BTS-6.01 - Information Technology Definitions

INFORMATION TECHNOLOGY DEFINITIONS
Administrative Rule Adopted by Council
ARC-BTS-6.01

Definitions

The following information and communications technology definitions and terms are used in the Bureau of Technology Services Administrative Rules and associated standards and guidelines. These definitions are not part of the binding BTS Administrative Rules.

802.11: A family of IEEE specifications for wireless local area networks.

802.1X: A standard developed by IEEE designed to enhance the security of both wired and wireless networks. 802.1X provides an authentication framework allowing a user or device to be authenticated by a central authority.

Access Control: Physical, procedural and/or electronic mechanism which ensures that only those who are authorized to view, update and/or delete data can access that data.

Access Point: Also know as a wireless base station. A hardware device that acts as a communication hub for users of a wireless device to connect to a wired local area network.

Algorithm: An unambiguous formula or set of rules for solving a problem in a finite number of steps. Algorithms for encryption are usually called Ciphers.

Analog Line: A communications line, such as a standard telephone line, that carries information in analog (continuously variable) form.

Analog Modem: Communications equipment which converts computer information/data, in the form of digital pulses to audio tones that can be carried over analog telephone lines.

Anonymous Access: A method which allows access to applications or systems without requiring user identification and password authentication.

Anti-Virus Software: A software program designed to identify and remove a known or potential computer virus, worm or trojan horse

Application: Software that performs a specific task or function, such as wordprocessing, creation of spreadsheets, generation of graphics, facilitating electronic mail, etc

Asset: A physical item, informational item, or capability required by an organization to maintain productivity. Examples include computing systems, communication systems and data.

Attachment: A file attached to an e-mail message.

Authentication: The assurance that a party to some computerized transaction is not an

impostor. Authentication typically involves using a password, certificate, PIN, or other information that can be used to validate the identity over a computer network

Authorization: The process of giving someone permission to do or have something; a system administrator defines for the system which users are allowed access to the system and what privileges are assigned.

Availability: The assurance that a computer system is accessible by authorized users whenever needed, as pre-defined, or as established through a Service Level Agreement.

Backup: The activity of copying electronic data so that it will be preserved in case of equipment failure, accidental or malicious loss or other catastrophe.

Breach: The successful defeat of security controls which could result in a penetration of the system. A violation of controls of a particular information system such that information assets or system components are unduly exposed.

Business System Owners: Individuals within the City who are ultimately accountable for the budget, management, and use of one or more electronic information systems or electronic applications that are associated with the City of Portland (e.g. Bureau Directors). Electronic information systems cover a wide range of business requirements and 'ownership'. They may be singlepurpose/ single-bureau business applications as well as multi-purpose/multibureau business applications. Business applications may also be 'enterprise' applications that serve the common functional requirements of all City bureaus and offices (e.g. various administrative information systems).

Change Management: Process of controlling changes to the infrastructure or any aspect of services, in a controlled manner, enabling approved changes with minimum disruption.

Cipher: A method that encrypts or disguises text. Ciphers replace the message letters with other letters, numbers or symbols, as in substitution, or move around the individual letters of the plaintext, as in transposition − or a combination of both.

Common Criteria: A comprehensive specification that first defines the targeted environment and then specifies the security requirements necessary to counter threats inherent in that environment.

Compliance: A user, device, computing system, network element or operating system is in compliance with a policy when it implements and adheres to all functional aspects explicitly stated as required in that policy.

Confidentiality: An attribute of information. Confidential information is sensitive or secret information, or information whose unauthorized disclosure could be harmful or prejudicial.

Cost-effective: To deliver desired results in beneficial financial terms.

Credential: A general term for privilege attribute data that has been certified by a trusted privilege certification authority

Cracking: The process of overcoming a security measure. Also commonly referred to as

Hacking.

Criticality: A relative measure of the consequence of a particular failure mode and its frequency of occurrence.

Cryptosystem: A system used for encrypting and decrypting data. Usually involves an algorithm for combining the original data (plaintext) with one or more keys - numbers or strings of characters known only to the sender and recipient - into cipher text.

Database: A shared collection of logically related data, designed to meet the information needs of multiple users in an organization.

Data Custodians: Data Custodians are business experts who have been officially designated by the Bureau of Technology Services and/or Bureau Business System Owners as accountable for the definition of specific business requirements regarding protection of the confidentiality of specific data that is transmitted, used, stored, and maintained on City of Portland information systems. Data Custodians help translate the business requirements into appropriate system security procedures that are aligned with the City of Portland Information System Security Policy.

