Agenda Item No. F-8

DATE SUBMITTED	08/29/2020
SUBMITTED BY	R. Alejandro Estrada
DATE ACTION REQUIRED	08/05/2020

COUNCIL ACTION	(x)
PUBLIC HEARING REQUIRED	( )
RESOLUTION	( )
ORDINANCE 1ST READING	( )
ORDINANCE 2ND READING	( )
CITY CLERK'S INITIALS	

IMPERIAL CITY COUNCIL
AGENDA ITEM

SUBJECT: DISCUSSION/ACTION:

1. APPROVE AND ADOPTION OF THE ACCENPTABLE USE POLICY (AUP)

DEPARTMENT INVOLVED: DEPARTMENT OF INFORMATION TECHNOLOGY

BACKGROUND/SUMMARY:

The City of Imperial Department of Information Technology's (DoIT) intentions for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to the City's established culture of openness, trust, and integrity. DoIT is committed to protecting the City of Imperial's employees, partners, and the City from illegal or damaging actions by individuals, either knowingly or unknowingly.

FISCAL IMPACT:

FINANCE INITIALS

STAFF RECOMMENDATION:

It is staffs recommendation to approve the AUP Policy.

DEPT. INITIALS

MANAGER'S RECOMMENDATION:

The City Manager agrees with staffs recommendation.

CITY MANAGER's INITIALS

MOTION:

SECONDED:
AYES:
NAYES:
ABSENT:

APPROVED ( ) REJECTED ( )
DISAPPROVED ( ) DEFERRED ( )

REFERRED TO:

1. Overview

The City of Imperial Department of Information Technology's (DoIT) intentions for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to the City's established culture of openness, trust, and integrity. DoIT is committed to protecting the City of Imperial's employees, partners, and the City from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of the City of Imperial. These systems are to be used for business purposes in serving the interests of the City, and of our community/customers/citizens in the course of normal operations.

Effective security is a team effort involving the participation and support of every City employee and affiliate who deals with information and information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at the City of Imperial. These rules are in place to protect the employee and the City. Inappropriate use exposes the City to risks, including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct City business or interact with internal networks and business systems, whether owned or leased by the City, the employee, or a third party. All employees at the City of Imperial are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources and in accordance with the City policies and standards, local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, at the City of Imperial, and to all equipment that is owned or leased by the City.

4. Policy

4.1 General Use and Ownership

4.1.1 The City of Imperial proprietary information stored on electronic and computing devices, whether owned or leased by the City, the employee, or a third party, remains the sole property of the City of Imperial. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Best Practices.*

4.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of the City of Imperial proprietary information.

4.1.3 You may access, use, or share proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment, the use of city resources for personal use is prohibited.

4.1.5 For security and network maintenance purposes, DoIT may monitor equipment, systems, and network traffic at any time.

4.1.6 The City of Imperial reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.

4.2.2 System-level and user-level passwords must comply with the High encryption password Standards.

4.2.3 Providing access or remote access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.4 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 20 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.5 Postings by employees from a City of Imperial e-mail address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the City of Imperial unless posting is in the course of business duties.

4.2.6 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempt from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of the City of Imperial authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing the City of Imperial-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City of Imperial.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the City of Imperial or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server, or an account for any purpose other than conducting City business, even if you have authorized access, is prohibited.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to the export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. Revealing your account password to others or allowing the use of your account by others. This includes family and other household members when work is being done at home.

7. Using a City computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any City account.

9. Making statements about warranty, expressly or implied, unless it is a part of regular job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to DoIT is made.

12. Executing any form of network monitoring, which will intercept data not intended for the employee's host, unless this activity is a part of the employee's regular job/duty.

13. Circumventing user authentication or security of any host, network, or account.

14. Introducing honeypots, honeynets, or similar technology on the City of Imperial network.

15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

17. Providing information about, or lists of, the City of Imperial employees to parties outside City.

18. Using a City computing asset, including mobile devices (laptops, cell phones, etc.) for personal activities or none City business-related, is prohibited.

4.3.2 E-mail and Communication Activities

When using City's resources to access and use the Internet, users must realize they represent the City. Whenever employees state an affiliation to the City, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the City". Questions may be addressed to the DoIT.

1. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
2. Any form of harassment via e-mail, telephone or texting, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of e-mail header information.
4. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited e-mail originating from within the City of Imperial's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the City or connected via City's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
8. The City of Imperial e-mail address shall be used for City business-related only, and never configured on a personal device.

4.3.3 Blogging and Social Media

1. Blogging by employees, whether using the City of Imperial's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of the City of Imperial's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the City of Imperial's policy, is not detrimental to the City of Imperial's best interests and does not interfere with an employee's regular work duties. Blogging from the City of Imperial's systems is also subject to monitoring.

2. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the City of Imperial and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when blogging or otherwise engaging in any conduct prohibited by the City of Imperial's *Non-Discrimination and Anti-Harassment* policy.

3. Employees may also not attribute personal statements, opinions, or beliefs to the City of Imperial when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not expressly or implicitly represent themselves as an employee or representative of the City of Imperial. Employees assume any and all risks associated with blogging.

4. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, City's trademarks, logos, and any other City intellectual property may also not be used in connection with any blogging activity

5. Policy Compliance

5.1 Compliance Measurement

The DoIT team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the DoIT team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Definitions and Terms

- Blogging
  - Short for Weblog, a blog is a Web page that serves as a publicly accessible personal journal for an individual. Typically updated daily, blogs often reflect the personality of the author. (v.) To author a Weblog. Other forms: Blogger (a person who blogs).
- Honeypot
  - A honeypot is a network-attached system set up as a decoy to lure cyber attackers and to detect, deflect, or study hacking attempts in order to gain unauthorized access to information systems.
- Honeynet
  - A honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack so that an attacker's activities and methods can be studied and that information used to increase network security.
- Proprietary Information

- In the United States, CPNI (Customer Proprietary Network Information) is information that telecommunications services such as local, long-distance, and wireless telephone companies acquire about their subscribers. It includes not only what services they use but their amount and type of usage.

- Spam
  - E-mail spam is not only annoying but also dangerous to users. So, what is e-mail spam? E-mail spam is nothing but junk e-mail or unsolicited bulk e-mails sent through the e-mail system. It refers to the use of an e-mail system to send unsolicited e-mails, especially advertising e-mails to a group of recipients.

EMPLOYEE ACKNOWLEDGMENT

If you have additional questions about this policy, please contact Human Resources before signing the following agreement.

I have read the City of Imperial's policy on the use of e-mail, network, and internet/intranet and agree to abide by it. I understand that violation of any of the above policies may result in discipline, up to and including termination.

User Name (Printed)	User Signature	Date