ACCEPTABLE USE OF CITY INFORMATION TECHNOLOGY RESOURCES Policy 800-006

REFERENCE…. **ACCEPTABLE USE OF CITY INFORMATION TECHNOLOGY RESOURCES 800-006**
APPROVED BY/DATE…….. Chris Searcy, City Administrator – 3/31/2023
REVIEWED..... Mike Reynolds, City Attorney – 1/1/2021
REVIEWED..... Joe Nanavich, Information Services Director – 3/31/2023

Table of Contents

ACCEPTABLE USE OF CITY INFORMATION TECHNOLOGY RESOURCES Policy 800-006

Section 1 - PURPOSE

Elected or appointed officials and employees of the City of Enumclaw are obligated to use, conserve and protect electronic information and information technology resources for the benefit of the public interest. Responsibility and accountability for the appropriate use of information technology resources ultimately rests with the individual official or employee who uses these resources or who authorizes such use. The intent of the following policy is to preserve and enhance the integrity of these resources which belong to the citizens of Enumclaw. By accessing or using city owned information technology resources, each end user must agree that they have read and understand and agree to abide by the terms and conditions of this policy. If an elected or appointed official or employee does not agree or understand any of the terms or conditions of this policy, they must immediately discontinue use of city information technology resources and notify their department head or City Administrator and the Information Services Director.

Section 2 – INFORMATION TECHNOLOGY RESOURCES DEFINED

"Information Technology Resources" consist of all electronic communication assets and equipment, hardware, software, systems, services, networks, data and peripherals owned, leased, rented, established or otherwise administered by the City of Enumclaw. These assets enable individuals to access or interact with information stored on or transmitted within the city

data network, telecommunication systems, cellular systems and other internal or external sources. These resources include, but are not limited to the following:

Antivirus Systems
Audio/Visual Equipment
Burglar Alarm Systems
Card Entry Systems
Cellular Devices
Cellular Services
Cloud Storage
Cloud Applications
Control Systems
Copiers
Credit Card Readers
Data Backup Systems
Data Racks
Data Transmission Cables
Desktop Computers
Desktop Printers
Digital Cameras
Digital Tape Drives
Distribution Lists
Electronic Data
Electronic Documents
Electronic Images
Electronic Mail Messages
Electronic Mail Systems
FAX Machines
Fiber Optic Systems
Financial Systems
Global Positioning Devices
Firewalls
Hubs
Internet Services
Intranet Services
Label Printers
Laptop Computers
Large Format Printers
Laser Printers
Mobile Telephones
Modems
Monitors
Network Bandwidth
Network Cabling
Network Security Cameras
Network Security Services
Operating Systems
Panic Alarm Systems
Point of Sale Devices
Point of Sale Systems
Projectors
Records Management Systems
Remote Access Systems
Routers
Scanners
Server Racks
Servers
Software Applications
Social Media Accounts
Surge Protectors
Switches
Tablet Computers
Telephone Services
Telephone Systems
Telephones
Televisions
Text Messages
UPS's
USB Drives
Utility Systems
Voicemail Systems
VPN Systems
Websites
Wireless Access Points

Section 3 – SCOPE

This policy applies to all elected or appointed officials, employees, temporary employees, contractors, consultants, volunteers, outside or partner agency personnel, vendors, and any others that use or are provided access to city information technology resources including those workers associated with any third parties who access city systems or information technology resources. Throughout this document, the word "employee" will be used to collectively refer to all such individuals. This document applies to all information technology resources, communications systems and equipment owned, leased, rented, established or otherwise administered by the City of Enumclaw both on and off city property. Any violation of this policy is subject to access revocation and/or disciplinary action up to and including termination.

Section 4 - GENERAL PROVISIONS

4.1 Purpose

Information technology resources are provided to City of Enumclaw employees for the purpose of conducting official city business, advancing and supporting the city's mission and to assist in providing services to its citizens. The purpose of this section is to outline general provisions which must be adhered to while using city owned information technology resources.

4.2 Absolute Prohibitions

The following uses of city information technology resources are absolutely prohibited:

a. Any use for the purpose of conducting outside business or other commercial use which is not directly related to conducting official business for the City of Enumclaw or authorized partner agencies.
b. Any campaign or political use, unless such use has been determined not a violation of RCW 42.17.130 and .190 by the City Attorney, Washington State Attorney General, or Washington Public Disclosure Commission, or as otherwise authorized by law.
c. Any use for private benefit or gain, including use of government contracts with vendors for the personal purchase of goods or services.
d. Any use of information technology resources for the purpose of storing, publishing copying or otherwise using any illegally obtained copyrighted material or material which violates copyright laws.
e. Any use of profane, abusive or otherwise objectionable language in either public or private communications.
f. Any use of the information technology resources for the purpose of engaging in gambling or to access online gambling websites.
g. Accessing, viewing, downloading, sending, forwarding, replying to, printing, storing or publishing items which contain pornographic, sexually explicit, offensive or disruptive content, promote violence, hate, aggression, harassment or illegal activity or contain any content that offensively addresses someone's age, gender, sexual orientation, religious or political beliefs, national origin, veteran status or disability.
h. Announcing union meetings or conducting other exclusively union business.
i. Attempting to gain unauthorized access to city systems or data, outside systems or data, or attempting to decrypt, bypass or otherwise override system security or passwords.
j. Any use which violates City of Enumclaw policy or city, county, state or federal law.

