Use of Information Technology Systems and Resources

I. Policy

Information Technology (IT) Systems and Resources enable the City of Gainesville ("City") to effectively and efficiently fulfill its municipal purposes. The purpose of this policy is to ensure that the City's IT Systems and Resources are used for their intended purposes, to define authorized and prohibited uses of the City's IT Systems and Resources, and to protect the integrity, availability, and performance of the City's IT Systems and Resources. Based on the foregoing purposes, it shall be the policy of the City to allow use of its IT Systems and Resources so long as Users conduct themselves in a responsible, efficient, professional, and ethical manner and in accordance with all City human resources policies, procedures, ~~and~~ guidelines, and practices, as well as federal, state, and local laws.

In addition, the purpose of this policy is to address the use of IT Systems and Resources not owned or leased/licensed by the City to conduct official City business. To ensure that electronic information related to official City business is properly stored and protected, it is the preference of the City that users conduct official City business on City IT Systems and Resources instead of Personal IT ~~s~~Systems and Resources.

II. Scope

This policy, and all policies referenced herein, ~~applies to~~ apply to all members of the City workforce, including staff, interns, temporary employees and independent contractors ~~all Users~~ (the "User(s)" or "you") who use, access, or otherwise employ, locally or remotely,~~of City~~ the City's IT Systems and Resources~~Personal IT Systems~~, whether individually controlled, shared, stand-alone, or networked.

III. Definitions

a. "City IT Systems and Resources" includes computing, networking, communications, applications, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based systems, Software as a Service (SaaS) systems, and any related materials and services, ~~means any computer system, software, accounts, or network (wireless or otherwise) used to receive, store, process, or distribute data that is~~ owned or leased by the City or licensed for use to the City. ~~Such systems include~~

~~desktop computers, laptop computers, portable storage devices, telephones, cellular phones, pagers, personal handheld devices, printers, global information systems, voicemail, electronic mail, internet, intranet, social media networks, text messaging services, instant messaging services, and any other computer system, software, or network used to receive, store, process, or distribute data.~~

b. "Personal IT Systems and Resources" means any computer system, software, accounts, or network (wireless or otherwise) used to receive, store, process, or distribute data, that is not owned or leased by the City but is ~~nevertheless~~ used for official City business. Such systems include desktop computers, laptop computers, portable storage devices, telephones, cellular phones, pagers, personal handheld devices, printers, global information systems, voicemail, electronic mail, internet, intranet, social media networks, text messaging services, instant messaging services, and any other computer system, software, or network used to receive, store, process, or distribute data.

c. A "User" is any person or entity who uses any City IT System or Resource, or any Personal IT System or Resource from any location, whether authorized or unauthorized, including, but not limited to, City Commissioners, Board Members, regular employees, probationary employees, temporary employees, interns, volunteers, guests, vendors, and contractors.

IV. Authorization of Use

a. The City authorizes Users to use City IT Systems and Resources only to conduct and support official City business.

b. Only authorized Users have the privilege to access and use the City IT Systems and Resources. Access and use is limited to the purposes that are consistent with the business of the City.

c. Users are responsible for any activity originating from their accounts which they can reasonably be expected to control. Accounts and passwords may not be shared or be used by persons other than those to whom they have been assigned by the account administrator. In cases when unauthorized use of accounts or resources is detected or suspected, the user should change the password and report the incident to the appropriate account administrator.

d. All digital content used to conduct and support official City business must be stored on City IT Systems and Resources, and should not be stored on

Personal IT Systems or Resources, regardless of the method by which such content was generated or obtained.

b.e. The City purchases and licenses the use of different types of licensed content, including music, videos, graphics, text, and software, to conduct and support official City business on City IT Systems and Resources. Often the City does not own the copyright, its related documentation, nor does the City have the right to reproduce such content for use beyond the licenses purchased by the City. Users may only use licensed content on City IT Systems and Resources according to the City's license agreement(s).

c.f. Users are permitted de minimis personal use of City IT Systems and Resources so long as such personal use does not conflict with official City business, is at no cost to the City, does not interfere with the ability of the User to accomplish the functions of his/her position with the City, and otherwise complies with this policy, and all other City human resources policies, procedures, guidelines and practices, as well as federal, state, and local laws. Specifically, Users are permitted de minimis personal use of City IT Systems and Resources, limited to after or before regular business hours, or during breaks, unless otherwise authorized by a User's supervisor. De minimis personal use may be temporarily or permanently suspended, limited, or extended at the discretion of the User's supervisor. In accordance with section V of this policy, Users shall have no expectation of privacy or confidentiality in their use of City IT Systems and Resources, even if such use is personal in nature.

