Document Code No.: ITG-P-21-01
Title: King County Acceptable Use Policy
Affected Agencies: Countywide
Authorities: King County Code Title 2A.380
Keywords: Acceptable Use Policy, AUP
Sponsoring Agency: Department of Information Technology

Chief Information Officer Signature: DocuSigned by: 920AF9FCB611460...
Date signed and effective: 2/16/2021

King County

I. Purpose:

The purpose of this policy is to describe the acceptable use of King County's technology assets (e.g., hardware, software, data, and authentication information) by King County workforce members. Acceptable use of technology assets is essential to ensure King County meets its regulatory requirements and maintains the confidentiality, integrity, and availability of technology assets used to provide public services. This policy reflects King County's pro equity and social justice commitment. Implementation of this information security policy aligns and complies, in every regard, with King County's equity and social justice policies and practices.

II. Applicability and Audience

A. Users

This policy applies to all persons working for, or on behalf of King County, including workforce members, third parties, volunteers, and contractors accessing technology assets owned and operated by King County. These requirements apply whether the user is working at a King County facility or connecting remotely. This policy does not apply to members of the public or workforce members while acting as a member of the public (e.g., while visiting www.kingcounty.gov to make a payment, look for information, or search for employment opportunities).

B. Technology Assets

This policy applies to the use of all King County technology assets including web or "cloud" based platforms, applications, and services that are owned and operated by a service provider on behalf of King County. This policy also applies to the use of third party or personal devices, if used to access King County's technology assets in the process of working for or on behalf of King County.

C. Exceptions

Requests for exceptions to this policy must follow the Department of Information Technology (KCIT) information security policy exceptions handling process. Please open a ticket with the helpdesk to request a policy exception.

III. Definitions

All definitions are contained within the King County Information Security Policy and Standards Glossary.

IV. Policy

A. System Use Notification

King County technology assets will display a system use notification where possible, prior to logging in, that states King County's ownership of the asset and that the asset is covered by King County policies and applicable law (e.g., logging into computers or servers, applications including web based or Software as a Service applications, or other equipment such as network and telecommunications equipment).

B. Acceptable Use Behavior

King County must protect the confidentiality (authorized access to systems and information), integrity (authorized modification of systems and information), and availability (making sure systems and information are available when needed) of all technology assets supporting King County's services. When engaged in the performance of your role with King County:

1. Attempts to disable or circumvent any King County security controls, policies, or procedures (e.g., disabling virus protection or installing unauthorized software) is prohibited. This includes, but is not limited to:
    a. Use of tools that compromise security (e.g., password crackers, network sniffers, attack frameworks and software distributions , proxies, unauthorized VPN clients, or other tunneling technology), except as authorized by the Chief Information Security and Privacy Officer
    b. Attempts to disable, defeat, or circumvent any King County information security components
    c. Intentional or careless interference with the normal operation of King County technology assets
2. Use that violates King County policy or local, state, and/or federal laws is strictly prohibited. This includes, but is not limited to:
    a. Theft of King County technology assets, including sensitive data
    b. Use of King County systems for any type of harassment, which includes using any words or phrases that may be construed as derogatory based on race, color, sex, age, creed, disability, marital status, national origin, religion, pregnancy, gender, gender identity or expression, genetic information, sexual orientation, veteran or military status, use of a service animal, or any other status protected by federal, state and local law
3. Unauthorized use, destruction, modification, or distribution of King County external and internal systems, applications, and data is prohibited. This includes, but is not limited to:
    a. Release or disclosure of King County data to unauthorized parties inconsistent with federal, state, and local law (e.g., HIPAA, Chapter 42.56 RCW, KCC 2.14),

King County policies, or inconsistent with your assigned job role and responsibilities

b. Attempts to modify administrative settings and configurations or repair hardware and software. Such modifications, configurations and repairs shall only be performed by authorized technology support personnel for your department or agency. This excludes basic troubleshooting such as closing and restarting an application or a restart/reboot of a single workstation. Modification, configuration and repairs of enterprise information technology equipment and networking infrastructure shall only be performed by authorized support personnel in the Department of Information Technology (KCIT).

c. Removal of technology assets from King County premises without prior approval by authorized technology support personnel for your department or agency is prohibited. This excludes technology issued directly to you for employment purposes approved for taking home or from King County premises by your supervisor, human resources personnel, or the Department of Information Technology (KCIT).