4.3 Prohibition against Use of Information Technology Resources for Personal Use

No employee may use city information technology resources for personal benefit or gain of the employee, or any other person or organization including but not limited to the use of information technology resources to conduct or operate a private business or to purchase or sell goods for personal use.

4.3.1 Exceptions to Personal Use

Notwithstanding the prohibition against use of city information technology resources for personal benefit set forth in this policy, department heads may allow an employee to may make de minimis, personal use of city information technology resources if:

a. There is no cost to the city;
b. The use of city information technology resources does not interfere with the performance of the employee's or other employee's official duties;

c. The use is during non-working hours, brief in duration, and does not disrupt or distract from the conduct of city business;
d. The use does not compromise the security or integrity of city information technology resources;
e. The use does not involve installation of hardware or software not purchased by the city;
f. The use does not involve the storage of personal photos, music, documents or other data on a city owned computer.

An elected or appointed official or department head may authorize use of city information technology resources to support, promote, or solicit for an outside charitable or community-based organization or group if the use of city information technology resources meets the provisions set forth above. Occasional, minor use of printers, photocopiers, telephones or fax machines by employees is permitted provided the employee receives prior permission from an elected or appointed official or department head and pays for use at the rate established in the city's consolidated fee schedule.

4.4 Elected or Appointed Officials or Department Heads May Implement More Restrictive Policies

Nothing in this policy is intended to limit the ability of an elected or appointed official or department head to adopt policies for their offices or departments that are more restrictive than the policies provided herein.

4.5 No Expectation of Privacy

The city reserves the right to access, monitor and audit the activity and use of city information technology resources, communications, data, files and documents of all elected or appointed officials and employees including content sent, received and/or stored through the use of such resources. Users shall have no expectation of privacy when using city information technology resources. Such records may be subject to disclosure under the Public Records Act or may be disclosed for audit or other legitimate city operational or management purposes. Any records created while conducting city business using personally owned information technology resources may also be subject to disclosure. Any accessing, monitoring or auditing of city information technology resources must be performed by or coordinated through the Information Services Department.

4.6 Authorized Equipment

Only city owned information technology resources purchased or authorized by the Information Services Department may be connected to the city network or to a city owned computer. Unless otherwise authorized by the Information Services Department, only city owned information technology resources may be used for conducting city business.

4.6.1 Exceptions for Vendors, Contractors and Outside Agencies.

The Information Services Department may authorize exceptions to section 4.6 for vendors, contractors and outside agencies for the sole purpose of conducting government business. Prior to allowing any non city owned computer or equipment to be connected to the city network, the Information Services Department will verify that the computer is virus free and employs an up to date virus prevention mechanism.

4.7 Prohibited Equipment

With the exception of connections designated "Public Access" or "Non Business Access" in section 4.8, personally owned computers laptops, wireless access points, routers, hubs, mobile devices (as defines in section 9) or other non city owned information technology resources may not be connected to the city network or to city owned information technology resources. An official or employee may use a personally owned mobile computer or mobile device during lunch, breaks or other non-working hours in non work areas (IE: in a break room, outside or in their personal vehicle) providing such use does not interfere with the performance of the employee's or other employee's official duties and does not disrupt or distract from the conduct of city business.

4.8 Computers and Networks designated as "Public Access."

Certain city information technology resources including computers and internet access may be designated as "Public Access" or "Non Business Access" by the Information Services Department and may be made available for use for non-business purposes. These include:

a. The separate external network and computers located within the public areas of the City of Enumclaw Youth Center are designated "Public Access."
b. The separate external network and computers located within the public areas of the City of Enumclaw Senior Center are designated "Public Access."

4.9 Ownership

All software, programs, documents, drawings, images, applications, templates, databases and data files residing on city computer systems or storage media or developed on city systems are the property of the City of Enumclaw and shall not be removed from the workplace without proper authorization. The city, therefore, may access, copy, change, alter, modify, destroy, delete or erase this property at any time without prior notice. All information technology resources defined in section 2 are the property of the City of Enumclaw and shall not be removed from the workplace without proper authorization.

4.10 Records Retention and Public Records

All electronic records, communications and data are the property of City of Enumclaw and may be subject to the Public Records Disclosure Act (RCW Ch. 42.17). Each employee is responsible for maintaining copies of electronic records, communications and data in accordance with the Secretary of States Records Retention Guidelines. If an employee has a doubt concerning the need to retain any electronic records, communications or data, the employee shall consult the State Records Retention Manual, the City Clerk, or the appropriate elected or appointed official or department head.

