RESOLUTION NO. 2022-011

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF DEER PARK, WASHINGTON IMPLEMENTING AN INFORMATION TECHNOLOGY POLICY FOR ELECTED OFFICIALS AND CITY STAFF, INCLUDING A SEVERABILITY PROVISION, AND SETTING AN EFFECTIVE DATE.

WHEREAS, the Washington State Auditor recommends that the City draft a technology policy for Elected Officials and City staff; and

WHEREAS, the City Clerk-Treasurer recommends adopting a technology policy in the form attached as Exhibit "A" to this Resolution which was preliminary approved by the State Auditor's Office; and

WHEREAS, the Mayor and City Council have reviewed the recommended technology policy and have determined that adoption of the same are in the best interest of the citizens of the City; NOW, THEREFORE,

THE CITY COUNCIL OF THE CITY OF DEER PARK, WASHINGTON, HEREBY RESOLVE AS FOLLOWS:

Section 1. The City hereby adopts an Information Technology Policy in the form attached as Exhibit "A" which is made a part of this Resolution by this reference.

Section 2. If any section, sentence, clause, or phrase of this Resolution shall be held to be invalid or unconstitutional by a court of competent jurisdiction, such invalidity or unconstitutionality shall not affect the validity or constitutionality of any other section, sentence, clause, or phrase of this Resolution.

Section 3. This Resolution shall be effective immediately upon passage by the City Council.

APPROVED by the City Council of the City of Deer Park, Washington at an Open Public Meeting the 19th day of October, 2022.

APPROVED:

TIMOTHY VERZAL, Mayor

ATTEST/AUTHENTICATED:

DEBY CRAGUN, CITY CLERK/TREASURER

APPROVED AS TO FORM:

KAIT M. SCHILLING, CITY ATTORNEY

EXHIBIT "A"

CITY OF DEER PARK TECHNOLOGY POLICY

The intent of the Information Technology Policy ("IT Policy") is to define the appropriate and acceptable use of technology at the City and to ensure that the City complies with all legal requirements. It outlines the responsibilities of those who work for and on behalf of the City in contributing to the maintenance and protection of its information resources in a secure, stable, and cost-effective manner.

I. IT Policy Scope

This IT Policy defines the oversight, use and protection of the City's computer equipment, network, servers, and electronic communications. This includes the acquisition, access, and use of all software, hardware, and shared resources.

It applies to all those who work on behalf of the City including, but not limited to, employees, contractors, consultants, temporary employees, volunteers, elected officials, members of all boards and commissions, and other workers including all personnel affiliated with third parties ("users"). This policy also applies to all technology equipment that is owned or leased by the City regardless of project and program funding sources.

II. Acquisition of Technology Resources

No technology resources including, but not limited to, software, hardware, cloud services, portable devices, removable devices, and related maintenance and support contracts, may be purchased or used in connection with City business without first obtaining authorization from the City Clerk-Treasurer or the IT personnel that are under contract to perform services for the City ("IT Personnel"). An employee, or other person described above in Section I, desiring to obtain a technology resource (computer, phone, camera, USB, etc.) should first contact the City Clerk-Treasurer.

III. Access to Technology Resources

- Passwords: Users are responsible for establishing and maintaining passwords consistent with the City's standards as defined in this IT Policy. A user who forgets his or her password should contact the City Clerk- Treasurer or IT Personnel, or use the password reset (if and when available). User accounts and passwords represent your identity and shall not be shared with anyone including management or IT Support personnel. In the event access to a user account is necessary while an employee is away or otherwise unavailable, IT Personnel should be contacted. Users should comply with the following password guidance:
    - Passwords should be changed every 120 days
    - Minimum length of fourteen (14) or more characters, including spaces and punctuation.
    - Users should not use their username, or first and last name as passwords.
- Logging off: Users should shut-down, restart, or log off their computer each night to prevent unauthorized activity unless otherwise directed by IT Personnel to enable off- shift maintenance

and security updates.

- Responsibility for access: All activity resulting from device, network, or software application access is the responsibility of the person assigned the user account.
- Personal hardware and devices: Personal hardware and devices shall not be connected to the City's network by any employee.
- Personal software: Personal software shall not be installed on the City's computers by any employee.

