270 –Technology Usage Policy

1.0 PURPOSE

The intent of the *Technology Usage Policy* is to define the acceptable use of technology at the Des Moines Pool Metropolitan Park District (District) and to ensure that the District complies with all legally mandated requirements. It outlines the responsibilities of those who work for and on behalf of the District in contributing to the maintenance and protection of its information resources in a secure, stable and cost-effective manner. This policy is consistent with the intent and requirements of the District's work policies and rules.

Use of technology in violation of this policy is subject to disciplinary action up to and including termination.

2.0 SCOPE

The District's *Technology Usage Policy* defines the oversight, use and protection of the District's computing equipment, network, voice, electronic communications and data repositories. This includes the acquisition, access and use of all software, hardware and shared resources, whether connected to the network, configured off the network, or while in transit (mobile). It applies to all those who work on behalf of the District including, but not limited to, employees, contractors, consultants, temporaries, supplementals, volunteers and other workers including all personnel affiliated with third parties. This policy also applies to all equipment that is owned or leased by the District regardless of project and program funding sources.

3.0 OWNERSHIP OF DATA

The District owns all data, files, information, and communications created on, stored on, transmitted, received or exchanged via its network, communications systems, equipment and devices (including email, voicemail, text messages and Internet usage logs even if such communications resides with a third-party provider) and reserves the right to inspect and monitor any and all such communications at any time, for any business purpose and with or without notice to the employee. The District may conduct random and requested audits of employee accounts (including accounts with commercial or other third party providers if used in the course of conducting District business) in order to ensure compliance with policies and requirements, to investigate suspicious activities that could be harmful to the organization, to assist The District in evaluating performance issues and concerns, and to identify productivity or related issues that need additional educational focus within the District. Internet, e-mail, voicemail, text message communications and Internet usage logs may be subject to public disclosure and the rules of discovery in the event of a lawsuit.

The District's Internet connection and usage is subject to monitoring at any time with or without notice to the employee. There is no right to privacy in the use of District technology resources.

4.0 ACQUISITION OF TECHNOLOGY RESOURCES

The IT provider must evaluate and approve all software, hardware, removable devices and related maintenance and support contracts, whether the selected products or solution will be on the network or off; used by one or many people; and for all program and project funding sources. Most District-owned technology has a pre-determined lifecycle replacement period and must be surrendered for replacement on a 1:1 basis or retired, according to that schedule. Such technology may not be redeployed or otherwise put back into use without approval from the IT provider.

5.0 ACCESS TO THE DISTRICT'S TECHNOLOGY RESOURCES

- The District General Manager or a designee must approve the setup of new user accounts.
- Users are responsible to establish and maintain passwords consistent with the IT provider's standards.
- User accounts and ALL passwords may not be shared with anyone other than the named owner. Examples include co-workers, subordinates, business associates, household members, etc.
- The individual logged onto the District network must be present while the logon credentials are being used to access Network resources, or must ensure that the account is locked or logged off and not being used by others when not present.
- The IT provider must approve connection of all devices using the District's infrastructure (i.e.; Internet, network, wireless channels and telephone lines).
- The IT provider must approve installation of all software, including shareware, freeware and software that is obtained for evaluation purposes.
- Direct peer-to-peer connections and modems are provided only in unique circumstances, requiring prior approval from The IT provider.
- Connection or installation of personally-owned hardware or software with the District-provided infrastructure (i.e. network, Internet, fax lines, telephone lines, and other computers) is not allowed.
- All activity resulting from device, network or software application access is the responsibility of the person assigned the user account.

6.0 PERSONAL USE

Technology resources may be used for incidental personal needs as long as such use does not result in or subject the District to additional cost or liability, interfere with business, productivity or performance, pose additional risk to security, reliability or privacy, cause or tend to cause damage to the District's reputation or credibility, or conflict with the intent or requirements of any District policy or work rule. Incidental personal usage should generally conform to limits typically associated with personal phone calls and shall comply with Policy 276. This document does not attempt to address every possible situation that may arise. Professional judgment, etiquette, and common sense should be exercised while using District technology resources. Please note that any data stored on District systems including but not limited to email, documents, and photos may be subject to public disclosure requests.

