

Return to University Data and Computing Policies, Standards and Procedures

Data and Computing Definitions

The definitions contained in this document apply to all University data and computing policies, standards and procedures to ensure consistent usage and understanding.

Academic Computing refers to computer systems that support the research and educational mission of the University.

Access Control refers to the process of limiting access to computing systems and resources to authorized users, programs, processes, or other systems.

Administrative Computing refers to computer systems that support the operational functions (e.g., financial, payroll/personnel, library, and student related data such as major, grades, courses, etc.) of the University.

Advertising is offering space on a web page/publication to another party for the purpose of promoting goods and services offered by that party in exchange for money, goods, or services.

Alt Tags are HTML codes that describe graphical elements in a web page/publication so that they are viewable by non-graphical browsers.

Alternate Facility or Alternate Operating Site is a temporary facility in which business functions will be performed during a recovery effort.

Anonymous Connection is the act of connecting to a remote computer as an unidentified or anonymous user.

Antivirus software is software that detects the existence of viruses, trojans and other malware threats on your computer system.

Application Administrator is the individual responsible for the functional operation of a data system (manual or electronic) including, but not limited to, business resumption and recovery.

Application Software is a program(s) written to perform a business process such as payroll.

Application Program Interface (API) is a formalized set of software calls and routines that can be referenced by an application program in order to access supporting network services.

Approved Users - Authorized Users who have been given explicit access to specific data by the Data Custodian.

Archival Records are records which have continuing administrative, research or historical value, or which document the University's organization, functions, policies, decisions, procedures, or operations. Examples include organization charts, memorandum, minutes, architectural drawings, graduate theses and senior honors theses, personal papers, etc

Audit Trail is a log(s) of specified access (e.g., when, how, from where and by whom data is accessed). For example, a log of all changes to student grades would be kept to monitor who was accessing such confidential data and what they were doing (e.g., reading, updating, deleting) or a log of network hardware/software changes would be maintained to monitor what configuration changes were made and by whom.

Authenticated Digital Signatures is the digital verification of the identity of a person or process. In a communication system, authentication verifies that messages really come from their stated source, like the signature on a (paper) letter.

Authentication Or User Authentication is the process by which the identity of an individual and their right to access specific categories of data are verified.

Authorized Users are all students and employees (including student, non-student, faculty, professional, classified, temporary, part-time, and full-time), and contracted consultants of the University of Massachusetts who are required to have access to data to perform their job function, academic assignment, or contractual obligations. Authorized users also include those individuals who are assigned courtesy accounts.

Baseline Level of Connection Service Quality is determined by factors that can affect radio transmissions, such as distance from the wireless access point (i.e., WAP), number of users sharing the bandwidth, state of the environment from which the transmission is taking place, and the presence of other wireless client devices that can cause interference.

Binary attachments refer to any file format for digital data encoded as a sequence of bits but not consisting of a sequence of printable characters (text). The term is often used for executable machine code.

Bridge is a device that connects two or more physical networks and forwards packets between them. Bridges can usually be made to "filter" packets, that is, to forward only certain traffic.

Browsers or Web Browsers are software programs that display Internet based information as defined by HTML.

A Bulletin Board/Newsgroup is a service that enables users to post information for or seek information from others who are interested in a certain topic(s).

Business Continuity Planning is the process of identifying critical data systems and business functions, analyzing the risks of disruption to the data systems and business functions, determining the probability of a disruption occurring and then developing plans to enable those systems and functions to be resumed in the event of a disruption. The process includes testing and maintaining the business resumption plans to ensure they are effective.

Business Disruption is an occurrence that impacts a data system to the extent that the capability to perform normal and routine operations is impaired.

Business Resumption Plan (BRP) is a document that details the steps to be taken in the event of a business disruption for a specific data system(s).

BRP Coordination Site is a temporary location with communication equipment from which initial resumption efforts are coordinated.

Button Bars are used to place fixed links between a series of pages to bind them into a document. In complex Web sites button bars may also be used to provide links to submenus, tables of contents, or other organizational pages.

Campus or University Computing Infrastructure refers to the underlying technology (e.g., hardware, cabling, telecommunications and software) required to support the primary University/Campus computing and data communications environments which are usually maintained by computing centers. This does NOT include departmental computing resources (e.g., a department level computing system or network).

