USE OF CITY INFORMATION TECHNOLOGY POLICY & PROCEDURES

1. Purpose

The purpose of this policy is to establish City of Woodburn's policy and guidelines for the acceptable use and security of the City's information technology resources.

The City of Woodburn relies on its information technology resources to conduct official business. The City has created this policy to ensure that information technology resources are used properly by its employees.

2. Scope

This policy covers all employees, including seasonal, temporary, volunteers, and interns, and other authorized users such as contractors, consultants, and vendors ("users") granted access to the City's information technology resources.

To the extent any applicable collective bargaining agreement differs from the conduct and procedures set forth in this policy, employees represented by that bargaining unit will be subject to the terms set forth in that agreement. To the extent that police department specific policies differ from the conduct and procedures set forth in this policy, employees who work at the police department (both sworn and nonsworn) will be subject to the terms set forth by their department policies.

This policy shall not be applied to prohibit or infringe upon an employee's privileged or protected speech.

3. Definitions:

Information Technology Resources: Information Technology Resources are tools that allow access to technological devices, or are technological devices themselves that service information, access information, and includes the information itself. These resources include all City-provided computers and servers; desktop workstations, laptop computers, handheld computing and tracking devices; cellular and office phones; network devices such as data, voice and wireless networks, routers, switches, hubs; peripheral devices

such as printers, scanners and cameras; pagers, radios, voice messaging, facsimile transmissions, copy machines, electronic communications, external network access such as the Internet; software, including packaged and internally developed applications; and all information and data stored on City equipment as well as any other equipment or communications that are considered an Information Technology Resource or any new technologies used in the future.

Information Technology Manager: Information Technology Manager is the City's Information Technology Manager.

4. Policy

It is City of Woodburn's policy that the City's information technology resources are used responsibly, professionally, ethically and lawfully. City departments may develop more restrictive work rules based on the operational needs of the particular department.

5. Ownership and Monitoring

All information and communications in any format, stored by any means on or received via City of Woodburn's electronic equipment, facilities or services is the sole property of City of Woodburn. The City is the sole owner and may monitor and disclose contents and usage at any time of any Information Technology Resource provided to users. There is no reasonable expectation of privacy in the use of any Information Technology Resource.

Any data created, received or transmitted using City equipment usually can be recovered even though deleted by the user. Documents, emails and other electronic records created using the City's information technologies are public records and may be subject to disclosure. The City will preserve these records in compliance with City record retention and preservation policies. The City monitors the use of information technologies including e-mail, website visits, other computer transmissions and any stored information created or received by City employees with City's Information Technology Resources. Monitoring may include the generation of reports logging usage and printed or electronic copies of email or stored information. Use of the City's Information Technology Resources constitutes an express consent to monitoring at all times.

Accessing the City's internal networks from employee owned computing devices such as employee owned home computers, or any portable computing device (such as a laptop, smartphone, or other electronic device used to access electronic data) may subject the employee's personal devices to disclosure. When conducting City business using any personal computing device, including a home computer or portable computing device, employees and City Officials should always use City email.

The City makes an effort to block access to certain Internet content deemed by the Information Technology Manager to be of high risk to the City network and users. This content is typically one that has the potential to deliver malware to the City's network and/or users. Content will also be blocked if it is deemed inappropriate. That determination will be made in consultation with the Human Resources Director.

Requests for monitoring and reporting of a City Information Technology Resource use, including but not limited to the Internet activity or e-mail use of an individual employee or department and monitoring and reporting of video/audio recording of an employee must be submitted in writing by the Department Director to the Human Resources Director. These requests may include, but are not limited to monitoring the inappropriate use of information technology, the fulfillment of public records requests, or the electronic discovery of evidence for actual or potential litigation in which the City is an affected party. Requests for monitoring a specific employee's technology use should contain a reason for the request. Neither individuals nor groups need to be notified of monitoring. However, if the report indicates usage which violates City rules, all applicable requirements in a collective bargaining agreement or in the HR Rules must be followed prior to implementing discipline.

