Title: King County Cybersecurity Policies & Standards Glossary

King County

I. Common Definitions

Definitions are based on the NIST Cybersecurity Glossary, NIST Computer Security Resource Center Glossary, and National Cyber Security Centre Glossary.

Access – The ability and means necessary to store data in, retrieve data from, communicate with, or make use of any resource of a system owned by the company.

Access Control – The process of granting or denying specific requests to: (1) obtain and use information or related systems or services; or (2) enter specific physical facilities.

Administrator – A person who is responsible for managing a computer system or network.

Application – An executable program capable of performing a specialized function other than system maintenance (which is performed by utilities). Games, educational programs, and communications software are all examples, as are word processors, spreadsheets, and databases. Also called software.

Asset – Any technology asset within the King County environment that must be protected or used in a business process or task. There are four primary asset classes or groups: Hardware, Software, Data, and Identities. Examples include but are not limited to a file, network switch or router, database, social media credentials, software program or application, technology product, IT Infrastructure, industrial control system (ICS), Internet of Things (IoT) hardware, a network connected television or display device, furniture, software, personnel, unmanned aerial vehicle (UAV), mobile data computer or terminal (MDC/MDT).

Asset Valuation – Dollar value assigned to an asset–based on actual cost and non–monetary expenses. Include costs to develop, maintain, administer, advertise, support, repair, or replace an asset.

Attack – The exploitation of a vulnerability by a threat agent; any intentional attempt to exploit a vulnerability of King County's security infrastructure to cause damage, loss, or disclosure of assets.

Attacker – Malicious actor who seeks to exploit computer systems with the intent to change, destroy, steal or disable their information, and then exploit the outcome.

Attribute Based Access Control – An access control paradigm whereby access rights are granted to users through the use of policies which combine attributes together. The policies can use any type of attributes (user attributes, resource attributes, environment attribute etc.

Audit Log – An audit log is a record of events occurring within an organization's systems and networks. Logs are composed of log entries, and each entry contains specific information about the event that occurred within a system or network.

Authentication – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authentication Credentials – Information used to establish the validity of a claimed identity. Credentials typically include a username, ID, password or may include additional types of authentication factors such as something you know, something you have, and something you are. Every authenticator has one or more authentication factors.

Authorization – Access privileges granted to a user, program, or process or the act of granting those privileges.

Availability – Timely, reliable access to data, information, and systems by authorized users. (CIA Triad)

Backups – A copy of information, files, and programs to facilitate recovery. Backups may be stored on the same machine that contains the original information, another machine, a storage device such as a thumb drive, or "in the cloud."

Biometrics – Measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity, of an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics.

Blacklist – A list of discrete entities, such as hosts or applications that have been previously determined to be associated with malicious activity.

Business Continuity Plan (BCP) – Business Continuity Plan; the assessment of risks to organizational processes and the creation of policies, plans, and procedures to minimize the impact those risks might have on the organization if they were to occur.

Business Impact Analysis (BIA) – A systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident, or emergency.

Breach – The occurrence of a security mechanism being bypassed or thwarted by a threat agent. When a breach is combined with an attack, a penetration or intrusion can result.

Change Management – development, approval, and implementation tasks are separated between different individuals or groups so that no one person can develop a change and move it to production.

Computer Security Incident – A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples include user provides or exposes sensitive information through peer to peer file sharing services or an attacker obtains sensitive data that threatens the details will be released publicly if King County doesn't pay a sum of money.

Commercial Software Applications – Software services, applications and solutions that already exists and are available from commercial sources. It is also referred to as off-the-shelf or commercial-off-the-shelf, COTS.

Confidentiality – Assurance that information is not disclosed to unauthorized individuals, processes, or devices. (CIA Triad)

Critical Business Functions or Systems – Those information technology functions stated or implied, that organizations are required to perform by statute or executive order, or are otherwise necessary, to provide essential County business services.

Cybersecurity Breach – see cybersecurity incident.

Cybersecurity Incident – An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or that constitutes a violation or imminent threat of violating security policies, security procedures, or acceptable use policies.

Data – Distinct pieces of information, which can exist in various forms such as numbers, text, bit, bytes, or memory.

