



Policy: Technology Acceptable Use

Purpose

This policy establishes acceptable and appropriate use of computer and information systems, software, networks, and other information technology assets used by City of Tacoma, Tacoma Public Utilities, and Tacoma Public Library employees, contractors, volunteers, and others to conduct City business. The purpose of this policy is to safeguard and protect City technology assets from anything other than authorized and intended use.

Scope

This policy applies to City of Tacoma, Tacoma Public Utilities, and Tacoma Public Library employees, elected officials, contractors, consultants, volunteers, vendors, and anyone else who has access to the City's physical and/or electronic information or data.

This policy does not apply to use of technology services provided for the public by Tacoma Public Library, which is governed by Tacoma Public Library's Public Use of Internet policy.

Definitions

Category 3 Confidential Information, Category 4 Confidential Information with Special Handling – See Information Classification Policy 4.30

Information Asset Owner – Individuals, normally the department head or a manager within a department, who serve as the primary contact for an information asset. They have *business* subject matter expertise and are responsible for understanding and communicating the business requirements associated with an information technology asset. They determine asset's value, criticality, and classification/sensitivity and disseminate this information so that appropriate protections can be implemented and enforced.

Multi-factor authentication (MFA) – a multi-step account login process that requires users to use a second source of validation before access is granted.

Cybersecurity Incident – an occurrence that actually or potentially jeopardizes, without lawful authority, the confidentiality, integrity or availability of information or an information system; or constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Technology Users - City of Tacoma, Tacoma Public Utilities, and Tacoma Public Library employees, elected officials, contractors, consultants, volunteers, vendors, and anyone else who has access to the City's physical and/or electronic information or data.

Policy Statements

The City of Tacoma authorizes the use of technology systems and services to carry out legitimate City business. All technology use is expected to be legal, ethical, and compliant with applicable copyright laws and with the terms of applicable licenses, contracts, and agreements.

Employee use of City technology in violation of this policy or otherwise inappropriate technology systems usage may be subject to disciplinary action, up to and including termination.

1.0 Acceptable Use

Technology Users are encouraged to make maximum use of City technology systems and services for the purpose of accomplishing the business of the City.

Technology Users should be aware that activities online are reflective of the City of Tacoma and are electronically associated with City network addresses and accounts. Activity can be easily traced back to the City of Tacoma. All online communications made while utilizing City technology systems and accounts shall be reflective of City policy and Guiding Principles.

1.1 Store Data in Designated Systems

City data should be stored and managed in the system where it is utilized for City business.

For example, Technology Users shall not:

- Establish accounts in cloud storage systems or collaboration solutions (such as Dropbox or Slack) to store or share City data without authorization
- Establish forwarding rules that send all City e-mail to personal or non-City e-mail accounts
- Transmit, store, share, display or otherwise expose Category 3 or Category 4 information outside of the system where it is utilized for City business without explicit direction by the Information Asset Owner

Technology Users should avoid storing City data solely on portable storage devices such as USB drives, local C drive of City laptops, or on mobile devices, to avoid the risk of data loss.

Category 3 and Category 4 Information should not be stored on portable storage devices such as USB drives or local C drives of City laptops, except for brief periods of time based on business necessity.

1.2 Retain Data Consistent with State Guidelines

Technology users must manage City electronic documents in accordance with record retention policies as established by Washington State Local Government Retention Schedules.

Records may be deleted when they have been kept long enough to meet any requirements, they are no longer needed by you, or others, for business and they are not on any legal or public disclosure holds.

For help with specific requirements, and to document destruction of public records, contact your Records Coordinator.

1.3 Follow Copyright Guidelines

Technology users should be aware that many types of content such as web page graphics, film clips, trademarks, photos, and logos may have copyright/usage restrictions.

Identify and obtain required permissions prior to copying or distributing copyrighted works.

1.4 Limit Personal Use

Incidental or “de minimus” personal use of City technology is allowed as long as such use is in compliance with this policy and does not result in, or subject the City to, additional cost or liability, or interfere with City service delivery, or your productivity or performance. This Policy does not attempt to address every possible situation that may arise. Professional judgement, etiquette, and common sense should be exercised.

Personal files should not be permanently stored on City systems. Be aware that the City owns all data and content stored on its information systems, and that all data stored on the City’s information systems is subject to public disclosure and the rules of discovery in the event of litigation.

1.5 Limit Collection of Personal Information

Technology users should limit collection of personal information about individuals, particularly more sensitive information such as social security numbers, birth dates, and other similar attributes, that, if lost, compromised or disclosed without authorization, could result in harm to the individual. Limit collection of personal information to attributes that are required for the business need.

Protect Category 3 and Category 4 information transmitted or stored in systems or on paper consistent with Information Classification Policy 4.30 and related policies, procedures, and standards.