Campus Procedures are statements designed to comply with the requirements of University Guidelines/Standards by establishing specific criteria that must be met by University students, staff, consultants, etc.

Central Administrative Services refers to the President's Office, Institute for Governmental Services, Treasurer's Office, University Audit, University Controller, and University Information Technology Services.

Campus Information Security Officer /Central Security Specialist is an individual(s) at each campus and the President's Office who has experience, knowledge and understanding of information systems security practices/requirements and who is responsible for data and computer security planning, control, oversight/monitoring, and coordination. This job function may be assigned to one or more individuals on a campus, and is not necessarily an official job title.

Chain E-mail refers to several types of e-mail messages including virus hoaxes, good luck/bad luck messages, and fake fund raisers that are sent out to several users and those users are asked to send the message to several more e-mail users and so on. Chain E-mail unduly strains the computing system and its resources.

Chain of Custody is a legal term that describes the collection, transportation, and storage of evidence to prevent alteration, loss, physical damage, or destruction)

Checklists refer to lists containing brief questions which when properly answered will reveal possible weakness in a system.

Classified Data refers to University data that has been identified as Operational or Confidential. See the University Data and Computing Standards for more information.

Client/Server Technology refers to an environment in which a software package running on one computer (server) is accessed by another computer (client) and the data stored in and processing occurs on the server.

Cold Site is a facility that contains no computing-related equipment except for environmental support such as air conditioners, water conduits, raised floors, motor generators, power outlets, and a security system made ready for installing computer equipment. This site may be University owned or vendor operated.

Computer Applications are sets of computer programs which when run read or modify data, and which can generate output such as reports, bills, checks, etc.

Convenience Records are copies of Official Records maintained by departments other than the Official Records Custodian. This includes records of all mediums and types.

Computer/Computing System(s) refers to the hardware, software and communications equipment (e.g. voice and data networks, servers, routers, modems, etc.) used in the processing and storage of electronic data.

Conference Chat is the ability to interactively communicate on-line in a real-time mode.

Confidential Data is data whose loss, corruption or unauthorized disclosure would be a violation of federal or state laws/regulations or University contracts (i.e., protected data); personally identifiable data; data that involves issues of personal privacy; or data whose loss, corruption or unauthorized disclosure may impair the academic, research or business functions of the University, or result in any business, financial, or legal loss.

Context-Sensitive Help is on-line documentation giving details about a word or topic.

Controls are mechanisms implemented to limit exposure, such as backing up data, storing backups offsite, using surge protectors and uninterruptible power supplies, running virus checking software and security software packages, etc.

Courtesy Accounts are accounts on University computer systems which may be provided to individuals who are not University employees, students, or contracted consultants but who have an established relationship with the University and need access. Examples include: alumni, business partnerships, individuals from other educational institutions, etc.

Coverage is the geographical area where a baseline level of connection service quality is attainable. Coverage area is also expressed as “footprint”.

Critical System is a data system considered to be integral to the accomplishment of the University mission(s) and its business functions, and without which University operations would be curtailed or otherwise severely impeded.

Data refers to information regardless of the medium on which it resides (e.g., tape, cartridge, disk, hard drive, etc.), and regardless of its form (e.g. text, graphic, video, voice, etc.).

Data Compression refers to reducing the amount of storage space required to store a given amount of data, or reducing the length of message required to transfer a given amount of information.

Data Custodian(s) are the individual(s) responsible for making decisions about the sensitivity and critically of specific University systems and data stored in these systems; determining the classification of data under their control; documenting the use of the specific system(s); and determining which University staff require access to that system and its data. University policy may restrict or dictate the Data Custodian's role regarding data design and control (e.g., a policy indicating how access to Institutional Data should be handled would take precedent over

individual Data Custodian decisions/ determinations). Examples of Data Custodians are: the Directors of Human Resources would have Data Custodian responsibility over payroll and personnel information and a Principal Investigator is the Data Custodian for research data related to their grant.

Data Integrity refers to the completeness and accuracy of data.