4.11 Disposal of Information Technology Resources

The Information Services Department is responsible for disposal of all city owned information technology hardware and software. Prior to disposal, all data residing on hard drives, disks, tapes, or other electronic storage media will be permanently deleted or destroyed to avoid unauthorized release of data. Any hard drives, disks, tapes, or other electronic storage media used in devices which access secure information such as CJIS data will be disposed of by shredding or incineration only. No information technology resources will be sold, destroyed,

transferred or otherwise disposed of except by, or with the authorization of the Information Services Department.

4.12 Authorized Users

With the exception of those resources designated "Public Access" or "Non Business Access" in section 4.8, only elected or appointed officials, paid city employees or volunteers authorized by the appropriate department head may use city information technology resources. (See also Section 11 for exceptions.)

4.13 Network Topology Drawings

It is the responsibility of the Information Services Department to maintain up to date network topology drawings of the city network infrastructure. These drawings will be updated no less than annually with the exception of changes made affecting access to criminal justice information systems which will be updated within one month of implementation. Network topology maps will be marked "For Official Use Only" and not be made available for distribution to the general public.

4.14 Designated Information Security Officer

The Information Services Director is the designated Information Security Officer for the City and is responsible for establishing and maintaining strategies and programs that ensure information assets and technologies are adequately protected. The Information Security Officer assists staff in identifying, developing, implementing and maintaining citywide processes for the purpose of reducing information risks related to the use of IT resources. In addition, the Information Security Officer is responsible for responding to incidents or breaches in security and managing security related technologies in use by the city.

Section 5 - SPECIAL PROVISIONS REGARDING COMPUTER ACCOUNTS

5.1 Purpose

Employees are responsible for the security of electronically stored information and/or data they have been given permission to use. All employees given permission to access data must act in a manner to protect said data from loss, unauthorized alteration access and use.

5.2 Assignment of Computer Accounts

Computer accounts are assigned by the Information Services Department to individual employees at the discretion of elected or appointed officials and department heads for their exclusive use in conducting city business. Only elected or appointed officials and paid city employees will be assigned computer accounts for the purpose of accessing city information systems. To ensure only authorized elected or appointed officials and city employees are granted access to city information systems, user accounts will only be created after the employee has been entered into the payroll system or in the case of elected or appointed official, immediately upon being elected or appointed. Users are responsible for all activities conducted with accounts assigned to them. Shared computer accounts for specialized purposes, and with limited access to data, may be authorized by the Information Services Department. Such shared accounts may also be exempted from password standards and access control requirements if authorized by the Information Services Department. (See also Section 11 for

exceptions.) The information Services Department will review user accounts no less than annually to ensure inactive users have been properly removed or retired.

5.3 Passwords

Passwords are to be kept secret except in the case of authorized shared accounts. Each user is responsible to maintain the secrecy of the passwords for accounts assigned to them. To maintain password integrity, passwords for accounts assigned to individuals must not be shared. If a user has knowledge that another person knows or is using their password, it is their responsibility to immediately change the password and to report it to the Information Services Department. In the event a user forgets their password, they should contact the Information Services Department to have it reset.

5.4 Access Control

User account and passwords are used to control access to city data resources based on an individual employee's need to access specific data. Users are responsible for data accessed, transmitted, copied, saved or deleted using their user account. Users are prohibited from accessing or attempting to access information, systems, data or other information technology resources to which they have not been granted access by the Information Services Department. To prevent unauthorized use, all users should log off of, or lock access to all city computers and systems before leaving their computers or systems unattended. This provision is not intended to restrict distribution of data resulting from public disclosure requests or the authorized release of information by the city.

5.5 Data Access and Accounts for Terminated Employees

When an employee or official ends their service with the City of Enumclaw, it is the responsibility of the appropriate official or department head to immediately notify Human Resources who will in turn, notify the Information Services Department. Based on the exit timeline provided by Human Resources, the Information Services Department will suspend and/or change the password for all user accounts assigned to that individual. At the request of the department head, email sent to the outgoing employee may be forwarded to another individual for a period of up to 90 days. Email for the outgoing employee will systematically be retained for 25 months via the standard archival process. The Information Services Department will move the outgoing employee’s documents and files from their computer and/or user drive to the Information Services directory. If the department head, manager or replacement employee needs access to the outgoing employee’s email, documents or files, they should contact the Information Services Department. When releasing email, documents or files, the Information Services Department will assist in identifying relevant data that does not contain personal or confidential information. Documents and Files will be permanently deleted after a period of 25 months. Department Heads for the outgoing employee are responsible for ensuring that all records with a retention requirement of more than two years are moved to a location where they can be properly retained.

5.6 Password Standards

The following minimum password and account lockout standards will be employed for users logging into the city network:

a. Passwords must be a minimum of 8 characters.

b. Passwords may not contain dictionary words, proper names or the user ID.
c. Passwords must be changed every 90 days.
d. Previous 10 passwords may not be re-used.
e. Accounts will be locked for 15 minutes after 5 invalid logon attempts.
f. No dictionary words or proper names may be used.
g. Password and logon ID must not be the same.

5.7 Exceptions for Information Services Staff and Other Authorized Individuals
Information Services Staff and other authorized individuals with the permission of the Information Services Department may, by nature of assigned duties and in support of authorized activities, be exempt from any or all of the provisions in section 5. Elected or appointed officials and department heads will be granted access to information and data accessed by their direct reports on request and without further authorization.