Data Asset – Any data that is created, stored, processed, transmitted, used, or observed by a King County system or by an individual working for or on behalf of King County. Data assets include any form (electronic, printed, website, voice record, email, CD, database, etc.) or location (in King County offices, personal residences, off–site, laptop computers, cellphones, etc.). A data asset also includes a service that may be provided to access data from an application.

Data at Rest – Describes data in persistent storage such as hard disks, removable media or backups.

Data Breach – An incident that involves sensitive, protected, or confidential information being copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so. Exposed information may include credit card numbers, personal health information, customer data, company trade secrets, or matters of national security, for example.

Data in Motion – Describes data moving over a communications channel (i.e., network, near field communication, Bluetooth, etc.).

Data Owner – Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Data Custodian – Data custodians are accountable for the technical control of data including security and privacy, scalability, configuration management, availability, accuracy, consistency, audit trail, backup and restore, compliance with standards and business rules.

Data in Use – Describes data in volatile memory (i.e., RAM, Cache, etc.).

Development Environment – The development environment (dev) is the environment in which changes to software are developed, most simply an individual developer's workstation. The developer's environment will include development tools like a compiler, integrated development environment, different or additional versions of libraries and support software, etc., which are not present in a user's environment.

Demilitarized Zone (DMZ) –An area which exists between the internet and internal network where publicly accessible services such as web servers or external email servers reside. Traffic from both the internet and internal network to the DMZ is filtered and controlled by a firewall.

Digital Forensics – The practice of gathering, retaining, and analyzing computer–related data for investigative purposes in a manner that maintains the integrity of the data.

Due Diligence – The expected duty of an individual to exercise care, responsibility, and prudence when evaluating a business decision that affects King County.

Emergency Change – Change type that is required for system functionality or business activity and is very time–sensitive.

Employee Information – Personal Information about King County employees.

Encryption – The transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state.

ePHI – Electronic protected health information (ePHI) refers to health information that is covered by the Health Insurance Portability and Accountability Act (HIPAA) security regulations and is produced, saved, transferred, or received in an electronic form

Event – Audit logs will record system events that could potentially affect the security state of the system. An event is an observable occurrence in the information system such as an email, failed login attempt, port scan, or system crash.

Essential County Business Services – The essential business services that must be performed by statute or executive order or are otherwise deemed necessary.

Exposure – The state of being susceptible to asset loss because of a threat or the possibility that a vulnerability could be exploited by a threat agent or event.

Extranet – Network segments dedicated to communications between King County and third–party connections.

Financial Information – Any information such as draft/final financial results, financial statements, reports, records, audit reports, auditor letters, bank records, cash activity records, budget, operating plans, or tax returns.

Financial Separation of Duties – Ensure tasks that could result in fraud are separated. For example, authorization and posting of journal entries are separated between different individuals or groups, and no one person can add a vendor and pay that said vendor.

Firewall – A device or program that restricts data communication traffic to or from a network and thus protects that network's system resources against threats from another network.

Hacker – Someone who attempts to or gains access to an information system, usually in an unauthorized manner. A “white hat” hacker is a cybersecurity specialist who breaks into systems with a goal of evaluating and ultimately improving the security of an organization’s systems.

Hardware Asset – The material physical components of an information system of value or exhibits properties to which value can be assigned.

Hot Fix Change – Change type that is a low risk such as quick fixes and repairing bugs.

HR Information – Any information that includes employee personal data, employee lists, org charts, compensation info, immigration records, evaluations, disciplinary records.

Identity – A set of attributes that uniquely describe a person within a given context.

Identity Asset – The set of discrete attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager’s responsibility, is sufficient to distinguish that entity from any other entity, which is valued by King County. This includes the set of physical and behavioral characteristics by which an individual is uniquely recognizable. Note: This also encompasses non-person, or machine, entities (NPEs).

Impact of Loss – The determination of the business and financial impacts to the organization if the asset is offline or unavailable.

Information Assets – Data gathered, used or observed by a user during their course of employment, and stored on devices such as company computers, telecommunication equipment (including mobile phones and pagers), personal digital assistants, flash memory devices, tape backups, other removable media, networks, automated data processing, databases, the Internet, the intranets, printing, management information systems, and related information, equipment, goods, and services.

