Use of Information Technology Systems

I. Policy

Information Technology (IT) Systems 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 are used for their intended purposes, to define authorized and prohibited uses of the City's IT Systems, and to protect the integrity, availability, and performance of the City's IT Systems. Based on the foregoing purposes, it shall be the policy of the City to allow use of its IT Systems 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, as well as federal, state, and local laws.

In addition, the purpose of this policy is to address the use of IT Systems not owned 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 instead of Personal IT systems.

II. Scope

This policy applies to all Users of City IT Systems and Personal IT Systems.

III. Definitions

a. "City IT Systems" means any computer system, software, accounts, or network (wireless or otherwise) used to receive, store, process, or distribute data that is owned by 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" means any computer system, software, accounts, or network (wireless or otherwise) used to receive, store, process, or distribute data that is not owned 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 Personal IT System 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 to conduct and support official City business.

b. 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. 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 according to the City's license agreement(s).

c. Users are permitted de minimis personal use of City IT Systems 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, as well as federal, state, and local laws. Specifically, Users are permitted de minimis personal use of City IT Systems, 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, 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. The City IT Systems 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, as well as federal, state, and local laws. In addition, at any time, City IT Systems may be inspected or copied to comply with the public records law, preserve evidence for litigation purposes, or defend the City in litigation. All contents of City IT Systems are the property of the City.

VI. Prohibited Uses of City IT Systems

Unless such activities are directly related to official City business, Users are prohibited from using the City IT Systems to engage in the following activities:

a. 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. Engaging in illegal activities;
c. Accessing, possessing, or distributing pornography, obscene, or sexually oriented materials;
d. Distributing profane, harassing, or threatening communications;
e. Accessing, possessing, or distributing information or communications related to illegal drugs or illegal drug paraphernalia;
f. Gambling or betting or accessing or distributing information related to gambling or betting;
g. Operating a private business or performing work for another employer;
h. Using a false or anonymous identity;
i. Knowingly distributing or launching computer viruses;
j. 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. Illegally downloading or copying content, including music, pictures, videos, graphics, text, or software;
l. Soliciting on behalf of any cause, group, or outside organization without express authorization from the appropriate Charter Officer or designee;
m. 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. 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. Engaging in political or religious activity; and
p. Using City IT Systems for personal use that is not de minimis in nature.

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. Public Records

In the course of using City IT Systems and Personal IT Systems, 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.

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 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.

Adopted: 11/17/11