

Department owner/sponsor:
IT Department/IT Advisory
Team (ITAT)

Effective: July 1, 2010
Supersedes: E-mail
Retention Policy and
Internet and Electronic
communication Use Policy

Policy: Information Systems Resources Usage

Policy Statement: Information systems resources used by the General Government and Department of Public Utilities employees shall be used in accordance with Federal, State and City of Tacoma laws, regulations and policies.

Purpose: To safeguard and protect information systems resources by establishing acceptable and appropriate use of those resources. For purposes of this policy the term information systems resources does not include those independent systems, data, networks and related equipment and software owned, operated and maintained by the Department of Public Utilities pursuant to City Council Resolution 37550.

Background: The following policy defines appropriate use of the information systems resources of the City of Tacoma’s data network, computers, all related peripherals, software, electronic communications, and Internet access. They apply to the access of the City’s network and use of computing information systems resources at any location, from any device, via wired or wireless connection. They apply to all users of City information systems resources regardless of employment status. Access to all networks and related information systems resources require that each user be familiar with these policies and associated work rules. The City of Tacoma authorizes the use of computing and network resources by City employees, contractors, volunteers and others to carry out legitimate City business. All employees of City computing and network resources will do so in an ethical, legal, and responsible manner. All use of technology resources must be consistent with the intent and requirements of all City policies and work rules. Information systems resources may not be used to facilitate operation of a personal business.

1. Ownership of Data/Monitoring Use On Information Systems Resources

The City owns all data stored on its information systems resources, including email, voicemail, file servers, computers and Internet usage logs and reserves the right to inspect and monitor any and all such data at any time, for any business purpose, with or without notice to the employee. The City may conduct random audits of employee accounts in order to ensure compliance with policies and requirements, to investigate suspicious activities that could be harmful to the organization, to assist Departments in evaluating performance issues and concerns, and to identify productivity or related issues that need additional educational focus within the City. All data on the City’s information systems resources, such as internet, wireless, and email communications are subject to public disclosure and the rules of discovery in the event of litigation. The City’s Internet, email, voicemail, text message, etc. 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 City information systems resources.

2. Personal Use

Information systems resources may be used for incidental personal needs as long as such use does not result in, or subject the City to, additional cost, or liability, interfere with City business, productivity or performance, pose risk to security, reliability or privacy, cause or tend to cause damage to the City’s reputation or credibility, or conflict with the intent or requirements of any Federal, State or City law, or City policy or work rule. Personal usage of information systems resources should generally conform to limits typically associated with personal phone calls. This document does not attempt to address every possible situation that may arise. Professional judgment, etiquette, and common sense should be exercised while using City information systems resources. This document provides policies and general rules for appropriate uses of resources. Employees’ use of information systems

resources in violation of this policy or otherwise inappropriate information systems resources usage is subject to disciplinary actions up to and including termination, as provided in 9.1.3.5 below.

3. Policy Intent

The policy is designed to establish acceptable and appropriate use of computer and information systems, networks and other information technology resources of the City of Tacoma. The purpose of this policy is to safeguard and protect all information systems resources from anything other than authorized and intended use. The main points are:

- a. The City provides computing and network resources ('information systems resources') to carry out legitimate City business.
- b. Employees shall use City provided information systems resources in compliance with the City of Tacoma Code of Ethics, TMC 1.46, and other applicable City of Tacoma rules and policies.
- c. Employees shall abide by all legal protections, copyrights, and licensing agreements associated with programs and data while using City information systems resources.
- d. Employees shall protect City data and access to City information systems resources from unauthorized use or disclosure.
- e. In addition to complying with City of Tacoma Code of Ethics, TMC 1.46 and all other applicable City of Tacoma rules and policies, employees may make reasonable use of City information systems resources for non-City purposes only under the following circumstances:
 - i. There is no direct measurable cost to the public regarding its use, or the direct measurable cost is so negligible that it would be fiscally impracticable to track expenditures, collect reimbursement, and audit such practices; AND
 - ii. There is no negative impact on employee performance of public duties.