Information Security Event – Any event that attempts to change the security state of the system (e.g., change access controls, change the security level of a user, change a user password). Also, any event that attempts to violate the security policy of the system (e.g., too many logon attempts).

Information Security Incident – An information security incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of the Acceptable Use Policy. Examples include, but is not limited to disclosure of sensitive information, denial of service attack, or loss or theft of computer data.

Information Technology – Computer data assets that include hardware, software, network, telecommunications, and interface components.

Information Technology (IT) Business Continuity – A process of advance arrangements, procedures or alternate business practices that enable an organization to respond to an event in such a manner that critical business functions continue within predictable and acceptable levels of service.

Integrity – A property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored. (CIA Triad)

Internal Network – Any network segment owned, configured, maintained, or monitored by King County. The internal network and the internet are separated by a firewall.

Internet of Things (IoT) – The interconnection of electronic devices embedded in everyday or specialized objects, enabling them to sense, collect, process, and transmit data. IoT devices include wearable fitness trackers, “smart” appliances, home automation devices, wireless health devices, and cars—among many others.

Intrusion Detection System – A system or software that monitors and analyzes network or system events for the purpose of finding and providing real–time or near real–time warning of attempts to access system resources in an unauthorized manner.

Intrusion Prevention System – A system or software that monitors and analyzes network or system events for the purpose of finding and providing real–time or near real–time warning of attempts to access system resources in an unauthorized manner. In addition, intrusion prevention systems can also attempt to stop the activity, ideally before it reaches its targets.

King County Systems – All Information Technology (IT) assets, data assets, corporate networks, systems, and applications that are owned or leased by King County. This includes internal and external systems, computer equipment, software, operating systems, storage media, fax machines, phones, network accounts, email, and Internet access, Software–as–a–Service (SaaS) and cloud–based solutions purchased or leased by King County.

Label – Explicit or implicit marking of a data structure or output media associated with an information system representing the King County Data Classification or security category, or distribution limitations or handling caveats of the information contained therein. This is the means used to associate, or tag, a set of security attributes, including protection requirements, with a specific information object as part of the data structure and for that object.

Least Privilege – The method used to grant access wherein authorized or approved users are given access to only those functions which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Any subsequent access request needs to go through an established company access control program.

Legal Information – Any information that includes contracts, stock records, patent and trademark applications, corporate transaction (mergers, acquisitions, reorganizations) files, transaction due diligence files, and legal dispute files.

Local Area Network (LAN) – A group of computers and associated devices (network) that share a common communications line or wireless link to a server. Typically, a LAN encompasses computers and peripherals connected to a server within a distinct geographic area such as an office building.

Machine Account – An administrative entity identified by an account name or number, used to maintain accountability, custody and control of information services, processes and/or procedures. Typically, these entities are associated with a Machine ID and established for non-human entities e.g. a machine or device acting on behalf of an individual, authorized to access an information system.

Malware – A computer program that is covertly placed onto a computer or electronic device with the intent to compromise the confidentiality, integrity, or availability of data, applications, or operating systems. Common types of malware include viruses, worms, malicious mobile code, Trojan horses, rootkits, spyware, and some forms of adware.

Major Change – Change type that is required for system functionality or business activity. This is a high–risk change type.

Managed Device – A device where KCIT can enforce and validate technical security controls such as encryption, credential management, or anti–malware software. Examples include laptops, cell phones, or desktops provisioned by KCIT.

Managed Platform – A platform where KCIT can enforce and validate technical security controls such as firewalls, session timeouts, or rights management. Examples include the King County web application, Single Sign–On solution, or email.

Material Change – Any change to a system's configuration, environment, information content, functionality, or users which has the potential to change the risk imposed upon its continued operations. This may be a low, medium or high risk change type.

Maximum Tolerable Downtime (MTD) – Maximum Tolerable Downtime; the maximum length of time a business function can be inoperable without causing irreparable harm to the business.

Minor Change – Change type of having the potential to impact key processes, but not immediate and does not require shutting down of the system or services.

Multi–factor authentication – Authentication using two or more factors to achieve authentication. Factors include: (1) something you know (e.g. password/PIN); (2) something you have (e.g., cryptographic identification device, token); or (3) something you are (e.g., biometric).

Network – An information system implemented with a collection of interconnected components such as computers, routers, hubs, cabling, and telecommunications controllers.