Data Or Information Security refers to the development and implementation of a reasonable system of measures/controls/safeguards to protect data (regardless of the medium on which it resides (e.g., tape, cartridge, disk, hard drive, etc.) and computing resources from unauthorized access, theft, removal, misuse, disclosure, and/or corruption so that data and computing resource availability and integrity is preserved. These controls when implemented will REDUCE the PROBABILITY of something negative occurring (e.g., unauthorized file access or modification). Computer Security includes the following categories of control: Administrative (e.g., policies/procedures, personnel, and business continuity planning); Hardware; Software (e.g., network, operating and application system software); Data; Communications/ Network; Physical and Environmental; Legal (e.g., state, federal & regulatory).

Data System is any method (e.g., manual, electronic or a combination of both) used to process data (e.g., this could include using paper ledger books, computerized processing, etc.).

Database is a formally structured collection of data or set of data that is required for a specific purpose.

Database Management System (DBMS) refers to a software system that facilitates the creation and maintenance of a database or databases, and the execution of computer programs using the database or databases.

Degree of Risk or Levels of Risk refers to the amount of exposure and/or vulnerability associated with a particular entity such as a computer system. Examples of exposure or vulnerability include: theft; unauthorized access; unauthorized alteration or destruction of the computer system or the data stored on it; human error; natural disasters, etc.

Deleted E-Mail refers to any e-mail which an e-mail user has specifically deleted/removed from their e-mail Inbox or electronic mail files. E-mail moved to a "trash" folder is considered deleted.

Device refers to any part of a computer other than the CPU or working memory (e.g., disks, keyboards, monitors, mice, printers, scanners, tape drives, microphones, speakers, cameras, etc.).

Disposition refers to how records are handled once the retention period has been met. Disposition includes archiving, transfer to another agency, or destruction.

Disruption is any situation or event which interrupts the routine and regular processing of data, thereby causing inaccessibility, harm or damage, sudden or serious misfortune or calamity, or the inability to perform these routine functions in part or in whole.

Distributed Platform refers to the fact the processing of data can be performed on various computers (e.g., mainframe, minicomputers, PC's, etc.) at different locations.

Domain Name consists of a sequence of names or labels separated by periods usually used to name Internet host computers uniquely.

Dynamic Host Configuration Protocol (DHCP) refers to a protocol that provides a means to dynamically allocate IP address to computers on local area networks. The network administrator assigns a range of IP addresses to DHCP and each client computer on the LAN has its TCP/IP software configured to request an IP address from the DHCP server

Electronic Mail (e-mail) refers to letters, files and messages sent by one computer user or a software agent to a specific user or set of users within the same computer system or over a computer network.

Electronic Mail Id is a unique code that identifies a specific person to an electronic mail system.

An **Electronic Mail Administrator** is the individual responsible for making decisions about how an electronic mail system(s) should be maintained, determining classes of individuals which may use the electronic mail system, and determining how the mail system and its capabilities will be implemented and secured.

An **Electronic Mail System** is a computer which has e-mail capabilities on it.

Electronic Signature is the method of ensuring that the purported signer of a document was the actual signer and the document has not been modified since signed.

Electronically Stored Data (i.e., ESI) is any data stored in electronic/digital form and includes but is not limited to: emails, instant messages, calendars, photographs, word processing, videos, spreadsheets, file shares, digital recordings, digital images, voicemail messages, backup tapes, off-site storage media, removable media (e.g., CD, DVD, floppy, USB flash drive, etc.), information in PDA's and smart phones, etc.

Employees are all student, non-student (faculty, professional, classified), temporary, part-time, full-time, contracted individuals and consultants who are paid from University funds and require access to electronic data to perform their job function.

Encryption refers to the process of converting plain text into unintelligible forms (i.e., scrambling) in order to prevent any but the intended recipient from reading that data. There are many types of data encryption, and they are the basis of network security. Common types include Data Encryption Standard (DES) and RSA.

Environmental Controls refer to the simultaneous controlling of the characteristics of air, such as temperature, humidity, cleanliness, motion, and pollutant concentration, in a space to meet the requirements of the equipment.

Executable Programs refer to programs in machine language, which are ready to be run (i.e., the process of carrying out the instructions in a computer program by a computer).

External E-mail Users are individuals who communicate with University mail systems from mail systems not controlled or administered by the University (e.g., Internet).

A **Filter** is a security method to "hide" e-mail message text from the view of electronic mail maintenance personnel.

Financial Records are records related to billing, financial aid disbursements, insurance, purchasing, accounting, and other operationally oriented business functions.

