Document Code No.: ITG-P-21-10
Title: King County Network Security Policy
Affected Agencies: Countywide
Authorities: King County Code Title 2A.380
Keywords: Network Security, Networking, Wireless, Wi-Fi, WiFi, WAN, LAN
Sponsoring Agency: Department of Information Technology (KCIT)

King County

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

I. Purpose:

The purpose of this policy is to define requirements for securing King County's network infrastructure. 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 workforce members responsible for technology asset ownership and support as well as any workforce members involved in purchasing, procuring, creating, or developing technology assets on behalf of King County.

B. Technology Assets

1. This policy applies to all of King County owned and operated network infrastructure, which includes, but is not limited to, the following:
    a. King County's office, branch office, and facility local-area networks (LAN)
    b. King County's data center networks
    c. King County cloud providers and virtual networks
    d. Internet connections installed at King County locations or through cloud platforms
    e. Mobile Device connections to King County's networks
    f. Wireless infrastructure, access points and security controllers
    g. Wide-area networks (WAN)
    h. Inter-Data Center network transports, leased circuits, and other telecommunications infrastructure
2. Institutional networks owned or leased by King County or its service providers for purposes of providing network services to third parties (e.g., cities, school districts, etc.) are in scope up to the demarcation point where King County equipment transitions to customer premise equipment. Customer premise equipment (e.g., network and server infrastructure, other technology assets) is not in scope of this policy.

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

King County's network infrastructure must be designed, implemented, and operated using methods that adequately protect King County technology assets.

A. Network Administration

1. The Department of Information Technology (KCIT) is responsible for the management and administration of the King County network infrastructure lifecycle including procurement, implementation, and decommissioning. King County operates a shared network infrastructure environment and must centralize these changes to ensure no department, division, or agency is able to introduce risk without centralized management and visibility.
2. Access to perform administrative changes to network infrastructure shall be granted in compliance with the Access Management Policy.
3. The Department of Information Technology (KCIT) must apply security patches and updates to network infrastructure equipment in compliance with the Vulnerability Management Policy.

B. Network Documentation and Change Management

1. The Department of Information Technology (KCIT) must review and validate documentation of King County's network infrastructure (e.g., physical, wireless, cloud, virtual) to identify and correct any deviation between documentation and what has been implemented at least annually. The items reviewed must include:
    a. Asset Inventory in accordance with the Asset Management Policy
    b. Network Diagrams, which must be comprehensive such that in a disaster recovery or business continuity scenario the loss of institutional knowledge and key personnel would not significantly hinder a third party consultant or vendor or other workforce members from re-establishing network services and operations
    c. Confirmation that configuration backups of all network infrastructure configurations and documentation are occurring at least once every 24 hours
    d. Administrative system accounts are documented and secured according to identity asset requirements within the Asset Management Policy

e. Physical access components such as keys, access cards, door lock codes, etc. that secure physical access to network infrastructure locations (e.g., wiring closets, server rooms, data centers, telco facilities, etc.) are documented, secured, and accessible by the Department of Information Technology (KCIT) senior leadership staff for business continuity purposes. Access and use (i.e., retrieval or checkout of a key and subsequent use to open a door by a specific individual) must be logged for auditing purposes.

f. Physical access codes are being changed regularly and when workforce members with knowledge of the codes are no longer authorized for access (e.g., job change, no longer employed by King County)

g. An audit of workforce members who have administrative access to network infrastructure equipment to ensure access is maintained in accordance with the Access Management Policy

h. Access to network infrastructure documentation is secured in accordance with the Information Classification Policy and Data Security Policy

2. Changes to King County's network infrastructure must utilize the Department of Information Technology (KCIT) change management process to ensure that changes will not adversely impact compliance with this policy.

C. Network Connections

1. Network infrastructure (e.g., physical, wireless, cloud, virtual) should be configured in a "deny all by default" configuration. Only approved and authorized ports, protocols, and connections (e.g., IP addresses, serial, etc.) should be allowed as defined in the Network Security Standard.

2. Access to network infrastructure shall be logged and monitored in accordance with the Audit Logging and Monitoring Standards.