Network Infrastructure – The physical layer consists of the hardware resources that are necessary to support the information services being provided, and typically includes server, storage and interconnected network components such as routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. Cloud and virtual network infrastructure can be viewed as containing both a physical layer and an abstraction layer. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

Network Segmentation – Splitting a network into sub-networks, for example, by creating separate areas on the network which are protected by firewalls configured to reject unnecessary traffic. Network segmentation minimizes the harm of malware and other threats by isolating it to a limited part of the network.

NIST Cybersecurity Framework – A widely used, risk–based approach to managing cybersecurity composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Cybersecurity Framework includes references to standards, guidelines, and best practices. The Framework is voluntary for private sector use; federal agencies must use this risk management approach.

Operating System – The software “master control application” that runs a computer or electronic device.

Organization – Every County Agency, Department, Official, Officer, Workforce Member, Judge, Elected Official, board or commission, facility, or other element or entity of King County government.

Passphrase – A secret sequence of words or other text used to authenticate a person’s or system’s identity. A passphrase is similar to a password but is generally longer for added security.

Password – A secret string of characters (letters, numbers, and other symbols) used to authenticate an identity, to verify access authorization or to derive cryptographic keys.

Patch – A “repair job” for a piece of programming, also known as a “fix.” When a software developer or distributor learns of a security weakness, a patch is the usual immediate solution that is provided to users and can sometimes be downloaded from the software maker’s web site.

PCI – Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. PCI– related data is any data relating to credit cards.

Penetration Testing – Security testing in which evaluators mimic real–world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.

Personal Data – Any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier. This includes but is not limited to name, identification number, location data, or an online identifier.

Personal Gain – An advantage or benefit specific to a particular person as opposed to an agency, group or organization.

Personal Identifiable Information (PII) – Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linkable to a specific individual (e.g., date and place of birth, mother’s maiden name, etc.).

Phishing – A technique for attempting to acquire sensitive data, such as bank account numbers, or access to a larger computerized system through a fraudulent solicitation in email or on a web site. The perpetrator typically masquerades as a legitimate business or reputable person.

Physical Access Codes – One factor used to authenticate an individual to a physical access control management system. Typically, used in conjunction with additional factors like an employee badge or ID to establish a claimed identity and checked against access authorization controls.

Privacy – Digital privacy is more than the security of personal information. It also covers the processing of information about individuals for a business' operational purposes throughout the information lifecycle (from collection through disposal) and addressing risks that this processing could create for these individuals. These problems could range from embarrassment, discrimination, or loss of autonomy to more tangible harms such as identity theft or physical harm.

Privileged Account – An information system account with approved authorizations of a privileged user. Privilege sets vary and this can include administrator privileges or privileged access that includes the ability to modify security settings, a particularly sensitive role.

Production Environment – The production environment (prod) is also known as live, particularly for servers, as it is the environment that users directly interact with.

Ransomware – A type of malware that attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid.

Record – Physical and electronic information prepared, generated, transmitted, received, or otherwise maintained or held by King County employees and independent contractors in connection with King County general business activities.

Recovery Point Objective (RPO) – Recovery Point Objective; the maximum targeted period in which data might be lost from an IT service due to a major incident.

Recovery Time Objective (RTO) – Recovery Time Objective; the amount of time in which King County can reasonably recover a function/process in the event of a disruption.

Remote Access – Access to an organization's information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

Risk – The extent to which an entity is threatened by a potential circumstance or event. Risk typically is a function of: (1) the adverse impacts that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence. Information system–related security risks arise from the loss of confidentiality, integrity, or availability of information or information systems. These risks reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Risk Management – The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation. Risk management includes: (1) establishing the context for risk–related activities; (2) assessing risk; (3) responding to risk once determined; and (4) monitoring risk over time.

Role–Based Access Control – Systems that employ role–based access controls define a subject's ability to access an object based on the subject's role or assigned tasks. Role–based access control is often implemented using groups.

Router – A device that allows communication between different networks. Routers determine the best path for forwarding data to its destination.

Safeguard – A countermeasure or control that removes or reduces a vulnerability or protects the vulnerability against one or more specific threats. Example: software patch or configuration change.