1.6 Recognize Additional Policy Requirements

Technology users should be aware that several other policies provide direction regarding technology use and security. A partial list of key policy statements is provided below.

Topic	Key Messages Regarding Technology Use	Policy
Anti-Discrimination and Harassment	Communications must not be discriminatory or harassing toward others	Antidiscrimination and Harassment Policy #130
Badge Protection	Take care to ensure safety and appropriate use of identification badges	City Identification Badges #3.03 TPU Access Control and Key Policy #3.08
Confidential Information	Category 3 and Category 4 information must be protected	Information Classification Policy #4.30
Information Security Program	Describes Enterprise Information Security program including roles, responsibilities, and exception management	Enterprise Information Security Policy #4.50
Meeting Recordings	Meetings may not be recorded unless there is a valid business reason	Meeting Recording Guidelines
Mobile Device Usage	See detailed policy guidance regarding use of Mobile Devices	Mobile Device Policy #4.20
Personally Owned Technology	Provides more detailed guidance regarding use of Personally Owned Technology	Limitations of Use for Personally Owned Technology – City of Tacoma Guideline
Purchasing Approvals	Technology purchases may require extra approvals and must meet technology standards. This includes purchase of hardware, software, software as a service, domain names, SSL certificates and other technology assets. Initiate requests by contacting the IT Service Desk.	Purchasing #FIN 2.0

Topic	Key Messages Regarding Technology Use	Policy
Social Media	Refer to Social Media policy prior to using Social Media for work purposes	Guidelines for Establishing Department Social Media Accounts TPU Social Media Policy
Telework	Follow policy and enrollment processes related to alternate work arrangements	Managing a Telework Arrangement Policy #3.17

1.7 Use of Personally Owned Technology

Technology users seeking additional guidance regarding use of personally owned technology beyond this policy section should refer to the City’s Limitations of Use for Personally Owned Technology Guideline and Mobile Device Policy.

1.7.1 Acceptable Uses

Personally-owned devices such as mobile phones and tablets may be used as follows:

- To access browser-based Tacoma technology systems such as e-mail and calendars. City records are retained in the web-based system and are not stored on the device.
- To be used for Multi-Factor Authentication, because doing so does not create City records subject to public disclosure on the device.
- To obtain Wi-fi access by connecting to “TacomaGuest”, “TPL” or other guest networks

Use of personal devices may be denied access if an insecure configuration is detected.

Technology users should charge personally owned devices via a power adapter plugged into power outlet rather than via connection to City computers.

Installation of mobile device management software will be required on authorized mobile devices, which includes City-owned devices and Employee-owned devices which have been authorized for business use. Authorized mobile devices will be allowed to do the following:

- Utilize native app connections to City cloud resources such as Outlook, OneDrive, and Teams
- Utilize local data synchronization
- Connect directly to the City’s wireless network

1.7.2 Unacceptable Uses

Network-capable personal computers and equipment may not be plugged into network jacks or otherwise connected to the City’s network while onsite.

Personal software or devices may not be loaded or attached to any City-owned equipment without written authorization by designated department manager.

Use of personal routers and wireless access points on the City network is not allowed.

2.0 Unacceptable Use

City technology may not be used to engage in any activity that:

- Violates laws, codes, regulations, or City policies
- Harasses or threatens others
- Uses information systems to promote, advertise or solicit for commercial ventures, religious or political causes, or for personal gain unrelated to the processes of working for or on behalf of the City unless explicitly allowed by law or City policy

- Uses technology for any discriminatory or harassing conduct on the basis of race, creed, color, family status, ancestry, marital status, national origin, sex, sexual orientation, gender identity, genetic information, age, religion, disability, or the use of a trained dog guide or service animal, or status as a veteran
- Violates copyright laws or applicable licenses
- Violates software licenses, contracts, or agreements
- Violates City Code of Ethics, Personnel Management Policies, or for Library employees violates Library personnel rules

3.0 Security

3.1 Technology Access

Access to City files and systems shall be granted when a valid business need exists to access those files. The City restricts access to information only to employees that have a legitimate need-to-know.

Departments shall designate employees who have authority to authorize accounts and access to technology resources.

When employees transfer from one position or role to another within the City, access to systems should be reviewed so that technology access no longer necessary can be disabled/revoked.

Filtering software is actively used to preclude access to inappropriate websites. Exemptions to web filtering may be granted if there is a requirement in the conduct of official City business.

Access to systems may be disabled by Information Technology Security staff if needed to contain a significant Cybersecurity Incident.

Access to city-managed technology systems from some international locations may be blocked via technical controls, to protect unauthorized information disclosure. When implemented, a list of blocked locations will be published.