3. Internet connections between the public internet and King County's private network create opportunities for possible attacks and as well as provide access to the general public.

   a. Internet connections to King County's private network must be procured, installed, managed, and decommissioned by the Department of Information Technology (KCIT) and must have security controls in place.

   b. Inbound and outbound access between the public internet and King County's private network infrastructure must be restricted to the ports and protocols necessary to meet business requirements.

   c. Technology assets that are configured to be accessible from the internet are at greater risk and require the minimum following network security controls:

      i. Stateful packet inspection to ensure only authorized ports and protocols are accessible

ii. Intrusion detection and prevention controls (e.g., web app firewall, IDS/IPS proxy)

iii. Session controls for periods of inactivity, max sessions per source/destination, and incomplete or anomalous session establishment or behavior

iv. Audit logging in accordance with the Audit Logging & Monitoring Policy

d. It is often necessary to configure development and test environments to be accessible from the internet for the purposes of validation and testing. Development and test environments typically have not received the same rigorous review and preparation as a production environment. Development and test environments may be configured to be accessible from the internet only if:

i. There is no production data in the environment and the environment is segmented from other production environments; or

ii. The development or test environment has received all the same protections as a production environment with the same requirements

4. Network traffic or packets destined to or sourced from King County facilities and network infrastructure and the internet or other external networks may be intercepted by King County security tools at King County network gateways and egress or demarcation points for the purposes of decryption and inspection for malicious activity, content filtering, enforcement of the Acceptable Use Policy, bandwidth preservation or control, security incident response, or network performance and operations troubleshooting.

5. Non-King County infrastructure equipment that has not been approved by the Department of Information Technology (KCIT) is not allowed to be connected to King County's networks. All wireless and cellular network infrastructure including wireless access points and controllers (on premise or cloud based) must be procured, installed, managed, and decommissioned by the Department of Information Technology (KCIT). This excludes devices such as a cellular phone or "hot spot" device intended to provide a cellular wireless internet connection to a single user.

6. Non-King County infrastructure equipment that has not been approved by the Department of Information Technology (KCIT) is not allowed to be connected to King County's networks. All wired network infrastructure including routers, switches, converters, aggregation and tap equipment, controllers (on premise or cloud based) must be procured, installed, managed, and decommissioned by Department of Information Technology (KCIT).

7. All virtual network infrastructure both on premise in King County facilities as well as virtual network infrastructure provided through cloud service providers to King County must be procured, configured, managed, and decommissioned by the Department of Information Technology (KCIT).

D. Firewalls, Security Tools and Appliances, Security Features and Functionality

All firewalls and network based security tools and appliances, security features and functionality deployed on King County's networks must be installed and maintained by the Department of Information Technology (KCIT). A consistent security posture across King County is required. One department or agency can affect all other departments and agencies. The Department of Information Technology (KCIT) will ensure that:

1. Firewalls are located at each internet connection and between any Demilitarized Zone (DMZ) and the internal network.
2. Internet-facing systems are reviewed to determine whether placement in a DMZ is appropriate in accordance with the Network Security Standard.
3. Security platforms, appliances, and tools may utilize routable public IP address space on external interfaces to intercept, inspect, and forward traffic to technology assets on King County's DMZ and private network segments.
4. Technology assets in King County DMZ or private network segments must use non-routable private IP address space as defined in RFC 1918 and 4193. Network Address Translation by a security platform, appliance, or tool can be used to enable publicly routable network traffic.
5. Network connections external to network infrastructure owned and operated by King County must terminate in a DMZ.
6. Firewalls perform stateful packet inspection and limit traffic to only that which is necessary for business operations.
7. Firewall traffic is logged and retained in accordance with the Audit Logging and Monitoring Policy.
8. Network based security tools and appliances, security features, and functionality are applied across all King County network infrastructure such that no one department or agency is introducing additional risk to another department or agency.

E. Host Based Firewalls

Firewall software or functionality must be installed or enabled on King County workstations and servers (virtual or physical) to ensure network traffic is limited to that which is necessary for business operations.

1. Host based firewalls must be configured as part of the provisioning process.
2. Users must be prevented from disabling the firewall or altering configurations in any way.
3. The firewall should only allow authorized network communications.

F. Virtual Private Networks (VPN)

A virtual private network or VPN can enable network connectivity similar to being directly connected to King County's private enterprise networks within a King County facility from

other locations such as a workforce member's home network, a Wi-Fi hotspot, or a remote site or facility with an internet connection. When establishing VPN connections:

1. King County Workforce Members
    a. Must have approval through King County's telecommuting policies and processes
    b. Must establish the need for a VPN to complete job role. If applications and data can be accessed without a VPN connection then VPN access will not be provided.
    c. King County may assess and/or enforce the following conditions and security requirements prior to allowing VPN connections:
        i. Up to date endpoint protection signatures (anti-virus/anti-malware)
        ii. Host based firewall
        iii. Split Tunneling settings
        iv. King County user account is not disabled
        v. King County user account is authorized to login at the current time
        vi. Multi-factor Authentication (MFA) is enabled for the user account
        vii. VPN access only to authorized network segments
        viii. Operating system is still supported by the manufacturer
        ix. VPN sessions are disconnected after 30 minutes of inactivity
        x. Maximum VPN session of 12 hours
2. Consultants, Vendors, and Technology Service Providers
    a. VPN access, site to site or user account based, for consultants, vendors, and technology service providers for support purposes is prohibited. The Department of Information Technology (KCIT) is responsible for providing a controlled vendor and third party remote access management solution that:
        i. Allows vendors to access only the systems they have been authorized to access
        ii. Requires approval prior to establishing a connection each time
        iii. Logs all connection information and actions taken by the vendor
        iv. Automatically disconnects after a maximum session time of 12 hours
    b. Access to King County technology assets by consultants, vendors, and technology service providers must be in compliance with the Access Management Policy.