Secure Socket Shell (SSH) – SSH, also known as Secure Socket Shell, is a network protocol that provides administrators with a secure way to access a remote computer. SSH also refers to the suite of utilities that implement the protocol.

Security Awareness – Security awareness is the focus of individuals' attention on security, and security awareness presentations shall enable King County users to recognize IT security concerns and how to respond.

Security Awareness Training – An educational program designed to reduce the number of security breaches that occur from the lack of employee security awareness.

Segregation of Duties (SoD) **–** A security principle that divides critical functions among different staff members to reduce the likelihood of providing one individual with enough information or access privilege to perpetrate damaging fraud.

Separation of Duties (SoD) – A security principle that divides critical functions among different staff members to reduce the likelihood of providing one individual with enough information or access privilege to perpetrate damaging fraud.

Service Account – An administrative entity identified by an account name or number, used to maintain accountability, custody and control of information services, processes and/or procedures. Typically, these entities are established for non-human users e.g. a service or (system) process acting on behalf of an individual, authorized to access an information system.

Service Provider – An external company that provides services that are used by information systems, such as an Internet Service Provider.

Social Media – Forms of electronic communications, including websites and applications, that enable users to create and share content or to participate in social networking.

Software Asset – Computer programs and associated data that may be dynamically written or modified during execution, to which value can be assigned.

Spam – Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Spear Phishing – A highly targeted phishing attack, usually to a specific individual or department within an organization.

Spyware – Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge.

Strategic Information – Any information that includes organizational plans, corporate partnerships, acquisitions, public or private offerings of stock, information regarding competitors, or new product offerings.

Technology Asset – ***See Asset***

Telecommuting – The ability for an organization's employees and contractors to conduct work from locations other than the organization's facilities.

Test Environment – The purpose of the test environment (test) is to allow individual testers to exercise new and changed code via either automated checks or non–automated techniques. After the developer accepts the new code and configurations through unit testing in the development environment, the items are moved to one or more test environments. Upon test failure, the test environment can remove the faulty code from the test platforms, contact the responsible developer, and provide detailed test and result logs. If all tests pass, the test environment or a continuous integration framework controlling the tests can automatically promote the code to the next deployment environment.

Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threat–Source – A circumstance or event with the potential to cause harm to an IT system. Common threat–sources are natural, human, or environmental.

Transport Layer Security (TLS) – Transport layer security (TLS) is a protocol that provides communication security between client/server applications that communicate with each other over the Internet. It enables privacy, integrity, and protection for the data that's transmitted between different nodes on the Internet.

Un–Managed Device – An unmanaged device is a device where KCIT does not have the ability to enforce and validate technical security controls. Examples include an employee–owned mobile device or personal desktops. Only managed devices that are compliant with King County policies shall be permitted to access non–public data, but unmanaged devices may be permitted access after review and approval from KCIT based on the security controls in place.

Untrusted Network – Any network or host not directly owned, configured, maintained or monitored by King County.

User – A user is defined as anyone with authorized access to King County technology resources including permanent and temporary employees or third–party personnel such as temporaries, contractors, consultants, and other parties with valid King County access accounts.

Vendor – A company, third–party, contractor, or person(s) providing a product or service to King County.

Virtual Private Network (VPN) – Virtual network built on top of existing networks that can provide a secure communications mechanism for data and Internet Protocol (IP) information transmitted via the virtual network.

Viruses – A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e–mail programs to spread itself to other computers, or even erase everything on a hard disk.

Vulnerability – A weakness that allows an attacker to compromise the integrity, availability, or confidentiality of a system.

War Dialing – Refers to the use of various technologies to automatically dial many phone numbers, usually in order to find weak spots in an IT security architecture. Hackers often use war dialing software to look for unprotected modems.

Whitelist – An approved list or register of entities provided a particular privilege, service, mobility, access, or recognition.

Wide Area Network (WAN) – A group of computers and associated devices (network) that exists over a large–scale geographical area. WANs connect different small networks such as LANs and metro area networks (MANs).

Workforce Member – Employees, volunteers, and other persons whose conduct, in the performance of work for King County, is under the direct control of King County, whether or not they are paid by King County. This includes full and part–time elected or appointed officials, members of boards and commissions, employees, affiliates, associates, students, volunteers, and staff from third–party entities who provide service to King County.