Reports on individual technology use are considered personnel information and should be viewed as confidential. Electronic content may also be confidential for other reasons and will be reviewed in a manner to protect that confidentiality and to comply with all applicable laws. All requests for disclosure should be referred to the City Attorney.

While personal passwords may be used for purposes of security, the use of a personal password does not affect City ownership of the Information Technology Resource accessed, or City's right to inspect such information. If passwords are applied to encrypted devices or individual files, the City may request those passwords at any time and the employee is obligated to provide the passwords. The City may override all personal passwords on City owned devices if it becomes necessary to do so for any reason.

6. Responsibilities

Users must comply with all aspects of this policy. Users are responsible for the acceptable use and security of designated Information Technology Resources. Users learning of, or reasonably suspecting any misuse of, Information Technology Resources must notify their supervisor. Users must accept accountability for all activities associated with their use of the Information Technology Resources related to their user accounts, and related access privileges.

Information Technology Resource users are responsible for the protection and security of Information technology resources. Information technology resources shall be protected, to the extent reasonably possible, from misuse, including, but not limited to: theft, unauthorized access and data transfers, fraudulent manipulation or alteration of data, attempts to circumvent the security controls, and any activity that could compromise the integrity or availability of data. The Information Technology Division is responsible for assuring that City approved anti-malware protections are installed, maintained, and active on all computers. Employees are expected to take all malware warnings seriously and to comply with procedures for reporting and responding to malware outbreaks. Deliberate transmission of data containing malware or willfully circumventing malware protection measures will be considered a breach of security and in violation of this policy.

Employees' use of Information Technology Resources must protect the integrity of the City's computer systems, data and networks. Employees' use of information technologies must also comply with all service and contractual agreements with commercial Internet service providers, and third-party intellectual property rights, copyright, and software license agreements.

Any user who receives communication or messaging that he or she reasonably suspects may be illegal or may reasonably be considered offensive, disruptive, harassing, and/or defamatory or threatening towards the City, any user, or any third party shall notify their supervisor.

Managers and supervisors are responsible for consistent enforcement of this policy. Any supervisor who knowingly permits a violation of this policy by employees under their direct supervision shall be subject to disciplinary action. Supervisors are responsible for limiting personal use of Information Technology Resource.

Public employees occupy a trusted position in the community, and thus, their statements have the potential to be perceived as the City's official stance. The City will carefully balance an individual employee's rights against the City's needs and interests when exercising a reasonable degree of control over its employees' speech and expression.

7. Acceptable Use

Employees should make every effort to use their personal devices for personal business. Information technology resources are provided solely for the conduct of City business. However, the City realizes and is aware of the large role technology (especially the Internet and email) plays in the daily lives of individuals. In this context, the City acknowledges that if an employee's personal device is unavailable, a limited amount of personal use of Information Technology Resources is acceptable. Unless otherwise

prohibited by law or department specific work rules, limited personal use is permitted according to the following guidelines:

1. It is incidental, occasional and of short duration;
2. It is done on the employee's personal time. Personal time means during breaks, lunch and/or before and after work as defined by collective bargaining agreements, City HR Rules and department policies;
3. It does not interfere with an employee's job activities. This includes activities which might pose a conflict of interest or appearance of impropriety with an individual's employment with the City;
4. It does not result in an expense to the City;
5. Any Information Technology Resources assigned to or in the possession of a user must be returned to the City when City management determines that the use of those resources is no longer required to conduct official City business;
6. It does not result in prohibited conduct as outlined in this policy;
7. It does not disrupt the Information Technology Division's ability to provide information technology services to City users; and
8. Anti-malware controls are used.

8. Prohibited Conduct

The following list of prohibited uses for information technologies is not intended to be all-inclusive. Except where it is otherwise protected by law:

Information technology resources must not be used for or contain any material that may reasonably be considered offensive, disruptive, harassing, defamatory or threatening towards the City, any user, or any third party. Furthermore, users are prohibited from engaging in any internal or external communications using Information Technology Resources that refer to violence, racism, sexism, drugs, illegal conduct, pornography, gambling, betting, or other subjects that would be offensive to a reasonable person in the work environment. Nothing in this section shall be construed to preclude any use that is objectively reasonably necessary for the performance of an employee's job responsibilities.