Section 6 - SPECIAL PROVISIONS REGARDING ELECTRONIC MAIL

6.1 Purpose
The purpose of this section is to establish guidelines specific to governing the acceptable use of city-provided electronic mail (e-mail) resources. By establishing and maintaining compliance with this policy, risks and costs to the city can be minimized while the valuable potential of this communication tool can be maximized.

6.2 Right of Inspection
The electronic mail system owned by the City of Enumclaw is intended solely for the purpose of conducting city business. Electronic mail communications constitute public records and the city has the right to access or monitor messages for work-related purposes, security, or to respond to public record requests. All messages should be composed with the expectation that they are public. Users shall have no expectation of privacy in e-mail messages, whether they are business related or an allowed personal use as provided herein. Use of the city's electronic mail system shall be considered consent to elected or appointed officials, department heads, and the Information Services Department to inspect, use, or disclose any electronic mail or other electronic communications and/or data without prior notice.

6.3 Forwarding of Electronic Mail
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.

6.4 Misdelivered Messages
If an electronic mail message is delivered to a user by mistake, the user should stop reading as soon as they realize the message was not intended for them and notify the sender and Information Services Department immediately.

6.5 User's Responsibility for Security
Users are responsible for the security of their electronic mail account password and any electronic mail that is sent via a user account. To protect a user account against unauthorized use, the same precautions outlined in section 5.3 should be followed with regards to a user's

email account. Users may not send electronic mail on behalf of another person or user without their knowledge and consent.

6.6 Use of Non-City Email Accounts

Non-city email accounts including web based email accounts may not be used to conduct city business. Elected or appointed officials and employees will be issued city email accounts as required for the purpose of conducting city business.

6.6.1 Exceptions for Information Services Staff and Other Authorized Individuals

The Information Services Department may establish and use outside email accounts for the purpose of testing or troubleshooting city email accounts and systems. Law enforcement personnel, for the sole purpose of conducting of investigations and with the express permission of the Chief of Police may be exempted from section 6.6.

6.7 Transmission of Confidential Information

Confidential material must not be sent via email as electronic mail messages are subject to being intercepted, copied, forwarded, viewed, and used for non-approved purposes.

6.8 Electronic Chain Mail

E-mail "chain letters" shall not be originated, forwarded or otherwise distributed using city information technology resources. An e-mail "chain letter" is defined as any message sent to one or more recipients which directs the recipient to forward it to one or more other recipients with the promise of reward for forwarding it or threat of consequences for not doing so.

6.9 Reporting Suspicious Email

When a user receives an email of suspicious origin, a suspected phishing attempt or an email containing potential malware or malicious links they should report it by sending a screen shot of the message to techsupport@ci.enumclaw.wa.us. If a malicious email is accidentally opened, do not forward it, reply to it, attempt to unsubscribe, open attachments or click on links, and notify Information Services immediately.

Section 7 - SPECIAL PROVISIONS REGARDING INTERNET ACCESS

7.1 Purpose

It is the policy of the City of Enumclaw to encourage effective and efficient use of city owned information technology resources for conducting city business. This includes use of the internet for employees to provide information to city residents, businesses, and other governmental agencies, to search for information, and for information exchange.

7.2 Certain Use of Internet Prohibited

In addition to the prohibitions outlined in section 4.2, the following specific internet related activities which are prohibited:

a. Use of the city internet service to access sites which provide streaming video, audio, internet radio or video broadcasts, interactive downloading of screen savers or browser features or other content that consumes excessive or continuous bandwidth except for the purpose of conducting city business.
b. Use of the city internet service to download, upload, store, purchase or share music or video files to or from the internet except for the purpose of conducting city business.

c. Use of the city internet service to buy or sell merchandise through online shopping or auction services or to conduct banking or financial transactions which are not directly related to conducting city business.
d. Use of instant messaging or other messaging services or software except for the purpose of conducting city business.

7.3 Exceptions for Law Enforcement Personnel

Law enforcement personnel, for the sole purpose of conducting investigations and with the express permission of the Chief of Police may be exempted from section 7.2.

7.4 Monitoring and Reporting of Internet Use

It is the responsibility of each department head to monitor and audit internet use within their department. The Information Services Department may monitor and record user access to internet sites and may provide department heads with information that can be used to track usage as required or requested to enforce city or department policy.

Section 8 - SPECIAL PROVISIONS REGARDING REMOTE ACCESS TO CITY SYSTEMS

8.1 Purpose

Remote access to certain city systems, applications, and data such as webmail or mobile access in city vehicles is maintained for selected employees. Other remote access systems are restricted only to those employees who show a demonstrated necessity to access data or applications while away from city facilities and only for the purpose of conducting city business.

8.2 Authorization Required

Remote web based access to city email is granted to all email users for the purpose of accessing their e-mail while at home, on leave or traveling. Certain city mobile computers are equipped with secure remote access for public safety functions. The Information Services Department may utilize remote access to systems for offsite troubleshooting and maintenance. All other requests for remote access to city systems must be authorized and implemented by the Information Services Department.