4. Use of personal devices including computers, network devices, or any other personal equipment to make a direct network connection (wired or wireless) to King County internal private networks within King County facilities is prohibited.

5. Personal devices such as mobile phones and tablets may be used to access King County technology such as email, calendar, and unified communications and for purposes of multi-factor authentication. Personal devices must utilize apps (mobile applications and/or software) authorized by the Department of Information Technology (KCIT). Personal devices may be denied access if insecure configurations are detected (e.g., a jailbroken phone, or a phone that does not use a password/PIN). King County reserves the right to require personal mobile devices or mobile apps to be managed by a mobile device or mobile app management solution to protect King County technology and data.

6. Use of information systems to solicit for commercial ventures, religious or political causes, or for personal gain unrelated to the processes of working for or on behalf of King County is prohibited unless explicitly allowed by King County policy or federal, state, or local law.

7. King County's assets must never be left unattended in an unsecured location (e.g., at the airport, or in a coffee shop). A secured location can be a locked vehicle (out of sight if possible), your home (secured from use by family members and guests), or within designated areas in King County facilities such as an assigned cubicle or equipment storage location. Please review King County telecommuting policies and guidance for further information regarding secured location requirements when telecommuting.

8. When working remotely or in a King County facility, workforce members must lock or log out of King County technology assets like laptops when not in use to prevent an

unauthorized individual from obtaining data or information. When working with regulated data, workforce members must take additional precautions (e.g., positioning the equipment so the screen cannot easily be viewed or using a screen protector) to prevent others from being able to view the information on the screen while in use. When regulated data is being communicated through phone calls or spoken aloud, workforce members must take precautions (e.g., closing a door, asking people to step out for a few moments, using a headphone, speaking softly, or finding an alternative way to communicate the information) to prevent access by unauthorized parties.

9. Lost or stolen King County technology assets must be reported immediately by opening a ticket with the helpdesk. Your department or agency may have additional procedures for lost or stolen assets. Please speak with your supervisor to determine what these additional procedures may be.
10. Upon termination of any King County workforce member, including a third party or contractor, all King County technology assets must be returned to King County.
11. Hardware and software must be procured in accordance with King County procurement policies, in compliance with Department of Information Technology (KCIT) policies and standards, and properly licensed and registered in the name of King County.

C. Personal Use

King County technology assets are purposed for conducting the business of King County. Occasional personal use of technology equipment issued to workforce members is permitted (e.g., phones and/or unified communication systems, workstations and peripherals like keyboards, monitors, mice, printers, copiers, and fax machines) if the use:

1. Does not introduce additional financial costs to King County;
2. Does not interfere with your assigned job duties;
3. Does not preempt or interfere with King County service delivery; and,
4. Does not otherwise violate King County, departmental, or agency policies.

Information created, processed, sent, received, or stored during personal use of King County technology assets will not be handled differently by King County. Such information may be subject to King County policies, and federal, state and local laws including Chapter 42.56 RCW (Public Records Act). Personal files should not be permanently stored on King County technology assets. King County is not responsible for backing up or recovering personal data.

D. Acceptable Use of the Internet

You are representing King County when using King County's technology to access the internet, and some types of activities on the internet can pose a security risk to King County's technology assets. You are responsible for ensuring that your use of the internet is appropriate, ethical, lawful, and within the scope of your employment at King County.