Employees shall have no expectation of privacy in their use of City information systems resources provided in the course of employment, and all such use may and will be monitored or audited at anytime without notice. All content of electronic records, including emails, are subject to disclosure.

4. Internet/Intranet Usage – Usage is for City business related tasks. Incidental personal use is allowed as long as it does not conflict with City policies and work rules.

- 4.1 Use of the Internet, as with the use of all information systems resources, should conform to all City code, policies and work rules.
- 4.2 Filtering software is actively used by the City to preclude access to inappropriate web sites. Exemptions to web filtering may be granted if there is a requirement in the conduct of official City business. Requests for exemptions need to be made by an authorized manager to the Information Technology Department. Attempts to alter or bypass filtering mechanisms are prohibited. Attempts to bypass the filtering mechanisms will be reported to the user's department.
- 4.3 Activities on Internet chat rooms, blogs and interactive web communication sites are reflective of the City of Tacoma and are electronically associated with City network addresses and accounts. Your activity can be easily traced back to the City of Tacoma. Therefore, all you're your communications shall be reflective of City policy.

5. Email Usage – Email on the City's information systems resources is the property of the City. There is no right to privacy.

- 5.1 Email content must conform to the same standards expected in any other form of written communication occurring in a business setting; all retained emails are subject to public disclosure.
- 5.2 Employees must manage their email in accordance with record retention policies and procedures as defined by the State Guidelines. The content of an email determines the retention period assigned to the message. Employees must determine whether messages sent and received are public records with retention value, or that they have no retention value and therefore may be destroyed when no longer

needed. In determining the proper length of retention for email, consider each message just as if it were conveyed on paper. Emails with no retention value should be deleted once the business function it relates to has been completed. If the email is not a public record and has no business value it should be deleted immediately.

- 5.3 Email accounts must be managed within assigned capacities. Email mailboxes have a maximum capacity. Email messages should be retained if necessary (see 5.2) or deleted. If Message (PST) files are utilized, they must be stored on a network drive (not on a computer's "C:" drive).
- 5.4 All broadcast email (addressed to "DIST All...") are to be approved by General Government department directors or TPU division heads before being sent. Under no circumstances should an employee "Reply to All" to an email sent to every email account in the City.
- 5.5 The City provides employees access to and support of the Exchange/Outlook messaging (email) system. Access or usage of any other messaging systems is not allowed unless it is web based. Subject to the personal use limitations explained above, employees may access web-based personal email but should not download personal documents or attachments from these sites.
- 5.6 Employees should be attentive to emails that have unusual or questionable subject lines, senders, etc. 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 phishing or script born viruses is suspected by an employee to be contained in email attachments, they must immediately contact their Computer Support Representative.
- 5.7 The use of email 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.
- 5.8 For purposes of disaster recovery, backups of the email system are retained for seven days. Only in the event of total system disaster or corruption will the backup be restored, thereby overwriting all email to a previous date/time. For this reason backups are not restored to recover items for an individual email inbox.

6. Social Networking and Instant Messaging

- 6.1 Refer to General Governments and TPU's *Social Media Policy* for further information and clarification.
- 6.2 Social networking sites such as Twitter, Facebook, etc., should only be utilized by departments with need for such activity. All activity on these sites should be captured to ensure records are managed in accordance with retention rules.
- 6.3 Instant Messaging (IM) –Instant Messages on the City's system are the property of the City. There is no right to privacy.
- 6.4 Instant Messaging content must conform to the same standards expected in any other form of written communication occurring in a business setting. Departments with a business need to utilize Instant Messaging should have a process for capturing all IM's.
- 6.5 All documents posted to any social networking site or captured in Instant Messaging are subject to public disclosure.