7.0 INTERNET/INTRANET USAGE

7.1 This technology usage agreement outlines appropriate use of the Internet/Intranet. Usage should be focused on business-related tasks. Incidental personal use is allowed as discussed under this section, but there is no right to privacy in an employee's use of the Internet/Intranet. Employee internet usage is monitored. Web Usage Reports will be provided to the District General Manager to assist in monitoring staff's use of the Internet.

7.2 Use of the Internet, as with use of all technology resources, should conform to all District policies and work rules. Filtering software will be used by the District to preclude access to inappropriate web sites. Attempts to alter or bypass filtering mechanisms are prohibited.

7.3 Except for District business related purposes, visiting or otherwise accessing the following types of sites is prohibited:

- "adult" or sexually-oriented web sites
- sites associated with hate crimes or violence
- personal dating sites

- gambling sites
- shopping sites
- sites that may be offensive to a reasonable person Personal social media accounts

8.0 DISTRICT SOCIAL MEDIA ACCOUNTS

The District recognizes that public Internet communications technologies are effective tools to promote community and government interaction and that District employees want to participate in public communication via blogging, discussion forums, wikis, mashups, social networking, message boards, e-mail groups and other media that are now commonplace tools by which the District may want to share ideas and information. However, since activities on public Internet communication sites are electronically associated with District network addresses and accounts, the following rules must be followed for participation on these interactive public Internet communication sites on behalf of the District:

8.1 Staff should not express personal views on the District's social medial accounts.

8.2 Always protect the confidentiality, integrity, and availability of all critical information. Keep in mind, all records created on the District's social media accounts are subject to records retention requirements and may be subject to public disclosure.

8.3 Employees must not post any material that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful, or embarrassing to or of any other employee, person, and/or entity.

8.4 To protect staff's privacy and the privacy of others, phone numbers or email addresses must not be included in the content body.

8.5 Public Internet communications activity should contribute to staff's body of work as an employee of the District and must not interfere with or diminish productivity.

9.0 E-MAIL USAGE

9.1 E-mail content must be consistent with the same standards as expected in any other form of written (or verbal) communication occurring in a business setting where documents are subject to public disclosure.

9.2 Users must manage their e-mail in accordance with records retention policies and procedures as defined and identified by the Records Retention Policy.

Commented [TC1]: Do you have an actual policy for records retention? If not, maybe change this to…"the Secretary of State record retention schedule."

9.3 Users should be attentive to emails that have unusual or questionable subject lines to mitigate spam, phishing and script born viruses that come into the network through email attachments or by clicking on links that lead to hostile web sites. If you suspect phishing or script born viruses in email attachments immediately contact IT Support (CMIT).

9.4 The use of e-mail to send or solicit the receipt of inappropriate content such as sexually oriented materials, hate mail, content that a reasonable person would view as obscene, harassing or threatening and having no legitimate or lawful purpose or contents falling within the inappropriate categories for internet usage is prohibited.

9.5 The incidental personal use of e-mail from a District account to express opinions or views other than those reflective of District policy must contain the following disclaimer: "The contents of this electronic mail message do not necessarily reflect the official views of the elected officials or citizens of the District."