1. King County reserves the right to block access to internet web sites and addresses, including malicious internet web sites or internet addresses unrelated to King County's business.
    a. Blocked websites may include possibly malicious or hacked websites, websites that contain inappropriate or offensive content, or websites provided from geographic locations known to be hostile to the United States. These websites could lead to disclosure of non-public information.
    b. You may submit a ticket to the helpdesk to unblock websites for legitimate business usage.
2. King County may restrict internet use to reserve bandwidth and resources for critical King County services during an emergency or severe internet service impact regardless of the legitimacy of the content.
3. King County may monitor and log the use of the internet by technology assets connected to King County operated networks to comply with various laws, legal proceedings, or internal policy, to troubleshoot and support technology, or to monitor and investigate unauthorized activity. This includes, but is not limited to:
    a. Use of monitoring tools installed locally on a workstation;
    b. Analysis of various logs generated by the user or system activity (such as proxy servers, network devices, authentication and directory servers, intrusion prevention/detection devices, firewalls, web/file servers, and other systems as necessary); and,
    c. Traffic analysis on inbound or outbound network traffic, including the interception, decryption, and inspection of encrypted traffic.
4. While using King County technology assets you must not:
    a. Use the internet for any unlawful activity or for personal gain
    b. Reproduce, distribute, or display copyrighted materials without prior permission of the copyright owner. This includes text, images, photographs, music files, sound effects, and other legally protected works.
    c. Represent personal opinions as those of King County, such as in social media, blogs, or forums
    d. Perform any activities that may harm the reputation of King County operations or staff with controversial issues (e.g., sexually explicit materials). This does not refer to appropriate and legal activities (e.g., activities by collective bargaining

units, or use of King County public or personnel feedback or complaint processes) regarding the delivery of King County services.

e. Perform any activities that violate King County's Code of Ethics as defined in Title 3.04 of King County Code

f. Use your King County password or email address as the account information for any personal accounts used to access internet services, websites, social media (e.g., LinkedIn). You must use separate credentials and your personal email address for those activities. You may use your King County email address as a username when creating an account related to your employment responsibilities at King County.

E. Acceptable Use of Electronic Messages

Malicious individuals often use email when trying to acquire King County customer data, non-public information and data, or to compromise King County's technology assets. You are required to use King County messaging applications (e.g., email, instant message, text messaging, etc.) in the following professional manner:

1. Not all workforce members are authorized to access the same data. Accounts are issued solely for the use of the individual to whom the account has been assigned. Sharing individual account information may lead to unintentional disclosure of data and is prohibited.

    a. Shared mailboxes where an authorized workgroup can monitor emails sent to and from the shared mailbox is allowed

    b. Administrative delegation of access to an individual email account is acceptable (e.g., an executive or administrative assistant or a peer), as long as this is accomplished through the email system's delegation functionality and not by sharing credentials.

2. If you have doubts or serious concerns about the origin or authenticity of an electronic message, or if you receive a highly abnormal or suspicious message, you should report the message by submitting a ticket to the helpdesk or by use of the messaging systems integrated reporting mechanism (e.g., a phishing button in email clients). Your department or agency may have additional reporting requirements so check with your supervisor.

3. Use caution when opening emails and attachments, particularly those received from an external sender.

    a. Don't open any attached files or click on hyperlinks to download files containing macros, scripts, or executables from an unknown or suspicious source.

    b. Malicious messages often appear to come from a valid source and could attempt to make you disclose personal or sensitive information. Use caution when opening attached files or clicking on hyperlinks, or when unusual requests or information is included in the email even if from a familiar sender.

c. Training will be provided on detecting malicious emails to all King County workforce members. Additional training may be required if there is repeated susceptibility to malicious emails by individuals.

4. Do not forward King County email containing confidential, sensitive or regulated data to personal email accounts.
5. Automatic forwarding of email through the use of rules to any external domain (non kingcounty.gov or other King County owned and operated domains) requires approval by the Department of Information Technology (KCIT) and can be requested by opening a ticket with the helpdesk.
6. Do not send fictitious or forged messages that could be mistaken for official King County statements, marketing, or materials.
7. Do not send junk mail or chain letters.
8. Do not use profanity, inappropriate language, pornography or sexually explicit material, slanderous, discriminatory language, harassment, or misleading contents.
9. Do not use King County messaging applications to send unprofessional, threatening, libelous, or derogatory messages.