3.2 Use Protective Measures and Precautions

Technology users shall:

- Protect login information, passwords, and MFA security codes
 - Personally assigned passwords should never be shared
 - MFA security codes should not be shared
- Recognize that remote access to systems requires MFA
- Recognize that Category 3 and Category 4 information may require extra data protection measures
- Recognize that access to computer rooms, data centers, wiring closets, and similar facilities is limited to authorized personnel based on business need. Access should not be granted to third parties except when escorted by authorized personnel.
- Take care to protect City assets – don't leave laptops and devices unattended in insecure locations
- Use caution in reviewing communications before clicking on links or responding to requests
 - Be cautious when opening e-mails, attachments, and text messages, especially those received from external or unfamiliar senders
 - Be cautious when unusual requests or information is included in an e-mail or a text message, even if from a familiar sender.

- Be aware that malicious messages often appear to come from a valid source and could attempt to make you disclose personal or sensitive information
- Use screen-lock or log out of technology assets when not in use
- Use “TacomaSecure” Wi-fi when connecting City-issued devices to the Internet while working onsite

3.3 Misuse of Technology

The following actions are prohibited:

- Attempts to gain unauthorized access to the City’s technology systems and services
- Attempts to bypass web filtering without authorization
- Installing, attaching, or plugging in unauthorized software or hardware
- Masking user’s identity or misrepresenting information and/or communicating as someone other than user, except as expressly allowed per Tacoma Police Department policy
- Unauthorized use of another employee/technology user’s user ID and password
- Use that interferes with the performance or operation of the City’s technology systems and services
- Use that exploits or attempts to exploit any vulnerability in any application or network security
- Any other use or attempt to bypass security controls including technical controls, policies, or standards without authorization

3.4 Cybersecurity Concerns Require Prompt Reporting

Some circumstances require prompt reporting so that the City can respond rapidly and submit mandated reports and notifications.

3.4.1 Lost/stolen Badge

Lost, misplaced, or stolen identification badges are to be reported to Public Works-Facilities or TPU Power-Facilities immediately. Technology users should also submit an online report to Risk Management.

3.4.2 Lost/stolen Device or Fraud Concern

Reporting for any of the following concerns should occur immediately:

- Lost/stolen device – mobile phones, tablets, or computers
- Potential fraud concern related to cash disbursements, compromised credit card or payroll information, or other potentially fraudulent activity

Notify IT Service Desk and Supervisor as soon as possible, and submit an online report to Risk Management, to ensure reporting occurs as required.

3.4.3 Suspected Cybersecurity Incident

Reporting for suspected Cybersecurity Incidents should occur immediately. Examples might include:

- Malware on computer, system, or mobile device,
- Threatening message demanding payment,
- Data that appears to be missing or changed or disclosed to an unauthorized third party,
- Unauthorized use of an account or system,
- System that appears to be behaving abnormally, or
- Any other circumstance that appears to represent a Cybersecurity Incident.

Technology users should:

- Gather factual information about the circumstance,

- Notify their supervisor and IT Service Desk.

3.5 Confidential Information and Devices Remain in United States

Category 3 and Category 4 information must remain in geographic locations governed by United States law.

Technology Users are strongly encouraged to ensure that City-owned technology assets remain in geographic locations governed by United States law, in order to protect these assets from theft and/or risk of unauthorized information disclosure.

- Technology Users should use extra caution when traveling to foreign countries with City-issued mobile devices, computers, and other technology.
- The IT Department shall develop and publish guidelines to provide appropriate recommendations and direction.

Ongoing Technology access occurring from outside of the United States, such as access by offshore contractors, shall be evaluated by the Chief Information Security Officer (CISO) during procurement decision processes or when such access is proposed. Access may or may not be granted and may require additional technical controls to protect City information and resources.

4.0 No Expectation of Privacy

Technology users shall have no expectation of privacy in their use of City technology provided in the course of employment or use of City systems, and all such use may and will be monitored or audited at any time without notice.

The City owns all data and content stored on its information systems.

All data stored on the City's information systems is subject to public disclosure and the rules of discovery in the event of litigation.

The City reserves the right to inspect logs, records and statistics regarding City technology usage to ensure the security and integrity of the technology resources, to investigate performance deviations and system problems, to determine if an individual is in compliance with this policy, or to ensure that City of Tacoma complies with applicable laws. Should it be discovered that data suggests that an employee has violated this policy, then such concerns shall be raised with the employee in an appropriate timeframe

5.0 Technology Use Responsibilities

5.1 Employee/Technology User Responsibilities

- **Be familiar with and understand** this policy and other City of Tacoma policies or guidance that apply to appropriate use of the City's technology
- **Protect** City equipment and data.
- **Complete** required training related to security awareness, technology use, and/or handling of Category 3 and Category 4 information.
- **Return** badges and all issued devices at end of employment.

