

Ohio Trustworthy Information Systems Handbook: Section 10

Glossary

Note: Definition sources are indicated by letters and listed at the end.

<u>Term</u>	<u>Definition</u>
Accountability	1. The quality of being responsible, answerable; the obligation to report, explain, or justify an event or situation.
Archival Value	1. "The values, evidential and/or informational that justify the continuing retention of records as archives." (i)
Archiving	1. "The process of creating a backup copy of computer files, especially for long-term storage." (h)
Asymmetric Encryption	1. "A form of cryptosystem in which encryption and decryption are performed using two different keys, one of which is referred to as the public key and one of which is referred to as the private key. Also known as public-key encryption." (a)
Audit Trail	1. "A record showing who has accessed a computer system and what operations he or she has performed during a given period of time." (b)
Authenticity	1. Authenticity is a function of a record's preservation and is a measure of a record's reliability over time.
Authentication	1. "A process used to verify the integrity of transmitted data, especially a message." (a) 2. "The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual." (b) 3. "The process of confirming an asserted identity with a specified, or understood, level of confidence. The mechanism can be based on something the user knows, such as a password, something the user possesses, such as a 'smart card,' something intrinsic to the person, such as a fingerprint, or a combination of two or more of these." (g)

Back-up	1. "To copy files to a second medium . . . as a precaution in case the first medium fails." (b)
Backup	1. "A substitute or alternative. The term backup usually refers to a disk or tape that contains a copy of data." (b)
Biometric-based Device	1. An authentication technique relying on measurable physical characteristics of the user that can be automatically checked. An example is a fingerprint scanner. (b)
Data	1. "Symbols, or representations, of facts or ideas that can be communicated, interpreted, or processed by manual or automated means." (h)
Data Model	1. A diagram that shows the various subjects about which information is stored, and the relationships between those subjects.
Data Warehouse	1. A computer-based information system that is home for "secondhand" data that originated from either another application or from an external system or source. A data warehouse is a read-only, integrated database designed to answer comparative and "what if" questions. Unlike operational databases that are set up to handle transactions and that are kept up to date as of the last transaction, a data warehouse is analytical, subject-oriented, and structured to aggregate transactions as a snapshot in time.
Digital	1. "Describes any system based on discontinuous data or events. Computers are digital machines because at their most basic level they can distinguish between just two values, 0 and 1, or off and on. There is no simple way to represent all the values in between, such as 0.25. All data that a computer processes must be encoded digitally, as a series of zeroes and ones." (b)
Digital Signature	1. "An authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature guarantees the source and integrity of the message." (a)
Disaster	1. "An unexpected occurrence inflicting widespread destruction and distress and having long-term adverse effects on agency operations. Each agency defines what a long-term adverse effect is in relation to its most critical program." (h)

Documentation

1. "The act or process of substantiating by recording actions and/or decisions." (h)
2. "Records required to plan, develop, operate, maintain, and use electronic records. Included are systems specifications, file specifications, codebooks, file layouts, user guides, and output specifications." (h)

Dynamic

1. "Refers to actions that take place at the moment they are needed rather than in advance." (b)

Electronic

1. "Of, or relating to, technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities." (e)

Electronic Document

1. "Recorded information that is recorded in a form that requires a computer or other machine to process it. Includes word processing documents; electronic mail messages; . . . Internet and intranet postings; numerical and textual spreadsheets and databases; electronic files; optical images; software; and information systems." (h)

Electronic Record

1. "A record created, generated, sent, communicated, received, or stored by electronic means." (e)

Firewall

1. "A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria." (b)

Format

1. "The shape, size, style, and general makeup of a particular record." (h)

Hard Copy

1. "A printout of data stored in a computer. It is considered hard because it exists physically on paper, whereas a soft copy exists only electronically." (b)

Information

1. Data, text, images, sounds, codes, computer programs, software, databases, etc. (e)

Information System

1. "An electronic system for creating, generating, sending, receiving, storing, displaying, or otherwise processing information." (e)
2. "The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. . . . Most often refers to a system containing electronic records, which involves input or source documents, records on electronic media, and output records, along with related documentation and any indexes." (h)