V. No Privacy or Confidentiality

Users shall have no expectation of privacy or confidentiality when using City IT Systems and Resources. The City IT Systems and Resources can and will be monitored at management's sole discretion through random and direct inspections, with or without notice, to ensure compliance with this policy.; and all City human resources policies, procedures, and guidelines, and practices; as well as federal, state, and local laws; and the terms of applicable contracts including software licenses. In addition, at any time, City IT Systems and Resources may be inspected or copied are subject to inspection and imaging to comply with the public records law, preserve evidence for litigation purposes, or defend the City in litigation. All contents of City IT Systems and Resources are the property of the City.

VI. Prohibited Uses of City IT Systems and Resources

Unless expressly authorized by the City, ~~such activities are directly related to official City business,~~ Users are prohibited from accessing or using ~~the~~ City IT Systems or Resources to engage in the following activities:

a. Initiating or participating in unauthorized mass mailings to news groups, mailing lists, or individuals, including, but not limited to, chain letters, unsolicited commercial email (commonly known as "spam") or political activity~~Violating the City's Equal Opportunity Policies, including but not limited to, using the City IT Systems to engage in inappropriate behavior based on race, color, gender, age, religion, national origin, marital status, sexual orientation, disability, or gender identity~~;
b. Using personal cloud based accounts by employees to transmit, share, store, download City Information/Data, without the prior approval of the City ~~Engaging in illegal activities~~;
c. Improperly storing, transmitting, accessing or securing HIPAA material ~~Accessing, possessing, or distributing pornography, obscene, or sexually oriented materials~~;
d. Giving others, by password or other means, unauthorized access to any User account or the IT Systems and Resources~~Distributing profane, harassing, or threatening communications~~;
e. Seeking to, without authorization, wrongly access, improperly use, interfere with, dismantle, disrupt, destroy, or prevent access to, any portion of the City IT Systems and Resources including User or network accounts~~Accessing, possessing, or distributing information or communications related to illegal drugs or illegal drug paraphernalia~~;
f. Violating or otherwise compromising the privacy, or any other personal or property right, of other Users or third parties through use of the City IT Systems and Resources~~Gambling or betting or accessing or distributing information related to gambling or betting~~;
g. Disguising or attempting to disguise the identity of the account or other City IT Resource being used including "spoofing" resource addresses, impersonating any other person or entity, or misrepresenting affiliation with any other person or entity~~Operating a private business or performing work for another employer~~;
h. Using the City IT Systems and Resources to gain or attempt to gain unauthorized access to networks and/or computer systems~~Using a false or anonymous identity~~;
i. Engaging in conduct constituting wasteful use of City IT Resources or which unfairly monopolizes them to the exclusion of others~~Knowingly distributing or launching computer viruses~~;
j. Engaging in conduct that results in interference or degradation of controls and security of the City IT Resources~~Installing software or hardware on City owned desktops or laptops without express, prior authorization from the City's IT Department (it is permissible to install software or hardware~~