Finger Command refers to a command that provides information about users on a network.

Firewall is a dedicated computer or device with special security precautions on it, used to filter outside network, especially Internet, connections and dial-in lines.

"**Flashable**" firmware is re-programmable software (programs or data) that has been written onto read-only memory (i.e., ROM).

Full-Interruption Testing describes a test in which the total business resumption plan for a data system(s) is activated. This test is costly, could disrupt normal operations and should be used and scheduled with extreme caution.

Graphics Interchange Format Standards (GIFS) are binary attachments that follow standards for digitized images.

Graphical user interface (GUI) is the use of pictures rather than just words to represent the input and output of a program. A program with a GUI runs under some windowing system (e.g. Microsoft Windows, etc.). The program displays certain icons, buttons, dialogue boxes etc. in its windows on the screen and the user controls it mainly by moving a pointer on the screen (typically controlled by a mouse) and selecting certain objects by pressing buttons on the mouse while the pointer is pointing at them.

Homepage refers to primary web page of an entity (e.g., University, department, person, etc.).

Hopping Sequence refers to the way a packet of data traverses between its source and destination.

Hot Site is a fully equipped data processing facility maintained on a standby basis for use in a business resumption operation.

Hub refers to a device within a network that accepts a signal from one point and redistributes it to one or more points.

Human Resources Records are non-payroll records related to University employees such as performance reviews, disciplinary actions, contracts, etc.

HyperText Markup Language (HTML) is code used to create Web pages/publications. These codes tell web browsers how to display the text (e.g., titles, headings, lists, etc.), link to other documents, and control character formatting (e.g., bold, italic, etc.)

Idle Time or Time-Out refers to a capability within computer systems to disconnect an authorized user if that user is logged on and has not communicated with the computer for a specified period of time (e.g., 15 minutes).

IETF conventions refers basic web development and security principles set up by the Internet Engineering Task Force (IETF) which is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Image Map is a graphical navigational tool that allows parts of an image or graphic to point to other web pages/publications.

Impacting System is a data system less essential to the accomplishment of the University mission(s) and its business functions than a data system classified as Critical but without which operations would be difficult yet not severely curtailed or impeded.

Information or Data Security refers to the development and implementation of a reasonable system of measures/controls/safeguards to protect data (regardless of the medium on which it resides (e.g., tape, cartridge, disk, hard drive, etc.) and computing resources from unauthorized access, theft, removal, misuse, disclosure, and/or corruption so that data and computing resource availability and integrity is preserved. These controls when implemented will REDUCE the PROBABILITY of something negative occurring (e.g., unauthorized file access or modification). Computer Security includes the following categories of control: Administrative (e.g., policies/procedures, personnel, and business continuity planning); Hardware; Software (e.g., network, operating and application system software); Data; Communications/ Network; Physical and Environmental; Legal (e.g., state, federal & regulatory).

In-Line Image is a graphic that appears inside a Web document.

Institutional Data is common summary and detail data that is essential to all campuses and the President's Office and is used to reflect a single organizational picture. Much of this type of data must be combined for organizational reporting to the Commonwealth or other agency.

Institutional Records are records that contain Institutional Data.

Inter-system Communications Security refers to the controls put in place to insure that communications between computer systems at different sites is private, complete and accurate, and that unauthorized access is denied.

Interference is the degradation of a wireless communication signal caused by electromagnetic radiation from another source. Such interference can either slow down a wireless transmission or completely eliminate it depending on the strength and location of the signal. Elevators, microwave ovens, cordless telephones and radioactive agents can emit interference.

Internal Records are records created by a department for use by that department's staff only, or records created by staff to carry out their University job function(s).

Internet is a network of computers that allows its users to send mail or access data worldwide.

Interoperability refers to the condition achieved among communications systems items when information or services can be exchanged directly and satisfactorily between them and/or their users.

Intranet is a private network contained within an enterprise and restricted to access from its employees.

Journaling is the process of recording access (read, changes, deletions, etc.) against data so that a previous version of the data can be reconstructed. This is also referred to as logging.

Laptop Computer is a portable personal computer of a size suitable to rest comfortably on one's legs. A laptop is smaller than a "luggable" (portable, but not comfortably) but bigger than a "palmtop" (easily carried in one hand or a shirt pocket).