10.0 SECURITY, STORAGE, AND PROTECTION

- District devices and computer equipment must be logged out or "locked" when unattended.
- All users must log off of their pc and leave it powered on at the end of their shift to enable off shift maintenance and security updates.
- Intruding or attempting to intrude into any gap in system or network security is prohibited.
- Sharing of information with others that facilitates their unauthorized access to the District's data, network or devices, or their exploitation of a security gap is also prohibited.
- It is the responsibility of each individual to prevent unauthorized and indiscriminate access to "personal information" (see Definitions) that could pose the threat of identity theft, thus risking a person's privacy, financial security and other interests.
- As noted above, user accounts and passwords may not be shared. The individual logged onto the District network must be present while logon credentials are being used to access Network resources
- In general, it is not permissible to download any information to any removable/portable device, including laptop computers, unless access to that information is within the scope of your job, your manager has approved the copy of information to a portable device and the data or device is encrypted. Removable devices such as USB drives and PDA/handhelds/smart phones, cameras, etc., must always be password-enabled.
- Transmitting confidential data in part or full via e-mail or another unencrypted medium is prohibited.
- 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.
- Individuals must report to the District any equipment, software or data that is lost, damaged or stolen at their first available opportunity. Reports will be made to a supervisor, manager or director. Unrecoverable equipment may incur additional replacement costs.
- Lost equipment, especially that containing sensitive or confidential information as defined here, must be reported immediately to the District General Manager
- Stolen computers, laptops, PDA's, thumb drives, etc. must be reported immediately (24 hours per day) to the District General Manager.
- Individuals must utilize District provided anti-virus software and scanning tools regularly to scan material from removable devices prior to use.
- Storage of any copyrighted material on a network server or local hard drive including, but not limited to, photographs from magazines, books or other copyrighted sources, copyrighted music, the installation of any copyrighted software for which the District or end user does not have an active license, or the installation of "pirated" software is strictly prohibited.

11.0 PASSWORD POLICY

11.1 This password policy applies to the following:

- Transaction programs
- Scheduling programs
- Access to firewall hardware and software
- Access to VOIP software and hardware
- Access to any server based shared drives or cloud based storage systems.
- All computers and portable computers

- Passwords shall comply with the following:
- Must be at least eight characters in length
- Use of both upper- and lower-case letters
- Inclusion of one or more numerical digits
- Inclusion of special characters, e.g. @, #, $ etc.
- No use of words found in a dictionary or the user's personal information
- No use of passwords that match the format of calendar dates, license plate numbers, telephone numbers, or other common numbers
- No use of company name or an abbreviation
- No use of an Environ password, of the following form: consonant, vowel, consonant, consonant, vowel, consonant, number, number (for example pinray45).

11.2 Passwords shall be changed immediately when prompted or if an intrusion has been detected. Passwords must be routinely changed every 90 days.

Employees shall:

- Never share an account or password
- Never tell a password to anyone, including people who claim to be from customer service or security
- Never communicate a password by telephone, e-mail or instant messaging
- Being careful to log off before leaving a computer unattended
- Changing passwords whenever there is suspicion they may have been compromised
- Never use online password generation tools

Violation of this Password Policy may result in discipline, up to and including termination.

12.0 SCANNING PORTABLE STORAGE DEVICES AND EMAIL ATTACHMENTS

All computers will be configured to scan any portable storage devices prior to opening the storage device. MAC computers may install the most current software version which will automatically scan any portable drives or email attachments prior to opening the device.

13.0 FIREWALL SERVER FILTERING

The District's IT provider will ensure the District firewall does a perimeter filtering of all incoming information, emails, attachments or files prior to anyone accessing the external files or information. Updates of the Firewall filtering will be done on a scheduled basis.

14.0 TRAINING

Training of existing employees will be done at least once per year on our IT policy and security. New employees will be trained upon hiring.

15.0 EMPLOYEE OR CONTRACTOR SEPARATION

Upon separation of any District employee or contractor, all access to any and all computers and programs shall be removed by the Aquatic Manager to prevent unauthorized access. Removal includes:

- Transaction programs
- Scheduling programs
- Access to firewall hardware and software
- Access to VOIP software and hardware
- Access to any server based shared drives or cloud based storage systems.
- All computers and portable computer

16.0 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 District's assets or data, should immediately report these to their department Supervisor, manager or director. Violations may result in disciplinary action up to and including termination of employment. Requests for exceptions to any of the Technology Usage Policy definitions must be submitted in writing to management. Exceptions require the approval of both the requesting department's management and the District Manager. Approvals must be documented in writing and limited in duration to provide for periodic re-evaluation.