Section 9 - SPECIAL PROVISIONS REGARDING TELEPHONES AND MOBILE DEVICES

9.1 Purpose

The purpose of this provision is to establish guidelines for the use of city issued mobile devices and desktop telephones and the on-duty use of mobile devices personally owned by employees. Mobile devices include, but are not limited to cellular phones, smart phones, PDA's, tablets, mobile computers, mobile data terminals and other mobile data collection devices.

9.2 Privacy Policy

Any employee utilizing any computer, internet service, phone service, or other wireless service provided by or funded by the city expressly acknowledges and agrees that the use of such service, whether for business or personal use, shall remove any expectation of privacy the employee, sender and recipient of any communication utilizing such service might otherwise have, including the content of any such communication. The city also expressly reserves the

right to access and audit any and all communications including content sent, received and or stored through the use of such service.

9.3 City Issued Mobile Devices and Landline Telephones

Depending on an employee's assignment and needs of the position, the city may, at the discretion of the appropriate department head, issue a mobile device and/or landline telephone. Such devices shall remain the sole property of the city and shall be subject to inspection or monitoring, including all related records and content, at any time without notice and without reason.

9.4 Individually Owned Mobile Devices

Employees may carry their own individually owned mobile devices while on duty subject to the following provisions:

a. Carrying an individually owned mobile device is optional.
b. The device shall be purchased, used and maintained at the employee's expense.
c. The employee is responsible for all mobile device hardware, software, service and support.

9.5 Use of Mobile Devices and Desktop Telephones

Mobile devices and desktop telephones should only be used by on-duty employees for legitimate city business. Occasional personal use of city owned mobile devices and desktop telephones must follow the guidelines set forth in section 4.3.1.

While employees may use personally owned mobile devices for personal communication during non-working hours such as breaks and lunches, such usage should be limited to areas where the communication will not disrupt other employees or where it could be seen or heard by members of the public. Extended or frequent use of city issued or personally owned mobile devices or landline phones for personal use is prohibited. Employees may be responsible for reimbursing the city for any charges incurred as a result of excessive personal use.

9.6 Mobile Device Use While Driving

Except as provided for in RCW 46.61.667, the use of mobile devices while operating a motor vehicle is prohibited.

9.7 Use of Text Messaging and Instant Messaging

Text messaging and instant messaging are to be used only for transitory messages with a short-term retention value that can be destroyed when no longer needed for city business. The Washington State Archives defines "transitory records" as those which "only document information of temporary short-term value," provided that the records are:

a. Not needed as evidence of a business transaction; and,
b. Not covered by a more specific records retention series.

Examples of "transitory records" include miscellaneous notices or memoranda which do not relate to the functional responsibility of the agency (notices of community affairs, holidays, etc.) Text messaging and instant messaging will not be used to provide any working direction to staff which is not documented in some other form for retention purposes. If for any reason a non-transitory text message or instant message is sent that does have retention value, the employee must immediately take steps to preserve the record. The record can be preserved via

logging, screen shot, photograph or transcription of the exact content to a recordable medium such as email. Once preserved, the record must be retained and/or destroyed in accordance with the Secretary of States Records Retention Guidelines.

Section 10 - SPECIAL PROVISIONS REGARDING INTERNET WEBSITES

10.1 Purpose

The purpose of this provision is to establish guidelines for the acquisition, creation and maintenance of internet websites and social media accounts owned, established or maintained by the City of Enumclaw. Internet Websites are established on behalf of the City of Enumclaw and its departments by the Information Services Department. These websites consist of both externally visible sites for use by the public and internal sites for use by elected or appointed officials and city employees. These sites contain information regarding programs, services, policies, and objectives of the City of Enumclaw and the surrounding area as well as links to other governmental and outside agency sites. External city websites are designed to provide convenient access to city related records, events and other resources for residents, visitors, businesses, non-profit organizations, other public agencies, and schools to access their city government. Internal sites are designed to provide elected or appointed officials and city employees with access to information, news, links and other content which improves the efficiency in which they perform their jobs. Social media websites are third party hosted online technologies that facilitate social interaction and dialogue through user participation and user-generated content. They include social networking sites, social bookmarking sites, social news sites, and other sites that are centered on user interaction.

10.2 Website Standards

All websites including social media accounts, owned by or which represent the government of the City of Enumclaw must present a consistent, professional image of the city, its elected or appointed officials, employees and the events, programs and services it offers. In order to ensure a consistent appearance and public image, all city websites shall be acquired, maintained and periodically reviewed by the Information Services Department. At its discretion, the Information Services Department may provide city departments with the ability to edit and maintain content on city owned or managed websites. The Information Services Department shall act as the city's registration authority for all city-owned domain names and shall acquire and maintain all domain registrations, websites, and social media accounts. Elected or appointed officials and employees are prohibited from acquiring or registering internet domains or establishing websites including social media accounts which are owned by or represent the City of Enumclaw, its departments, divisions, events, programs or services.