Input Device

1. Any apparatus, such as a keyboard, that allows data to be fed or entered into a computer. (b)

Internet

1. A decentralized global network connecting millions of computers.

Intranet

1. "A network . . . belonging to an organization . . . accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like any other Web sites, but the firewall surrounding an intranet fends off unauthorized access." (b)

Legacy System

1. "An application in which a company or organization has already invested considerable time and money." (b)

Log-in

1. To enter information before gaining access to a computer system. At the minimum, log-in typically requires a username and password.

Metadata

1. Data about data.
2. "The description of the data resources, its characteristics, location, usage, and so on. Metadata is used to identify, describe, and define user data." (h)

Microform

1. "Any form containing greatly reduced images, or microimages, usually on microfilm. Roll, or generally serialized, microforms include microfilm on reels, cartridges, and cassettes. Flat, or generally unitized, microforms include microfiche, microfilm jackets, aperture cards, and microcards, or micro-opaques." (h)

Migration

1. The process of moving computer files from one information system or medium to another.

Official Record

1. "In disposal scheduling, the copy of the record held by the office of record. Any other copies of the record can then be destroyed whenever they are no longer required." (i)

Output Device

1. Any machine capable of representing information from a computer, including display screens, printers, plotters, and synthesizers. (b)

Password

1. "A character string used to authenticate an identity. Knowledge of the password and its associated user ID is considered proof of authorization to use the capabilities associated with that user ID." (a)

Permanent Value

See **Archival Value**

Private Key

1. "One of the two keys used in an asymmetric encryption system. For secure communication, the private key should be known only to its creator." (a)

Public Key

1. "One of the two keys used in an asymmetric encryption system. The public key is made public, to be used in conjunction with a corresponding private key." (a)

Record

1. "Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." (e)
2. Information created or received during the course of government business that becomes part of an official transaction.
3. "Records" includes any document, device, or item, regardless of physical form or characteristic, created or received by, or coming under the jurisdiction of any public office of the state or its political subdivisions, which serves to document the organization, functions, policies, decisions, procedures, operations, or other activities of the office. (j)

Reliability

1. Reliability is the measure of a record's authority and is determined solely by the circumstances of the record's creation.

Removable Media

1. Media, such as tapes, floppy disks, and CD ROMs, that can be physically removed from the computer environment.

Retention Period

1. "The period of time, usually based on an estimate of the frequency of current and future use, and taking into account statutory and regulatory provisions, that records need to be retained before their final disposal." (i)

Retention Schedule

1. A plan for the management of records including a list of record series, coverage dates, locations, formats, volume, data practices classifications, and retention periods.

Risk Analysis

1. A component of risk management that evaluates risks (the possibility of incurring loss or injury), examining the probability of loss or injury occurring, then determining the amount of risk that is acceptable for a given situation or event; a prioritization of risks.

Spoilation

1. The destruction of evidence.

Storage Device

1. A device capable of storing data such as disk drives and tape drives. (b)

System Development Life Cycle

1. "A systematic and orderly approach to solving business problems, and developing and supporting resulting information systems." Typical phases of the system development life cycle include: Planning, Analysis, Design, Implementation, and Support. (d)

Transaction

1. "An action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs." (f)

Trustworthy

1. An information system that produces reliable and authentic records.

URL

1. "Abbreviation of Uniform Resource Locator, the global address of documents and other resources on the World Wide Web." (b)

Virus

1. "Code embedded within a program that causes a copy of itself to be inserted in one or more other programs. In addition to propagation, the virus usually performs some unwanted function." (a)

World Wide Web (WWW)

1. "A system of Internet servers that support specially formatted documents. The documents are formatted in a language called HTML (HyperText Markup Language) that supports links to other documents, as well as graphics, audio, and video files." (b)

Worm

1. "Program that can replicate itself and send copies from computer to computer across network connections. Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function." (a)