DMZ: Short for demilitarized zone which is an internal network typically used exclusively for servers that are accessed by external clients on the Internet, such as web servers. Placing these public access servers on a separate isolated network, provides an extra measure of security for internal networks

DNS: Also know as a Domain Name System (or Service) which translates alphabetic domain names into numeric IP addresses.

Download: Transferring data (usually a file) from another computer to the computer you are using.

E-Commerce: A way of supporting real-time business transactions via the internet.

E-Government: The process by which the City delivers information and services electronically. It allows citizens and businesses easy access to government information and streamlined business processes.

Encryption: The transformation of data into a form unreadable by anyone without a secret decryption key. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it was not intended, including those who can see the encrypted data.

Entitlement: Any of the benefits to which one is entitled, or to which one is given a right, by meeting specific eligibility requirements.

Electronic Protected Health Information (ePHI): Individually identifiable electronic health information that is stored and/or transmitted that relates to the past, present or future physical or mental health condition of an individual, the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual.

Ethernet: The common method of networking computers in a LAN, or Local Area Network.

Extranet: A private network that uses internet protocols and the public telecommunications system to securely share part of a business's information or operations with suppliers, vendors, partners, customers or other businesses.

Firewall: A combination of hardware and software that secures access to and from a network based on rules.

Frame Relay: Standard packet-switched protocol for transmission of voice and data that creates "virtual" dedicated circuits. These are less expensive than dedicated circuits.

Gateway: A hardware and/or software set-up that translates between two dissimilar protocols

Governance: The authority for defining policy, providing leadership, and managing and coordinating the procedures and resources that ensure the security of information systems

Hash Number: Also called "hash function" or hashing, used extensively in many encryption algorithms. Hashing transforms a string of characters usually into a shorter, fixed-length value or key.

HIPAA: Short for the Health Insurance Portability and Accountability Act of 1996**.**

Incident Response: The ability to respond appropriately and completely to any incidents, situational compromises, or threats from any source at anytime.

Information System: The network or combinations of all computing equipment, telecommunication or other communication or information processing devices and channels used within an organization.

Infrastructure: The computer and communication hardware, software, databases, people, and policies supporting the enterprise's information management functions.

Integrity: The condition of data or a system, in which that data or system remains intact, unaltered, and hence reliable.

Internet: The vast collection of inter-connected networks that all use the TCP/IP protocols and that evolved from the ARPANET of the late 60's and early 70's.

Intranet: Contrary to the public Internet, an intranet is a private network inside a company or organization.

Intrusion Detection: A security management system and or process that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attack from outside the organization) and misuse (attacks from within the organization).

IPSEC: Short for Internet Protocol Security. Security functions (authentication and encryption) implemented at the IP level of the protocol stack.

ISDN Line: Also know as an Integrated Services Digital Network. A digital telephony scheme that allows a user to connect to the Internet over standard phone lines at speeds higher than a 56K modem allows.

Language: A formal language with a particular set of 'grammatical' rules and guidelines used in writing a computer program or software.

LDAP: An acronym for Lightweight Directory Access Protocol which is a network protocol designed to help users extract information from a hierarchical directory in a network, whether on the Internet or on a corporate intranet.

Mobile Device: Any computing or communications device intended to frequently move location while maintaining function and operation.

Modem: A device that allows computers to communicate with each other over telephone lines or other delivery systems by changing digital signals to telephone signals for transmission and then back to digital signals.

Malware: Short for malicious software and is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms and trojan horses.

MAC Address: Short for media access control address; the unique physical address of each device's network interface card

Memory: The space used by a computer to hold the program that is currently running, along with the data it needs.

Mitigate: The action of reducing or minimizing the severity of the impact or likelihood of a risk or an event.

Multi-user: A system or program designed to accommodate simultaneous use by multiple users,

Need-to-Know: An administrative action certifying that a given individual requires access to specified private information in order to perform his or her assigned duties.

Network: A collection of two or more computer or communication systems interconnected by telephone lines, communications cables, satellite links, radio, and/or other communication techniques.

Network Interface Card: An expansion board you insert into a computer so the computer can be connected to a network.

Non-repudiation: A mutually agreed process, secured evidence, or other method of operation which provides for proof of receipt or protection from denial of an electronic transaction or other activity.

Operating System: The foundation software of a machine; that which schedules tasks, allocates storage, and presents a default interface to the user between applications.

Ownership: The term that signifies decision-making authority and accountability for a given span of control.

Password Protection: The ability to protect a system, data or object using a password

Pass Phrase: The word or phrase that protects private key files. It prevents unauthorized users from encrypting them.