10.3 Links from City Websites

The city’s websites may contain links to outside content which provide information relevant to the residents, elected or appointed officials, and employees of the City of Enumclaw. At its sole discretion, the Information Services Department may include on city websites links to outside content of the following nature:

a. Federal, state, local and educational entities.

b. Private organizations if these organizations offer services that complement the information or services offered by the City of Enumclaw.
c. Non-profit organizations if these organizations offer services that complement the information or services offered by the City of Enumclaw.
d. News, weather, search engine, mapping or other sites which may improve employee efficiency in performing their duties.

The determination of whether to establish links to outside sites organizations is made on a case-by-case basis by the Information Services Department.

10.4 Political Content Prohibited

In order to avoid the appearance of City endorsement of political content, no content shall be placed on any City website which promotes or opposes any candidate for political office, political party, or advocates for or against a particular issue on a local, state, or national level.

10.5 Social Media Accounts

Social media accounts shall be subject to the following guidelines:

a. To avoid the potential of prohibited or libelous content appearing on a city sponsored social media account, social media accounts will not be established which allow posts or other content from the public.
b. The Information Services Department or assigned departmental employees will maintain accurate city information on social media accounts by frequently reviewing and updating content as necessary and appropriate.
c. Information posted using the city's social media accounts is subject to the Public Records Act and associated retention schedule. In order to ensure appropriate retention of public records, the Information Services Department shall ensure all content posted on City social media accounts is systematically archived.
d. A link to the city's website, www.cityofenumclaw.net, must be included on all social media sites, directing users back to the City of Enumclaw website for in-depth information on the posted content.
e. Elected or appointed and appointed officials, board members, commissioners and other officials and appointed volunteers should avoid commenting or otherwise communicating on social meeting sites where such participation would constitute a violation of the Open Public Meetings Act.

10.6 Exceptions for Law Enforcement Personnel

Law enforcement personnel, for the sole purpose of conducting investigations and with the express permission of the Chief of Police may be exempted from sections 10.2 and 10.5.

Section 11 – SPECIAL PROVISIONS FOR VOLUNTEERS, CONTRACTORS, PARTNER AGENCIES AND OTHER AUTHORIZED INDIVIDUALS

11.1 Purpose

To ensure data integrity and security and to discourage unauthorized use of city resources, care must be taken in issuing logon ID's and granting access to city systems and resources. Unless authorized as described herein, only elected or appointed officials and paid city employees will be issued logon ID's and granted access to city owned information technology resources. Individuals to whom access is granted must agree to abide by the terms and conditions of the city Acceptable Use policy whenever accessing city systems or when using information technology resources.

11.2 Exceptions for Unpaid City Volunteers, Private Contractors and Contract Employees.

When a legitimate business need exists, at the request of an elected or appointed official or department head and with written permission of the City Administrator, unpaid city volunteers, private contractors or contract employees may be issued temporary logon ID's and/or granted access to city information technology resources.

11.3 Exceptions for Employees of Partner Agencies

At the discretion of the Information Services Director and for the purpose of supporting the needs of and sharing information and resources with partner agencies, employees of partner agencies may be issued logon ID's and/or granted access to city information technology resources.

Section 12 – SPECIAL PROVISIONS REGARDING ACCESS TO CRIMINAL JUSTICE INFORMATION SYSTEMS

12.1 Purpose

The Criminal Justice Information Services (CJIS) Division of the FBI requires appropriate controls be put in place to ensure the integrity and security of Criminal Justice Information (CJI) data. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operates in support of, criminal justice services and information.

12.2 Authorized Users

Prior to accessing any CJIS data, all personnel who have direct access to CJI data including department personnel, information services staff and authorized vendors must be authorized by the Chief of Police and meet the following requirements:

a. Personnel must have a state of residency fingerprint background record check completed.
b. Personnel must have a state of residency fingerprint re-background record check completed every 5 years.
c. Personnel must sign the signature log acknowledging that they have they viewed the Washington State Patrol ACCESS Division technical security awareness training.

12.3 Outside Agency Policies

All personnel who have direct access to CJIS data including department personnel, information services staff and authorized vendors must agree to abide by the policies set forth by the

Washington State Patrol ACCESS Division and the Criminal Justice Information Services Department of the FBI. Individuals accessing CJIS data are required to operate their terminals according to the rules and policies of Washington Crime Information Center/National Crime Information Center (WACIC/NCIC.)

12.4 Reporting Suspected Misuse of CJIS.

Any individual who suspects that an individual is obtaining CJIS data for non criminal justice purposes or misuse of CJIS data or violation of the policies mentioned in section 12 shall immediately report the suspected misuse or violation to the Chief of Police. The Chief of Police or their designee shall then immediately notify the ACCESS Section of the Washington State Patrol of any suspected misuse or violation.

12.5 Misuse of CJIS

Violations of the rules, regulations, policies or procedures developed by the City of Enumclaw, Enumclaw Police Department, WACIC/NCIC, Washington State Patrol or FBI, or any other misuse or abuse of the ACCESS system or other CJIS system or data may result in disciplinary action up to and including termination and/or criminal prosecution.