3. Partners and Service Providers of King County Services
    a. VPN access for King County partners and service providers, entities that are also public institutions or legal or contractual extensions of King County in order to provide public services, is prohibited unless the technology assets in use by the partner or service provider are controlled and managed by King County.
    b. Access to King County technology assets can be securely provided in a targeted and limited fashion as oppose to utilizing virtual private network connections. The Department of Information Technology (KCIT) will provide alternative options for access to King County technology assets for authorized partners and service providers. These alternative methods may include temporary screen sharing by authorized technology support staff, application proxies, cloud based applications, and bastion hosts. These alternative methods must only allow access to technology assets for which the partner or service provider needs to provide King County the contracted or intended service.
4. Site to Site Virtual Private Networks configured for King County owned and operated facilities are allowed and must be configured in compliance with the Network Security Standard.

G. Network Segmentation

The Department of Information Technology (KCIT) must utilize network segmentation requirements in its design and implementation of King County network infrastructure including:

1. Establishment of network segments that limit network access to authorized users, network connections, applications, and data within administrative boundaries established in King County Code (e.g., separate branches of government, departments, criminal justice agencies, etc.) or established by Department and Agency Directors or Presiding Judge
2. Establishment of network segments that limit network access to authorized users, network connections, applications, and data according to federal and state regulations (e.g., HIPAA, CJIS Security Policy)
3. Establishment of network segments that limit network access to authorized users, network connections, applications, and data according to industry standards that have the authority to deny services critical to King County such as financial merchant services (e.g., PCI DSS)
4. Establishment of network segments that allow King County workforce members responsible for network administration to disable a compromised network segment to prevent further disruption or adverse effects to other network segments
5. Establishment of network segments for software development lifecycle segmentation between non-production and production environments

6. Establishment of network segments for Voice over Internet Protocol (VoIP) network traffic from network segments containing unencrypted criminal justice information (CJI)
7. Establishment of network segments for critical infrastructure environments as defined by the Department of Homeland Security (e.g., Water Utility, Public Utility, Transportation, Emergency Services)
8. Establishment of network segments that protect access to highly sensitive technology assets in accordance with special handling requirements defined by Technology Asset owners.

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

- Network Device Configuration Standard
- Acceptable Use Policy
- Vulnerability Management Policy
- Identification and Authentication Policy
- Access Management Policy
- Audit Logging Standard
- Monitoring Standard

- Data Encryption Standard
- Information Security Policy and Standards Glossary

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
	164.312(e)	Transmission Security
CJIS Policy v5.9	5.5.6	Remote Access
	5.7.1.2	Network Diagram
	5.10.1	Information Flow Enforcement
	5.10.3	Partitioning and Virtualization
	5.13.1	Wireless Communications Technologies
	5.13.4.3	Personal Firewall
PCI DSS v3.2.1	1	Install and maintain a firewall configuration to protect cardholder data
	4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: Only trusted keys and certificates are accepted. The protocol in use only supports secure versions or configurations. The encryption strength is appropriate for the encryption methodology in use.
	4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data

		environment, use industry best practices to implement strong encryption for authentication and transmission.
	6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any change. Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.
	11.1	Implement processes to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.
	11.4	Use intrusion-detection or intrusion-prevention techniques to detect or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.
	12.3.6	Acceptable network locations for the technologies
NIST CSF	ID.AM-3	Organizational Communication and Data Flows are Mapped
	PR.AC-3	Remote Access is Managed
	PR.AC-5	Network Integrity is Protected (e.g., network segregation, network segmentation)

	PR.PT-4	Communications and Control Networks are Protected
	DE.AE-1	A Baseline of Network Operations and Expected Data Flows for Users and Systems is Established and Managed
	DE.CM-1	The Network is Monitored to Detect Potential Cybersecurity Events
NIST 800-53r5	AC-4	Information Flow Enforcement
	AC-6(3)	Network Access to Privileged Commands
	AC-17	Remote Access
	AC-18	Wireless Access
	CP-8	Telecommunications Services
	CP-11	Alternate Communications Protocols
	SC-5	Denial of Service Protection
	SC-7	Boundary Protection
	SC-8	Transmission Confidentiality and Integrity
	SC-10	Network Disconnect
	SC-40	Wireless Link Protection
CIS Controls v7.1	9	Limitation of and Control of Network Ports, Protocols and Services
	12	Boundary Defense