Patch: A piece of code added to software in order to fix a vulnerability or bug, especially as a temporary correction between software releases

PDA: Short for personal digital assistant, a small handheld device that combines one or more computing and/or communications functions such as email, calendar, internet and phone.

Penetration Testing: A security evaluation performance wherein practitioners attempt to gain access to a system despite security features.

Physical Security: The component of information security that results from all physical measures necessary to safeguard equipment and data, from access by unauthorized persons or electrical or environmental (fire, smoke, temperature, etc) damage.

Portal: A starting point web page with a hierarchical, topical directory, a search window, and added features like news headlines applications and links to informative and collaborative services and applications.

Port Scanning: A program that attempts to learn about the weaknesses of a computer or network device by repeatedly probing it with requests for information.

Principle of Least Privilege: An operations principle that requires access privileges for any user to be limited to only what they need to have (nothing in addition) to be able to complete their assigned duties or functions.

Principle of Separation of Duties: An operations principle that requires that whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse or other harm.

Privacy: The protection of sensitive data and personal information from unintentional and intentional attacks and disclosure.

Privilege: A user's right to perform a specific task on an information system. Privileges are assigned by administrators to individual users or groups of users as part of the security settings for the computer.

Proprietary: Refers to a technological design or architecture whose configuration is unavailable to the public and may not be duplicated without permission from the designer or architect.

Protocol: Agreed-upon methods of communications used by computers. A specification that describes the rules and procedures that products should follow to perform activities on a network, such as transmitting data.

Quarantine: Enforced isolation or restriction of communications imposed to prevent the introduction or spread of computer viruses.

RADIUS: Short for Remote Authentication Dial-In User Service. A client/server protocol and software that enables remote access servers to communicate with a central server to authenticate remote users and authorize their access to the requested system or service.

Retention Schedule: The defined period of time for which electronic data must be retained and accessible in support of business and legal requirements.

SCADA: An acronym for Supervisory Control And Data Acquisition, a process control application that collects data from sensors and machines on a shop floor or in remote locations and sends them to a central computer for management and control.

Security: An attribute of information systems which includes specific policy-based mechanisms and assurances for protecting the confidentiality and integrity of information, the availability and functionality of critical services and the privacy of individuals.

Security Audit: A search through an information system designed to detect security problems and vulnerabilities and measure compliance to security policies and standards.

Secure Channel: Refers to information sent encrypted over the network.

SNMP: An abbreviation for Simple Network Management Protocol, an Internet standard that defines methods for remotely managing active network components such as servers, switches, hubs, routers, and bridges.

Source Code: The readable form of code that you create in a high-level programming language. Source code is converted to machine-language object code by a compiler or interpreter.

SplitTunneling: Simultaneous access to a non-City network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into the City network via a VPN connection.

SSH: Short for Secure Shell. A protocol for creating a secure connection between two systems using a client/server architecture. SSH provides mutual authentication, data encryption and data integrity.

SSID: Also know as a service set identifier. A unique identifier that stations must use to be able to communicate with a wireless access point.

System Operators: BTS and/or bureau technical support staff who implement, conduct routine day-to-day tasks, and maintain information systems, including authorization tables, security systems and back-up systems, in accordance with established City of Portland enterprise and business-specific policies, standards, procedures and guidelines.

Tamper: To interfere improperly or in violation of policy or rule such as to tamper with computing software or systems.

Token: A hardware device or software program that generates a one-time password to authenticate its owner or authorized user.

Trust Relationship: The relationship between two domains that enables a user or resource in one domain to access resources in another domain

Trojan Horse: Software that is written to allow access to a computer via some method not intended by the owner of the system. Typically embedded in some other form of software Trojan code attempts to camouflage its presence to avoid detection.

USB Thumb Drive : A small, removable solid state data storage device which can be easily connected to and removed from a computer via its universal serial bus (USB) port.

Users: Any individual that has been granted privileges and access to computing, cummunications and network services, applications, resources, and information.

User Name: The name that identifies a user to a computer network; generally used in conjunction with a password to establish the user's right to access a host; also called account name or user ID.

Virtual Private Network (VPN): A way to provide remote access to an organization's network via a secure communications tunnel over the Internet

Virus: A software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the same computer. A true virus cannot spread to another computer without human assistance

Waiver: The voluntary and intentional relinquishment of a known right, claim or privilege.

Web Service: A Standardized way of integrating web-based applications which share business logic, data and processes through a programmatic interface across a network.

Wireless: Communications in which electromagnetic waves, rather than cables or wires, carry the signal over part or all of the communication path **Worm:** A software programs capable of reproducing itself that can spread from one computer to the next over a network without human assistance

---

History
Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.