12.6 Physical Protection of CJI Data

Controls shall be in place to protect electronic and physical media containing CJI data while being stored, transported or accessed. Electronic media includes memory devices in server and computer hard drives and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disks, flash drives, external hard drives, or digital memory cards. Physical media includes hardcopy documents and imagery that contain CJI data. Individuals shall adhere to the following guidelines when accessing, storing or transporting CJI data:

a. Store all electronic and physical media within a physically secure or controlled area or within the immediate control of an employee authorized to access such data. A secured area includes a locked drawer, cabinet, or room.
b. Restrict access to electronic and physical media to authorized individuals.
c. Ensure that only authorized users remove hardcopy or digital media from secured locations.
d. Only use information technology resources acquired and approved by the city Information Services Department to access, process, store, or transmit CJI data.
e. Store all hardcopy CJI records in a secure area accessible to only those employees whose job function requires them to handle such data.
f. Precautions must be taken to obscure CJI data from public view, such as by means of an opaque file folder or envelope for hardcopy records or screen locks or privacy filters for computer terminals.
g. When CJI data is stored electronically outside the boundary of a physically secure location, the data shall be protected using encryption.

h. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.
i. Lock or log off computer when not in immediate vicinity of work area to protect CJI data.
j. Limit the collection, disclosure, sharing and use of CJI data to authorized personnel.
k. Secure hand carried electronic and paper documents by storing them in a locked briefcase or lockbox.
l. Only view or access CJI data in a physically secure location.
m. When mailing or shipping CJI data, do not mark the package "Confidential" and ensure packages are sent by methods that provide for complete shipment tracking and history, and signature confirmation of delivery.
n. Unless equipped with two factor authentication, computers and other devices that are capable of accessing CJIS protected data including those mounted in Police Department vehicles must only be used in a secure area as defined by the FBI CJIS Policy Manual such as inside the police vehicle or inside the Police Department building.

12.7 Destruction of CJI/CHRI Data

The Information Services Department is responsible for the destruction of all obsolete technology resources containing CJI/CHRI data. When no longer usable, hard drives, removeable media, printouts, and other technology resources used to process, store and/or transmit CJI/CHRI and classified or sensitive data shall be properly disposed of in accordance with the following measures:

a. Electronic media such as hard drives and removeable media shall be disposed of by wiping the device using a utility capable of meeting US DOD 5220.22-M standards with no fewer than three pass overwriting. Once wiped, the devices will be stored in the secure area of the Police Department until they can be delivered to a commercial facility for shredding. Wiping, transporting and shredding must be performed or witnessed by a WSP ACCESS certified Information Services employee.
b. End users of physical media (hard copies, printouts, ribbons and other similar items) shall be responsible for destruction by shredding using agency crosscut shredders.

12.8 Reporting CJIS/CHRI Security Events

It is the responsibility of any individual who becomes aware of a security incident related to Criminal Justice Information Systems/Criminal History Record Information (CJIS/CHRI) to immediately notify the Information Security Officer designated in section 4.14 of this policy. It is the responsibility of the Designated Security Officer to promptly report incident information to the Washington State Patrol ACCESS Information Security Officer (ISO) by email at ACCESS@wsp.wa.gov using the FBI Security Incident Reporting Form available on the ACCESS webpage:
http://www.wsp.wa.gov/_secured/access/docs/access_cjis_security_incident_report.pdf.

Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. It is the responsibility of the Information Services Department to ensure formal event reporting and escalation procedures are in place. Wherever feasible, the Information Services Department shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third-party users shall be made aware of the procedures for reporting security events and weakness that might have an impact on the security of technology resources and are required to report any security events and weaknesses as quickly as possible as described above.

If a mobile device with access to CJIS/CHRI is lost or stolen, the user must immediately inform the Information Services Department of the loss or theft and whether the device was known to be locked or unlocked. The Information Services Department shall immediately attempt to remotely wipe the device and report the loss or theft to the Designated Security Officer.

12.9 Collection of Evidence

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Section 13 – SPECIAL PROVISIONS REGARDING CLOUD STORAGE AND APPLICATIONS

13.1 Purpose

Special precautions must be taken when utilizing cloud storage, applications and services to ensure the city properly protects, archives and maintains control over data located on external systems. Cloud based systems include cloud-based email, document storage and sharing, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and any other application or service where data is stored outside of the physical boundaries of city buildings.

13.2 Cloud Storage and Application Standards

All users who utilize cloud services for storage and/or processing of city data must utilize only those services approved and acquired through the Information Services Department for such activities. Anyone wishing to utilize services outside of existing approved solutions must submit a copy of the contract for such services to the Information Services Director for review prior to purchase. The Information Services Department will review rights and permissions requested by cloud service providers prior to installation to ensure they do not put city data or systems at risk of being compromised. Personal cloud services or accounts, or those services or accounts set up without the approval of the Information Services Department may not be used for the storage, manipulation or exchange of data for the purpose of conducting city business.