F. Acceptable Use of Voice Communications Systems

King County's phone and communication systems are provided to facilitate business activities. Similar to internet browsing and other computing activities, phone call information and metadata (e.g. Caller ID, Date and Time of Call, Call Duration) may be monitored and logged.

1. If the call will be recorded, you must notify all call participants that the call will be monitored or recorded, including the purpose of recording at the outset of the recording and include the notification in the recording. This does not apply to lawful monitoring or recording that does not require consent in accordance with federal, state, or local law (e.g., RCW 9.73.030). Voicemail or other automated telephony system recordings comply with this section if the recorded greeting clearly indicates that the caller has reached a voicemail system or is about to be recorded.
2. Call recordings containing sensitive or regulated data presents serious security and compliance risk and should be avoided. Departments or agencies that will purposefully and continuously record sensitive or regulated data such as payment card data or protected health information must notify the Chief Information Security and Privacy Officer unless explicitly authorized in federal, state, or local law (e.g., calls to 911).

G. Acceptable Use of Wireless Networks

Not all wireless networks are configured with strong security protections. In addition, unauthorized and malicious wireless devices may pose a risk to King County technology assets. While performing your role at King County:

1. Direct connections (i.e., directly connected to internal wireless access points or physical network infrastructure like a data jack in a wall plate or a network switch port) to King County's protected internal private wired and wireless network is provided only to King County workforce members using King County owned and operated technology assets. Third parties, vendors, contractors, and other non-King County personnel access to King County's protected internal private wireless or wired network is prohibited without prior approval by the Department of Information Technology (KCIT) who may employ security measures to prevent unauthorized network connectivity. If an exception is required for a legitimate business need please open a ticket with the helpdesk.
2. Third-party internet access (such as access provided at airports, hotels, and coffee shops) carry potential security risks to King County technology assets. Special care should be taken to ensure you are connecting to the correct network and not bypassing any security alerts and warnings.
3. King County's wireless network infrastructure may only be altered and managed by authorized Department of Information Technology (KCIT) personnel.
4. You must not install, connect, or modify any wireless infrastructure such as Wireless Access Point (WAPs) to King County's network without explicit written authorization from the Department of Information Technology (KCIT).

H. Acceptable Use While Utilizing Remote Access Technology

Remote access to King County's applications is available for workforce members to work outside of the office or for telecommuting. While using remote access:

1. Ensure you do not type any remote access passwords while someone is watching.
2. Only store passwords in a password manager or browser configuration approved by the Department of Information Technology (KCIT).
3. Do not leave technology assets unattended and remotely logged on to King County's network. When not in use, store your equipment and media used to remotely access King County systems in a secured location.
4. Do not share passwords, smart cards, tokens, keys, fobs or any other access or authentication devices with any other person.
5. Vendors must be limited to the minimum amount of privilege and access required to perform the necessary duties while using remote access methods approved by the Department of Information Technology (KCIT).
    a. Remote support sessions must first be authorized by King County technology support personnel before the session is established and terminated as soon as the vendor has finished their work.
    b. No vendor may be given remote access that is not strictly controlled and monitored.

c. Vendors shall not be given permanent remote access to King County's network unless that access is strictly limited to the systems supported by the vendor and controls are in place to monitor their activities to ensure they are not able to gain additional access to other King County technology assets from the systems they are able to remotely access.

6. Remote access to technology assets that contain sensitive or regulated data requires multi-factor authentication and use of a secure connection between the host and the remote device.

   a. You must not use remote access products like TeamViewer, GoToMyPC, or similar products unless approved by the Department of Information Technology (KCIT).

   b. Do not use unsecured public or private wireless networks. Do not bypass warnings that indicate the wireless network is not secure.