7. Security – Employees are responsible for protecting City equipment and data, no matter what technology.

- 7.1 Employees are assigned unique user ID's and passwords for network access. Passwords shall be complex and expire every 120 days either via automated methods, as with the network password, or manual methods, incumbent upon the employee to change their password every 120 days, as with the SAP system. Access to systems and applications containing critical information are allowed via unique user IDs. Access will be monitored and actions will be traceable to authorized employees.
 - 7.2 Employee shall not share their user ID or password with any other person. If computer support representatives or technical employees become aware of an employee's password while troubleshooting an issue, the employee shall change their password upon completion of troubleshooting.
 - 7.3 The use of another person's account or attempt to capture other employees' passwords is prohibited. Each employee is responsible for restricting unauthorized access to the network by locking their computer or logging out of their computer account when leaving their computer unattended. If you discover unauthorized use of your account, immediately report it to **Network SUPPORT Center (NSC) or (253) 591-2057.
 - 7.4 The City of Tacoma will take the necessary steps to protect the confidentiality, integrity, and availability of information.
 - 7.5 Employees must take reasonable steps to ensure the safety of City information contained on information systems resources including: encrypting data any time it is electronically transported outside the City network, encrypting of portable devices such as computer laptops; ensuring that inadvertent viewing of information does not take place, and destroying or rendering the information unreadable when done with it.
 - 7.6 The City will restrict access to critical information only to employees that have a legitimate business need-to-know. Each system owner is responsible for keeping an inventory of critical information and ensuring that access to it is limited.
- 8. Network Access and Usage – IT must approve all devices connecting to the City's network.**
- 8.1. The Information Technology Department (ITD) must approve connecting devices to the City's network. This includes PCs, network hubs and switches, printers, handhelds, scanners, remote connections, wireless access points, and any other wireless or wired devices. In many cases, the connecting devices, such as wireless access points, are centrally managed by ITD to ensure network stability.
 - 8.2 The use of personal routers and wireless access points on the City network is not allowed. Connecting such devices can have a detrimental effect on the network for all employees.
 - 8.3 Personal software or devices may not be loaded or attached to any City-owned equipment without written authorization by a designated department manager.
 - 8.4 Attached City PCs and servers shall have the standard anti-virus software loaded, active and maintained for prevention and detection of viruses. Any one device not properly protected can have a detrimental effect on the network for all employees.
 - 8.5 Exploiting or attempting to exploit any vulnerability in any application or network security is prohibited. Sharing of internal information to others that facilitates their exploitation of vulnerability in any application or network security is also prohibited. It is also prohibited to knowingly propagate any kind of spyware, denial of service attack, or virus onto the City network or computers. If you encounter or observe vulnerability in any application or network security, report it to **Network SUPPORT Center (NSC) or (253) 591-2057.

- 8.6 Obey privacy rules governing the use of any information accessible through the network, even if that information is not securely protected.
- 8.7 Non-COT employees (e.g. vendors, contractors) are required to have their PC scanned for virus detection prior to connecting to the COT network. Representatives of the contracting departments are responsible for assisting their contractors to engage their Computer Support Representative to perform these services.
- 8.8 Disabling, altering, over-riding, or turning off any mechanism put in place for the protection of the network and workstation environments is strictly forbidden.
- 8.9 Because of band-width limitations inherent in any network system, use of the City network to download non-business related information is prohibited. Examples of potentially non-business related information include streaming video of baseball games, streaming audio of radio programs, MP3 files, and on-line games.
- 8.10 Transmission, distribution, or storage of any information or materials in violation of federal, state or municipal law is prohibited. Software that is copyrighted or licensed may not be shared or illegally distributed. Copyright violations are federal offenses that may result in civil and criminal penalties to employees and the City of Tacoma.
- 8.11 Employees must manage their electronic documents in accordance with record retention policies as established by the State Guidelines. Documents past their retention schedules should be deleted from the network to save space and eliminate the need to backup unnecessary files. In addition, employees shall not store files, documents, pictures, etc on the network storage devices which are not related to City business.
- 8.12 Access to the City's network via VPN requires approval from ITD. VPN accounts will be audited on a quarterly basis and accounts inactive for 30 days will be deactivated unless an exception is granted by ITD. Reactivation of intermittently used VPN accounts for vendor support purposes will be accommodated upon request.
- 8.13 TPU will coordinate the access and connection to the City's networks and systems with ITD for independent systems, networks and related equipment operated and maintained by TPU.