13.3 Sensitive Information

Special precautions must be taken to ensure sensitive information such as credit card data, personal information, CJIS data and law enforcement investigation data stored utilizing cloud services is secure. The Information Services Department will ensure appropriate safeguards are

in place prior to authorizing cloud storage or applications intended to house sensitive information.

13.4 Cloud Storage and Records Retention

All users who utilize cloud services for storage and/or processing of city data must ensure that records are being properly archived in accordance with the Secretary of States Records Retention Guidelines. Cloud storage of data is generally intended to be used for short term storage only and users are responsible for ensuring a primary copy of the data is kept on internal systems for retention purposes. The Information Services Department must ensure that long term cloud storage applications and services provide for the proper backup and archival of data.

Section 14 – ACQUISITION OF INFORMATION TECHNOLOGY RESOURCES

14.1 Purpose

In order to reduce expense to the city, the Information Services Department shall be responsible for managing the acquisition of all information technology resources. Significant cost savings, stability and reduced overhead can be achieved through vendor consolidation, hardware and software standardization, volume purchases and utilization of government contracts.

Acquisition of information technology resources as defined in section 2 shall be the sole responsibility of the Information Services Department. Notwithstanding the exceptions provided herein, it is a violation of this policy to procure or otherwise acquire information technology resources outside the centralized procurement process managed by the Information Services Department.

14.2 Hardware and Software Standards

All city information technology acquisitions shall meet or exceed performance standards set forth by the Information Services Department with regards to hardware, software and system capabilities. The Information Services Department will occasionally review and revise these standards to ensure that information technology resources meet the needs of end users and the business requirements of the city. City owned software shall not be installed on a computer not owned or administered by the City of Enumclaw without the authorization of the Information Service Director. Non city owned software or software obtained outside of the standard Information Services Department procurement process shall not be installed on a city owned or administered computer or system without the authorization of the Information Service Director.

14.3 Grant Purchases

Information technology resources obtained from grants or through grant purchases must be coordinated with the Information Services Department prior to applying for the grant to ensure any technology acquisitions meet current city standards for hardware and software.

14.4 Capital Purchases

Capital purchases of information technology resources will be requested through the annual budget process by the Information Services Department. Information technology resources obtained as a component of a larger capital purchase must be coordinated with the Information

Services Department prior to preparing the capital request to ensure any technology acquisitions meet current city standards for hardware and software.

14.5 Seized Information Technology Resources

Police seizures of information technology resources are not allowed to be utilized as an information technology resource without prior authorization from the Information Services Director. Seized items must meet or exceed current hardware and software standards before being considered for internal use and all items must be inspected and scanned for viruses by the Information Services Department prior to being connected to the city network.

14.6 Donated Information Technology Resources

Donations of information technology resources may not be accepted from individuals or outside agencies without prior authorization from the Information Services Director. Donated items must meet or exceed current hardware and software standards before being considered for internal use and all items must be inspected and scanned for viruses by the Information Services Department prior to being connected to the city network.

14.7 Acquisition and Establishment of Internet Websites and Social Media Accounts

Requests for the acquisition or establishment of internet websites or social media accounts shall be made by the department director to the City Administrator. Upon approval by the City Administrator the acquisition and establishment of internet websites or social media accounts shall be the sole responsibility of the Information Services Department. Notwithstanding the exceptions provided herein, it is a violation of this policy to procure or otherwise establish internet websites or social media accounts which represent the government of the City of Enumclaw, its departments, divisions, services or programs outside the centralized procurement process managed by the Information Services Department.

14.8 Acquisition of Landline Telephone and Mobile Device Service and Equipment

The acquisition of all telecommunication equipment including telephone systems and service, landline and cellular telephones and other mobile devices shall be the sole responsibility of the Information Services Department. Notwithstanding the exceptions provided herein, it is a violation of this policy to acquire telephone systems or services, landline and cellular telephones and other mobile devices outside the centralized procurement process managed by the Information Services Department.

14.9 Exceptions

Elected or appointed officials and department heads may authorize the purchase of computer related consumables and minor peripherals such as CD's, toner and ink cartridges, keyboards, mice, digital cameras, USB drives, furniture, keyboard trays, cases, screen protectors and ergonomic accessories as necessary to conduct city business. The Mayor, City Administrator, Chief of Police or Information Services Director may authorize exceptions to section 14 of this policy for short periods of time due to special circumstances such as disasters or other citywide emergencies where acquisitions of information technology resources may require increased expediency.

Section 15 – IMPLEMENTATION

This policy shall be effective immediately upon adoption and shall supersede all policies previously adopted by the City of Enumclaw. The most current version of this policy will be made available on the city intranet site, the external city website and in printed form from the Information Services Department or Human Resources. Elected or appointed officials and employees are responsible for understanding and agreeing to abide by all provisions in the most current version of this policy. The City Administrator shall have the authority and responsibility for the implementation of this policy and may make interpretations on issues that are not clearly articulated or not included within. Notwithstanding the exceptions provided within, any exceptions to this policy must be authorized in writing by the City Administrator.

Chris Searcy Digitally signed by Chris Searcy
Date: 2023.04.04 12:41:00 -07'00'

Chris Searcy – City Administrator

April 4, 2023
Date