Legal Discovery refers to the process by which relevant information is exchanged between parties in a lawsuit.

Legal Records are records that provide legal proof of agency authority and business transactions and the information that forms the basis for legal actions.

Levels of Risk or Degree of Risk refers to the amount of exposure and/or vulnerability associated with a particular entity such as a computer system. Examples of exposure or vulnerability include: theft; unauthorized access; unauthorized alteration or destruction of the computer system or the data stored on it; human error; natural disasters, etc.

Licensed Software is software that has been developed for commercial "sale" or for limited/restricted use. The software developer maintains copyright to the software and sells others the right to use the software for a fee. Note that the developer retains ownership of the software and controls how the software can be used.

Link refers to a one-way connection from one web page/publication to another web page/publication. A link may be a "link to" or "link from" one web page/publication to another.

Local Area Network (LAN) refers to a several computers within in the immediate area, usually the same building or floor of a building, linked together on one network. These computers are linked together on one centrally administered network and file directory.

Login Banner is a screen displayed that requests an individuals logon Id/operator id and password, and which may also display other information such as date, time, site name, phone numbers, instructions, etc.

A **Logon or Operator Id** is a unique code that identifies a specific person to the computer system. A Logon or Operator Id may also identify a type of user (e.g., Internet) to the computer system.

Low Level Formatting refers to the process whereby hardware file allocation tables are rewritten. This process completely erases a drive, one sector at a time.

Mail Bombing refers to flooding an individual's electronic mailbox with numerous or large messages with an intent to disrupt the recipient's normal work. Not only does this negatively affect the person who is being mail bombed, but everyone on the network.

Mailbox is the area in the computer in which e-mail users receive electronic mail messages.

Mainframe is a large computer, usually one to which other computers and/or terminals are connected to share its resources and computing power.

Mainframe Computer Environment is an environment in which data processing is performed centrally on a large computer system.

Medical Records are records related to the physical or mental health of an individual, regardless of category (i.e., staff, student, etc.).

Message Encryption is the scrambling of e-mail messages so that they are more secure and not easily read by anyone other than the designated recipient who has been given the "key" to unscramble the message.

Microcomputer/PC refers to a computer in which the processing unit is a microprocessor and that usually consists of a microprocessor, a storage unit, an input channel, and an output channel, all of which may be on one chip.

Multipurpose Internet Mail Extensions (MIME) is a standard for multi-part, multimedia electronic mail messages and WorldWide Web hypertext documents on the Internet. MIME provides the ability to transfer non-textual data, such as graphics, audio and fax.

Navigation Aides are tools to help you move easily through the WWW.

Network-based intrusion-detection systems monitor traffic on networks and logs suspicious behavior.

Notebook is a portable personal computer the size of a notebook.

Official Record is the primary or original version of a record maintained by the University. For example, the official record of a purchase is the purchase order filed in the campus Procurement Department. Other copies of the same purchase order are considered Convenience Records.

Official Record Custodian (ORC) is the department responsible for maintaining the Official Record of a specific document. For example, the Human Resources area is the official record custodian for staff contracts.

Official University Web Pages/Publications or Official Web Pages/Publications are those web pages/publications on University web servers which have been created by the University, its campuses, colleges, schools, departments or other administrative offices, for University business. Official web pages/publications DO NOT include, among others, web pages/publications created by individual faculty, staff, students or student organizations. Official web pages/publications shall contain the statement, "This is an Official Page/Publication of the University of Massachusetts _____ (Campus, unit name - e.g., English Department) and must

meet University guidelines/standards for design and content." Additionally, the word "Official" in the statement above will link to a page containing the following disclaimer:

As a service and for informational purposes only, the University may provide listings of and/or links to web pages/publications maintained by University faculty, staff, students, student organizations, non-University organizations and others. The University is not responsible for and does not monitor the content or administration of these pages. These pages and their content, including but not limited to factual statements and opinions, are the sole responsibility of their creators and do not represent, explicitly or implicitly, positions, policies or opinions of the University of Massachusetts.

Additionally, the campus designation in the statement above (e.g., Campus, unit) will link to the appropriate Campus' primary homepage.

Open Industry Standards are standards that can be used in software that allow the software to communicate with other products regardless of their architecture.