~~on smartphones, tablets or other devices that are not members of the City's network)~~;

k. Exploiting or otherwise using the City IT Systems and Resources for any non-sanctioned commercial purpose~~Illegally downloading or copying content, including music, pictures, videos, graphics, text, or software~~;

l. Intentionally or unintentionally violating any applicable local, state, federal, or international law~~Soliciting on behalf of any cause, group, or outside organization without express authorization from the appropriate Charter Officer or designee~~;

m. Engaging in computer crimes or other prohibited acts~~Attempting to or successfully gaining access to any City IT System or information on such a system a User is not authorized to access~~;

n. Knowingly or negligently running, installing, uploading, posting, emailing, or otherwise transmitting any computer code, file, or program, including, but not limited to, computer viruses, Trojan horses, worms, or any other malware, which damages, exposes to unauthorized access, disrupts, or places excessive load on any computer system, network, or other IT Resource~~Distributing or accessing confidential or proprietary information, such as medical records, trade secrets, or copyrighted information, through the use of any City IT System without authorization~~;

o. Using any IT System or Resource, including email or other communication system or content to post or transmit any information, including data, text, files, links, software, chat, or collaboration, that is abusive, disparaging, discriminatory, combative, threatening, harassing, intimidating, defamatory, pornographic, or obscene; that insults or embarrasses others; or to create a hostile or offensive environment~~Engaging in political or religious activity~~; and

p. To interfere unreasonably with an individual's work, research, or educational performance~~Using City IT Systems for personal use that is not de minimis in nature~~.

~~p.~~

Periodically, the City will conduct information sessions to present, or provide through official communications, specific examples of inappropriate uses of the City IT Systems and Resources. In the interest of creating a well-informed User community, the IT Department also encourages questions about proper use. Please direct inquiries to the City IT Service Desk at (352) 393-1111, or the City Human Resources Department at (352) 334-5077. ~~The City has designed access to its IT Systems to ensure the safety and security of the City's IT Systems. Any attempt by a User, other than authorized members of the City's IT Department, to circumvent, disable, destroy, or defeat any City security feature is a violation of this policy. Any User, other than authorized members of the City's IT Department, who enables or disables anti-virus, security, or remote access applications on any City IT System will be in violation of this policy.~~

~~VII. Conducting Official City Business on Personal IT Systems~~

~~Users are prohibited from regularly conducting official City business on Personal IT Systems other than through the use of a VPN (or similar) connection to the City's network or webmail, and they are prohibited from regularly downloading City information or data onto Personal IT Systems. Users are also prohibited from regularly using personal e-mail, social media, or other electronic accounts to conduct official City business.~~

~~The City recognizes that a person or entity may communicate with a User regarding official City business on Personal IT Systems through no fault of the User. Such communications are not a violation of this policy; however, Users shall request the person or entity to communicate with the User through City IT Systems and, if possible, copy the electronic communication onto the City IT Systems. In addition, due to work requirements, it may be occasionally necessary to use Personal IT Systems to conduct official City business. Such occasional use is not a violation of this policy; however, Users shall, if possible, copy all electronic information related to official City business onto the City IT Systems.~~

~~To the extent that Users conduct official City business Personal IT Systems, without the use of a VPN (or similar) connection or webmail, such electronic information is fully owned by the City and such conduct will cause Users to lose any expectation of privacy in his/her Personal IT Systems. For example, in such a case, an employee's personal computer may be seized by the City to respond to a public records request or for discovery purposes during a lawsuit involving official City business.~~

~~VIII.~~VII. **Public Records**

In the course of using City IT Systems and Resources, and Personal IT Systems and Resources, Users may create or receive public records. If public records are in fact created or received, Users are required to retain such records and make them available for inspection and copying in accordance with Florida's public records law. For additional information regarding public records requirements, Users should refer to the City's public records policy and procedure.

VIII. Retention

Each individual User, designated as the custodian of their records is responsible for adherence to Florida Statute FS 119, City Policy and Administrative Guidelines for document retention and management.

IX. Non- Compliance with Use of Technology Policy

Violations of this policy may cost the City money, expose the City to risk, waste scarce resources, tarnish the City's image, and violate the law. Users who violate this policy are subject to a full range of penalties, including loss of use of City IT Systems and Resources without notification, disciplinary action, up to and including termination of employment, and all other penalties available under the law. In the event a User is suspected of violating federal, state, or local laws, all relevant materials will be made available to law enforcement for investigation and possible criminal prosecution.

X. User Obligation to Review

The City will periodically update this policy. By accessing and using the City IT Systems and Resources, each User represents and acknowledges that he or she has checked and read this policy on an annual basis.

Adopted: 11/17/11
Revised: 10/04/18