IV. Security of City Technology Resources

Effective security requires the participation and support of every user in the City. It is the responsibility of every user of City technology to remain vigilant in their awareness and protection of the City's technology resources. Specific due diligence requirements are outlined below:

- Intruding or attempting to intrude into any gap in system or network security is prohibited. Sharing of information with others that may facilitate their unauthorized access to the City's data, network, or devices, or their exploitation of a security gap, is also prohibited.
- User accounts and passwords may not be shared.
- It is the responsibility of each user to prevent unauthorized access to personal, sensitive, or confidential information that could present a risk of identity theft, thus jeopardizing a person's privacy, financial security, or other interests.
- In general, it is not permissible to download personal, sensitive, or confidential information to any removable/portable device, including laptop computers, USB devices, or thumb drives unless access to that information is within the scope of your job, and the data or device is encrypted. Transmitting personal, sensitive, or confidential data via e-mail or other unencrypted medium is prohibited. Personal, sensitive, or confidential data should be stored in a file folder that is accessible only to those who need to view it.
- Prior to accessing a removable device such as a USB or thumb drive, other mobile devices, cameras, etc., the user shall scan the device for viruses and malware to avoid infecting the City's systems.
- Leaving personal, sensitive, or confidential information exposed to view while unattended, either on paper or on screen, is prohibited.
- Whenever possible, laptop and desktop hard drives and removable devices should only contain copies of source files, not the original file. Original source files should be stored on the City's network to ensure they are backed up to prevent loss.
- Lost or stolen computers, laptops, mobile devices, etc. must be reported immediately to the local Police Department and IT Personnel. A report should also be made to the City Clerk-Treasurer.
- Lost or stolen devices (including portable media such as thumb drives, CDs, DVDs) or hardcopy reports that contain personal, sensitive, or confidential information and/or information that is subject to the City Procurement Policy, City credit card policy, the Health Insurance Portability and Accountability Act, or other legal mandate should be reported immediately to the City Clerk-Treasurer and IT Personnel to determine any action that must be taken under those regulations.

V. Use of Technology Resources

The City's technology resources are City property and are intended to be used for the conduct of City business. Use of City technology resources is not permitted when the use is related to the conduct of an

outside business; is for the purpose of supporting, promoting, or soliciting for any non-City sponsored outside organization or group; religious, campaign or political use; commercial use; to conduct illegal activities; any entertainment use; use which results in the City being placed on electronic mailing lists related to prohibited uses; downloading personal email to the City's system or attaching a personal email box.

Limited personal use is permitted as long as the use does not result in a cost to the City, does not interfere with the user's responsibilities and fulfillment of job duties, is brief in duration and frequency, does not distract from the conduct of City business, and does not compromise the security or integrity of City information or software. It is strongly advised that only personal devices should be used to access the Internet or personal email while on breaks.

When using City technology it is a good idea to ask yourself this question: Can I directly support a work purpose for this use? If the answer is yes, there should be no problem. If the answer is no, you probably shouldn't do it unless you are confident that the use is permitted as a limited personal use described above. If you have questions about the appropriateness of using City technology resources for any particular purpose, contact the City Clerk-Treasurer for guidance.

There is no right to privacy when using the City's technology resources, whether for City business or incidental personal use. The City owns all data stored on its network and peripheral devices and reserves the right to inspect and monitor any use at any time (examples include e-mail, voicemail, internet logs, computers, laptops, mobile devices, etc.)

VI. Internet Usage

Content and images posted on the City website(s) should conform to the same professional standards as with written business correspondence. A professional tone should prevail.

All information that is posted, copied, or shared, either on the City's servers, desktops, website or social media sites, should conform to laws that govern copyrighted materials including, but not limited to, photographs, magazines, books, music, or the installation of any software for which the City does not have an active license. The installation of pirated software is strictly prohibited.

Internet usage that significantly impacts City network bandwidth may be restricted. Employees should utilize only the City's tools (such as the City-standard browser) and recommended best practices to manage their connections when viewing, downloading, sharing, and printing information to ensure that these shared resources are not negatively impacted.