9. Administration, Reporting and Violations/Discipline – Disciplinary action, up to and including termination, may be applied to anyone violating the use of technology policies.

Each Department will designate specific employees who have the authority to authorize ITD to provide accounts and access to information systems resources. Suspected violations or concerns should be reported to Department, Division or IT management.

- 9.1 ITD, the Departments and HR share responsibilities in enforcing these policies, specifically:

- 9.1.1 ITD's Responsibilities**

- 9.1.1.1 ITD is responsible for recommending information systems resources usage policy guidelines that are enforceable.

- 9.1.1.2 ITD, if requested, is responsible for enterprise monitoring of information systems resources using security and monitoring tools. Security and monitoring information will be provided to HR or the department as requested to support the investigation of information systems resources usage policy infractions.

9.1.1.3 If, in the normal course of business activities, ITD discovers violations of this Information Technology Resource Usage Policy, ITD will report the activities to the employee member's Department Director, Director of HR and /or to the City Manager.

9.1.2 Departments' Responsibilities

9.1.2.1 Departments assist in the development and adoption of this Information Technology Resources Usage Policy through participation in the ITAT.

9.1.2.2 If, in the course of normal business activities, department management suspects an employee member is violating this Policy, they will report the suspected infractions to Human Resources and ITD.

9.1.2.3 Departments are responsible for carrying out any disciplinary actions in response to Information Technology Resource Usage Policy violations.

9.1.2.4 Departments will review the Information Technology Resources Usage Policy annually with their employees.

9.1.3 Human Resources' Responsibilities

9.1.3.1 Human Resources are responsible for integrating this Information Technology Resource Usage Policy into new hire training, orientation and ongoing training of City work rules and policies.

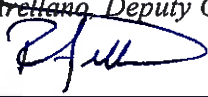
9.1.3.2 Human Resources are responsible for the evaluation of reported infractions of this Information Technology Resource Usage Policy and may request additional monitoring information (e.g., security logs) from ITD as part of their investigation and evaluation process.

9.1.3.3 Human Resources are responsible for providing necessary information to Department heads to facilitate the consistent application of disciplinary action when infractions of the Information Technology Resources Usage Policy occur.

9.1.3.4 As with any set of policies or rules, exceptions may be granted and documented on a case-by-case basis. These require authorization from the Department involved as well as from ITD.

9.1.3.5 Violations of this Information Technology Resource Usage Policy and Work Rules or otherwise inappropriate use of information systems resources are subject to disciplinary action up to and including termination.

9.1.3.6 Should a suspected violation potentially involve independent systems, networks and related equipment operated and maintained by TPU that are connected to information systems resources occur, ITD in partnership with TPU shall jointly investigate and report findings and measures taken involving information systems resources and disciplinary actions.

Reference:	<i>City of Tacoma Code of Ethics, Tacoma Municipal Code Chapter 1.46 Title 40 RCW (Revised Code of Washington) , Public Documents, Records, and Publications Chapter 40.14 RCW - Preservation and Destruction of Public Records Chapter 42.56 RCW - Public Records Act Records Management Guidelines for Local Government Agencies of Washington State</i>
Contact Info:	<i>Bill Bogue, IT Assistant Director, 253-573-2358</i>
Policy History:	<i>Consolidates and supersedes the E-mail Retention Policy and the Internet and Electronic Communications Use Policy</i>
Approval:	<i>Rey Arellano, Deputy City Manager and Chief Information Officer</i> 
Date:	<i>8/16/10</i>