I. Acceptable Use of Social Media

1. You must exercise judgment and use caution when interacting online. It is important to remember that in an online environment, the lines between public and private, and personal and professional, are not always clear. When you identify yourself as a King County workforce member, employee or affiliate on social media, a perception is created about you as a representative of King County, your expertise, King County customers, and King County itself.
2. Creation and use of a social media account on behalf of King County must be done in compliance with King County social media policies.

J. No Expectation of Privacy

1. King County must monitor all systems and users of technology assets in order to maintain a secure environment and meet compliance requirements. You should have no expectation of privacy or confidentiality while using King County technology assets, including internet access and emails. Usage may be monitored for policy, security, or network management reasons and is subject to inspection at any time. Inspection and monitoring of King County technology assets by management does not require the consent of individual workforce members.
2. All electronic messages or data created, stored, transmitted, or received over King County systems or through King County internet connections are subject to inspection or monitoring. King County reserves the right to store and/or access the contents of any messages or data sent over its networks and use that information to enforce its policies or comply with federal, state, or local law. If the content violates regulations or laws, King County reserves the right to submit the information to law enforcement for potential prosecution.

K. Reporting Known or Suspected Vulnerabilities or Security Incidents

You must report known or suspected security weaknesses, instances of inappropriate access, and suspicious activities to the Department of Information Technology (KCIT) by opening a ticket with the helpdesk. Your department or agency may also have reporting requirements so please check with your supervisor.

1. You will be responsible for the confidentiality, integrity, and availability of your files. If concerning circumstances occur with your files such as inappropriate access, loss of the files, or changes are made to files without your consent please speak with your supervisor and report this issue by opening a ticket with the helpdesk.
2. You must report suspicious activities happening to or on your workstation such as someone remote controlling the workstation without your consent or new and unfamiliar software performing unusual activities by opening a ticket with the helpdesk.

V. Implementation Plan

This policy becomes effective for countywide use on the date that it is signed by Chief Information Officer. All new technology implementations and new material changes to existing technology implementations must ensure compliance with this policy as of the effective date. All other technology implementations must be brought into compliance within four years after the effective date.

VI. Maintenance

A. This policy will be maintained by the Department of Information Technology (KCIT), Office of the CIO, or its successor agency. This includes, but may not be limited to:
1. Interpretation of this policy
2. Ensuring this policy content is kept current
3. Recommending updates to this policy and related resources
4. Developing an escalation and mitigation process if an Organization is not in compliance
5. Assisting Organizations to understand how to comply with this policy
6. Monitoring annual compliance by Organizations

B. This policy will automatically expire five (5) years after its effective date. A new, revised, or renewed policy will be initiated by the Office of the CIO, or its successor agency prior to the expiration date.

VII. Consequences for Noncompliance

Violations of this policy may be grounds for disciplinary action, up to and including termination and enforcement action which may include civil or criminal charges.

VIII. Appendix A: References

- 45 CFR Part 164 (HIPAA)
- Chapter 42.56 RCW
- Chapter 9.73.030 RCW
- Title 3.04 King County Code (Employee Code of Ethics)

- Title 2.14 King County Code (Public Access To Electronic Records And Information)

IX. Appendix B: Relevant Compliance Requirements

This section provides references to key regulations and standards that apply to King County. This section does not replace the authoritative source and is just a reference to assist with further research. Please use the Compliance Standard and Section No. to further research the entirety of the regulation, framework or standard from the authoritative source.

Compliance Standard	Section No.	Description
HIPAA	45 CFR 164 Subpart C	Security Standards for the Protection of Electronic Protected Health Information
	45 CFR 164.316	Policies and procedures and documentation requirements.
CJIS Security Policy v5.9	5.2.1	Basic Security Awareness Training
PCI DSS v3.2	12.3.5	Acceptable Uses of the Technology
NIST CSF	PR.AT	Awareness and Training
	PR.IP	Information Protection Processes and Procedures
NIST 800-53r5	AC-8	System Use Notification
	AT-1	Policies and Procedures
	PL-4	Rules of Behavior
	PS-6	Access Agreements
CIS Controls v7.1	17	Implement a Security Awareness Training Program