing a complete work (poem, essay, etc.). You must not accept payments, discounts, or anything of value in return for placing anything on your web page. The City's disk space and communication capacity are not yours to sell. This applies to all computers directly connected to the City's network, even if they are privately owned.

(P) Users shall not utilize any electronic mail services other than those maintained by Town of Ashland City's Information Technology Department. Comments: You are prohibited from using other mail services such as AOL, Yahoo™, Hotmail, MSN, etc. on City computers. These types of servers cause several problems including (but not limited to) a lack of security and increased bandwidth usage.

(Q) Data which is exempted from disclosure under the Freedom of Information Act (Public law 93-502) or whose disclosure is forbidden by the Privacy Act (Public law 93-579) will not be

transmitted over the Internet network unless encrypted. Comments: Logon Ids and passwords are frequently classified as sensitive information.

(R) Users shall not store City data on personal online storage accounts. Comments: User data belongs to the City and shall only be stored on City approved servers and cloud solutions.

(S) Users shall report any suspicious activity to the Information Technology department immediately. Comments: Users should call the Information Technology department immediately. Users should then notify their supervisors of the suspicious activity. New state and federal laws concerning computer abuse continue to be passed, and important court decisions occur frequently. For up-to-date guidance about specific questions, consult the Information Technology Department

Computer Usage (Possible Employee Misuse)

Purpose

In order to ensure that Town of Ashland City work rules and procedures are being followed, a department head or Human Resources may need to review the use of a computer or the network (including the Internet) at the Town of Ashland City. This policy provides a process by which IT is authorized to monitor and report the use of City computers and files stored on any computer or server on the network and the Internet.

Policy

IT will not initiate the monitoring of the usage of any computer on the Town of Ashland City network without the authorization as described below.

- Any request under this policy will be kept confidential by the IT department.
- To request the monitoring of the usage of a Town of Ashland City computer, the department head and HR director will jointly contact IT. The request will include the beginning and ending date for the requested monitoring.
- To request access to an employee's email, a date range or keywords should be provided. If the employee email access is for a department head, the HR director or the mayor can initiate the request.
- To request access to an employee's files stored on the network, the department head will contact IT. If the employee file access is for a department head, the HR director or the mayor can initiate the request. IT will provide access to the employee's files for the department head.

Email Signature

All emails should be signed with employee first and last name, job title, department name, town name and logo. And all emails should have the following disclaimer:

Disclaimer: This electronic message may contain information that is CONFIDENTIAL or legally privileged. It is intended only for the use of the individual(s) and entity named in the message. If you are not an intended recipient of this message, please notify the sender immediately and delete the material from your computer. Do not deliver, distribute, or copy this message and do not disclose its contents or take any action in reliance on the information it contains.

IT Ticketing

All employees must submit an IT ticket through the Freshdesk Support Portal in order to receive technical support or assistance. The IT department receives a high volume of requests from all departments daily and in order to be efficient and productive, this will be the most effective way to track all incoming requests.

As an employee of the Town of Ashland City, I certify that I have read and understand the IT Policy. I agree to abide by the policy.

_____ _____

Employee Date

_____ _____

Human Resources Date