Users shall not violate software license agreements or any other contractual terms and conditions of using Information Technology Resources regardless of whether harm is intended.

Users are prohibited from introducing, downloading, or accepting any unauthorized Information Technology Resources into the City's environment or infrastructure.

Users are prohibited from anonymous use of Information Technology Resources. In practice, this means users must sign in with their uniquely assigned User ID before accessing/using Information Technology Resources. Similarly, "spoofing" or otherwise

modifying or obscuring a user's IP Address or any other user's IP Address is prohibited. Circumventing user authentication or security of any host, network, or account is also prohibited.

Users may not use City provided email addresses to create or manage personal accounts (e.g., shopping websites, personal bank accounts, and social media accounts).

A user forwarding a message, which originates from someone else, may not make changes to that message without clearly disclosing the exact nature of the changes and the identity of the person who made the changes.

Messages received from the City Attorney, or private attorneys acting on behalf of the City, its officers or employees, may be privileged communications and therefore, confidential, and these messages shall not be forwarded without the prior approval of the author.

If an electronic mail message comes to a user by mistake, the user should stop reading as soon as they realize the message was not meant for them, and delete the message, notify the sender or system administrator immediately.

Employees may not install hardware or software on City's computer systems without written approval from Information Technology Manager. All software installed on City's computer systems must be licensed. Copying or transferring of City owned software may be done only with the written authorization of the Information Technology Manager.

Users are prohibited from using Information Technology Resources for commercial gain; or the creation or distribution of chain emails and/or material that is in violation of City's harassment policy; consumption of City network and system resources for non-business related activities (such as video, audio or downloading large files) or excessive time spent using information technology resources for non-business purposes (e.g. shopping, social networking, sports related sites, et al).

It is prohibited to willingly engage in any action that renders the user's computer equipment unusable, or that interferes with another City employee's use of information technologies; use of City information resources, regardless of physical or electronic form or media, for the commission of an illegal act or grant or allow personal access by any person or entity to City information technology systems or data.

Users should not perform commercial endorsement or use City information technologies in a manner that would constitute an endorsement of a specific commercial entity, its products, services, or business practices. The City's e-mail system may not be used for commercial activities, religious causes, or support for other activities that are not related to the direct conduct of city business.

Use of City information technologies for political activity or in a manner that would directly or indirectly assist a campaign for election of any person to any office, or for the promotion of or opposition to any ballot proposition is prohibited. This prohibition shall not apply to the use of City computer or network resources for the development or delivery of a neutral and objective presentation of facts relevant to a ballot proposition as allowed by state law, provided that such use must be a part of the normal and regular conduct of the employees developing or delivering the presentation of facts.

Remote access to certain City systems, applications, and data is maintained for selected employees. City remote access systems require a high level of application and user maintenance as well as monitoring. In addition, they significantly increase the security risks associated with outside access to applications and data. Remote access systems are therefore restricted only to those City Officials and employees who show a demonstrated necessity to access data or applications while away from City facilities and only for City business.

User shall not destroy City records in violation of records retention and preservation policies.

Remote access to City systems has the potential to result in overtime payments. Time spent accessing data or email remotely is considered compensated time for employees subject to overtime rules. Overtime eligible employees are not allowed to use City issued mobile devices outside of work hours for work-related purposes. Overtime eligible employees are not allowed to have remote access to City IT systems, except with prior written approval from the department director before engaging in offsite work. Employees who conduct such work will record all hours engaged in work and will report it immediately through payroll.

9. Social Media

The users should refer to City's Social Media Policy concerning the use of social media.

10. References

Oregon Administrative Rules Chapter 166, Division 200 City general records retention schedule

Oregon Revised Code Chapter 192 Records, public reports and meetings

City of Woodburn HR Rules

City of Woodburn Non-discrimination policy and procedures

City of Woodburn Social Media policy and procedures

11. Review of Policy and Procedures

This policy will be reviewed every three years or as state and federal regulations are revised and necessitate a change in the policy or procedures.

Adopted: February 2018