Operational Use Only Data - University data whose loss, corruption or unauthorized disclosure would not necessarily result in any business, financial or legal loss BUT which is made available to Data Custodian approved users only.

Packet refers to a "bundle" of information sent over network. Packets usually include information regarding where the data is being sent, the actual data, and a record indicating the end of the packet.

Packet Sniffing is a technique in which an individual inserts a software program at remote network switches or computers for the purpose of monitoring information sent over the network.

Palmtop is a portable personal computer of a size easily carried in one hand or a shirt pocket.

Parallel Testing describes a test in which historical (e.g., yesterday's) transactions are processed against the preceding day's backup files at the backup site to test agreement with transactions produced under normal operations.

A **Password** is a confidential, unique code used in conjunction with the logon id to verify that the user trying to access the computer is the person to whom the Logon/Operator ID was assigned.

Password Creation Checking is the process of a computer system comparing a user's password to words in a dictionary; user specific data such as logon id, name, birth date, social security number; and common character sequences such as "123456" or "abcdef".

Permanent Records are those records that will be kept indefinitely or at least 100 years. This designation is given to all records that the Central Administrative Services or Campus records administrator and archivist have determined as having continued historical or administrative value. Most records with a permanent retention period are transferred to the University or Campus archives when they become inactive. In a few instances, however, records with a permanent retention period are maintained in the offices of the Official Records Custodian, not the University or Campus archives.

Personal Computer (PC) is a general-purpose single-user microcomputer operated by one person at a time.

Personal Digital Assistants (PDA) are handheld computers designed as personal organizers and usually include a date book, address book, task list, and memo pad. PDA's also include synchronization of information (e.g., email) with the desktop.

Personally identifiable Information (i.e., PII) is assigned a security classification of CONFIDENTIAL and includes University data whose loss, corruption or unauthorized disclosure would be a violation of federal or state laws/regulations or University contracts. PII includes, but is not limited to:

- An individual's first name and last name or first initial and last name in combination with one or more of the following data elements: social security number, driver's license number or state-identification card number, or financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account. This information is protected under Massachusetts Law Chapter 93H.
- Individually identifiable health information (i.e., information relating to past, present or future physical or mental health or condition of an individual; provision of healthcare to an individual or payment for the provision of healthcare to an individual; Individually identifiable health information may include, but is not limited to: name, telephone/fax number, email address, social security number, driver's license number, internet address or any other unique identifying number, characteristic or code). Some, but not all, health information is protected under the Health Insurance Portability and Accountability Act of 1996 (i.e., HIPAA)
- Student education records not defined as "directory information" student directory (e.g., student number, grades, courses taken, etc.) by the University and its Campuses are protected under the Family Educational Rights and Privacy Act i.e., FERPA).
- "Customer" records such as names, addresses, phone numbers, bank and credit card account numbers, credit histories, or social security numbers as they related to student financial aid information are protected under the Graham Leach Bliley Act of 1999 (i.e., GLB).
- Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including: name; address; telephone number; social security number; date of birth; government issued driver's license or identification number; alien registration number; government passport number; employer or taxpayer identification number; unique electronic identification number; or computer's Internet Protocol address or routing code. This information is protected under the Fair and Accurate Credit Transactions Act of 2003. 16 C. F. R. § 681.

Port refers to a point at which signals can enter or leave the network en route to or from another network.

Privacy is the condition that is achieved when successfully maintaining the confidentiality of personal, student and/or employee information transmitted over a network.

Protected Information/Data is assigned a security classification of CONFIDENTIAL and includes University data whose disclosure would not result in any business, financial or legal loss BUT involves issues of personal credibility, reputation, or other issues of personal privacy. The security and protection of this data is dictated by a desire to maintain staff and student privacy. Protected data includes an individual's first name or initial and last name in combination with one or more of the following data elements: their mother's maiden name, state employee salary, electronic signature, fingerprint, photograph or computerized image, or physical characteristics or description.

Protocol is a set of formats and procedures governing the exchange of information between computer systems.

A **Public and Private Mailing List** is an e-mail address that is an alias for a list of several e-mail addresses. Some mailing lists are simple "reflectors," redirecting mail sent to them to the list of recipients. Others are filtered by humans or programs of varying degrees of sophistication; lists filtered by humans are said to be "moderated". Public lists are available to all users of a communication system, while private lists are available to specific e-mail users.