5.2 Management/Supervisor Responsibilities

- **Communicate** this policy and ensure all employees receive appropriate training on it at onboarding and at least once annually
- **Provide** more specific direction and/or expectations regarding use of technology to employees as appropriate for the department
- **Ensure** badge and issued devices are accounted for when employees separate from employment
- **Submit** offboarding documents and/or access change requests promptly so that technology access can be properly disabled when employees leave the City or transfer to another role within the City
- **Submit** policy exception requests for employees to Chief Information Security Officer by submitting an IT Service Desk ticket

5.3 Department Responsibilities

- **Designate** employees who have authority to authorize accounts and access to technology resources
- If, in the course of normal business activities, department management suspects an employee is violating this Policy, they will **report** the suspected infractions to Human Resources.
- Departments are responsible for **carrying out** any disciplinary actions in response to Technology Use Policy violations.
- **Ensure** employees complete annual training related to Security Awareness and this policy

5.4 Information Technology Department (ITD)

- **Approve** all devices connecting to the City's network
- **Recommend** Technology-related policies, standards, and guidelines that are enforceable
- **Perform enterprise monitoring** of Information technology resources using security and monitoring tools. Security and monitoring information will be provided to Human Resources or the department as requested to support the investigation of policy violations.

5.5 Human Resources Department Responsibilities

- **Integrate** this policy into new hire training, orientation, and ongoing training of City work rules and policies
- **Evaluate** reported infractions of this policy and may request additional monitoring information from ITD as part of their investigation and evaluation process

5.6 Chief Information Security Officer (CISO) Responsibilities

- **Consult** with departments and Information Asset Owners regarding safeguarding and security controls in accordance with City standards, Regulatory requirements, and Risk Assessment results.
- **Review** and **grant or deny** requested security-related exceptions based on a risk assessment process.
 - **Refer** exception challenges or complex requests to Technology Risk Advisory Board (TRAB) consistent with Enterprise Information Security Policy #4.50.

- **Identify, monitor, and/or initiate** breach notifications that may be required by Federal or State laws and regulations, contractual obligations, or other agreements.
- **Submits** reports to risk management, as soon as Cybersecurity Incidents are confirmed

6.0 Policy Compliance and Exceptions

Employees found to be in violation of this policy may be subject to disciplinary action up to and including termination.

Exceptions to this policy related to Security provisions (Section 3.0) or other exception requests related to technical systems use must be expressly authorized by the Chief Information Security Officer.

Department/Division Managers request exceptions related to Security provisions by submitting an IT Service Desk ticket.

Appendix A: References

City of Tacoma/Tacoma Public Utilities

Policies and Guidelines – See Section 1.6

Tacoma Municipal Code – [Code of Ethics, Chapter 1.46](#)

Washington State



Public Records Act - [RCW.42.56](#)

Preservation and Destruction of Public Records – [RCW.40.14](#)

Appendix B: Relevant Compliance Requirements

Compliance Standard	Section(s)	Description
CIS Controls v8.0	6.1, 6.2, 6.4 14.1-14.6	Access Control Management Security Awareness Training Program
CJIS Policy 5.9.2	5.2 AT-2(a)(1)	Provide training as part of initial training for new users
HIPAA	164.308(a)(5)	Administrative Safeguards, Security Awareness and Training Standard
NIST CSF v1.1	PR.AT-1 PR.AT-4 PR.AC-1 PR.AC-2 PR.AC-4 PR.AC-7	Awareness and Training – All users informed and trained Senior executives understand roles and responsibilities Identities and credentials are issued, managed, and audited Physical access to assets is managed and protected Access permissions and authorizations are managed Users, devices, credentials authenticated commensurate with risk of the transaction
PCI DSS v3.2.1	12.3.5 12.6.1	Acceptable uses of the Technology Educate personnel upon hire and at least annually

Version History and Approvals

Contact Info:	Paul Federighi, Chief Information Security Officer Information Technology Department Phone 253-382-2606 E-mail pfederig@cityoftacoma.org
Policy History:	E-mail Retention Policy and Internet and Electronic Communications Use Policies, consolidated and superseded Policy 4.1 Information Systems Resource Usage, effective 7/01/2010, rescinded/replaced Policy 4.1 Technology Acceptable Use, effective 03/01/2024
Approval:	Elizabeth Pauli, City Manager <small>DocuSigned by:</small>  12/18/2023 <small>04DC6935E7F348B</small>
Effective Date:	Jackie Flowers, Director of Utilities <small>DocuSigned by:</small>  12/13/2023 <small>BD8D15F89A9447B...</small>