Examples of Permissible Internet Use

The following are examples of Internet use that will be allowed, so long as the previously stated permissible use requirements are met:

- Use of the Internet to view City job announcements.
- Use of the Internet to check the weather for the upcoming weekend.
- Use of a City computer to check local news websites during your break.
-

Examples of Impermissible Internet and Intranet Use

- Use of the Internet to access nude or sexually explicit materials (text, photographs, graphics, etc.) that are not related to the user's job duties.
- Supporting, promoting, or soliciting for any non-City sponsored outside organization or group.
- Conducting illegal activities.
- Engaging in activity that would violate the City's ethics and/or conflict of interest policies.

VII. E-mail Use

- E-mail communications should conform to the same professional standards as with written business correspondence. A professional tone should prevail.
- Minimal personal use of the City's email system is permitted. However, personal e-mail must conform to limited use standards and may not be related to activities listed as prohibited uses.
- Use of e-mail systems other than the City's email system to conduct City business is not advised due to records retention and public disclosure laws and should only occur in limited circumstances.
- E-mail is considered a public record and is subject to disclosure under Washington State law, Chapter 42.56 RCW. Managing individual e-mail storage and retention is the responsibility of each individual, consistent with the City's document and records-retention guidelines. Users should avoid unnecessary e-mail traffic and are encouraged to minimize the size of attachment files and use network drives or SharePoint sites to share file attachments.
- The citywide e-mail distribution list should be used for critical and time-sensitive City business information only.
- Any attempt to misrepresent one's identity when using City e- mail is prohibited.

Examples of Permissible E-mail Use

The following are examples of e-mail use that will be allowed, so long as the previously stated permissible use requirements are met. When possible, users shall opt to use personal devices for the below described permissive uses.

- Sending an e-mail communication home to make sure one's children have arrived safely from school.
- Receiving an e-mail from a son or daughter, who is away at college, solely for the purpose of telling the parent he or she is coming home for the weekend.
- When the user had planned to fly to visit relatives but flight plans have changed, and the user sends an e-mail solely for the purpose of informing the relative of the new arrival time.

Examples of Impermissible E-mail Use

- Use of City e-mail to conduct illegal activities.
- Use of City e-mail to conduct an outside business.
- Engaging in activity that would violate the City's ethics and/or conflict of interest policies.
- Use of City email to campaign in support of or in opposition to a political candidate or ballot issue.

VIII. Text and Instant Message Use

- Text and instant messages should conform to the same professional standards as with written business correspondence. A professional tone should prevail.
- The use of text messaging and instant messaging to conduct City business from personal cell phones is prohibited. This prohibition applies even if the employee receives a stipend from the City to use the personal cell phone. The rationale behind this prohibition is that text messaging and instant messaging on personal cell phones are not backed up on the City's server but, nevertheless, are government records subject to records retention laws and the Public Records Act, Chapter 42.56 RCW.
- Text and instant messaging for conducting City business is permitted only on City equipment.
- Text and instant messaging should be used for transitory communication only.
- Any attempt to misrepresent one's identity when using City text or instant messaging is prohibited.

Examples of Permissible Text and Instant Message Use - City- Owned Devices Only

- "I'll be late to the meeting."
- "I'll meet you at 9:00."
- "Are you available for a quick chat?"

Examples of Impermissible Text and Instant Message Use

- "I authorize you to spend the $300,000 for that project."
- "City Council should authorize the ordinance pertaining to homelessness."

IX. Reporting and Administration

Anyone who observes or suspects a violation of these policies and requirements, or a potential gap in security or protection of the City's assets or data, should immediately make a report to their department director or to the City Clerk-Treasurer Failure to do so may result in disciplinary action up to and including termination of employment.

X. Exceptions to this IT Policy

Requests for exceptions to any provision of this IT Policy must be submitted in writing to the City Clerk-Treasurer. Exceptions require the approval of both the City Clerk-Treasurer and department director. Approvals must be documented in writing and limited in duration to provide for periodic re-evaluation.