Public Domain Software is software for which the titles and copyrights have been explicitly relinquished by the author, so that anyone can use it as they please, free of charge.

Rebroadcast is to transmit or make information accessible to individuals not materially involved in the issue that the information relates to (e.g. posting the information to a newsgroup, emailing it to others, or creating a link to the information from a publicly available Web page).

Reciprocal Agreement is an agreement between two organizations whereby each organization agrees to share the other's computing facility in the event of a business disruption.

Records are any type of media (e.g., paper, punch card, audio, video, electronic, tape, disk, fiche, film, CD-ROM, etc.) containing data. These include books, papers, images, maps, photographs, financial statements, statistical tabulations, etc.

Records Administrator is the individual(s) assigned the responsibility of implementing and monitoring the records administration and management portion of the University/Campus Records Management & Retention Program. The records administrator(s) is a job function which may be part or all of an individual's area of responsibility. Additionally, the record administrator may be the same individual(s) or a different individual(s) than the records archivist.

Records Archivist is the individual(s) assigned the responsibility of implementing and monitoring the records archiving and storage portion of the University/Campus Records Management & Retention Program. The records archivist(s) is a job function which may be part or all of an individual's area of responsibility. Additionally, the record archivist may be the same individual(s) or a different individual(s) than the records administrator.

Records Conservation Board is the agency of the Commonwealth responsible for approving actions relating to the retention and disposition of state records.

Records Management involves the arrangement of information/records, the process that leads to filing information/records and the equipment/facilities in which the records are stored.

Remote Access (dial-in, network, etc.) refers to communication with a data processing facility or its systems from a remote location or facility.

Research Computers are any University computers which contain data related to faculty/staff/student research. This does not include the accounting data related to the financial functions of a research grant.

Retention Designation is the retention classification assigned to a record or group of records. Designations available are: Permanent, Until Superseded, Until Obsolete, and Specific.

Retention Period is the length of time a record must be maintained. Retention Period is based on the purposes for which the record was created, legal or contractual requirements/agreements, fiscal or administrative requirements of the University and/or interested external agencies, and the criticality of the data on the record.

Retention Standards are requirements which indicate the period of time a type of data or message should be retrievable.

Risk Analysis or Assessment is the comprehensive study of potential disruptions to business continuity, assignment of an occurrence probability, determination of probable effects, and definition of controls that could minimize or eliminate the disruption. There are two components to risk identification: knowing your assets and identifying possible risks to them.

Risk Management is the balancing potential loss against the cost of reducing or eliminating vulnerability to threats/probable disruptions.

Risk Manager is the senior level individual at each Campus and Common Administrative Services responsible for ensuring that risk analysis, control implementation, and BRP testing and updating are performed for all critical and impacting data systems at their campus/site.

Rogue access points are those installed in University facilities without coordinating with campus information security officer and network management.

Router is device that may be used to connect parts of a data network or two or more local area networks (LANs) to the network.

SATAN is a testing and reporting tool that collects a variety of information about specified hosts and networks by examining network services.

Saturation, in a communications system, refers to the condition in which a component of the system has reached its maximum message/data traffic handling capacity.

Secure Sockets Layer (SSL) is a protocol designed by Netscape Communications Corporation to provide encrypted communications on the Internet.

Secured Data refers to data that is available to authorized users who require this access to perform their job function and who have obtained Data Custodian approval for this access.

Security includes measures and controls implemented to protect data and computing resources from unauthorized access, misuse, disclosure, or corruption so that data and computing resource availability and integrity is preserved.

Server refers to computers that provide resources or information to other computers. There are many types of servers including file servers, terminal servers, and name servers.

Service Bureau is a company which provides a service related to a University function (e.g., data processing, data entry, report printing, etc.)

Service Set Identifiers (i.e., SSID) is a unique identifier attached to the header of packets sent over an 802.11 Wireless Local Area Network (i.e., WLAN). It is primarily intended to differentiate WLANs from one another.

Shareware refers to copyrighted software whose license allows the software to be freely copied and shared. The use of Shareware usually requires the payment of a fee after some time period specified in the software's license.

Signature Block is a few lines of information about the sender of an electronic mail message or news posting.

Signature Images refer to the entry of a signature on a computerized document by electronic means.

Simple Network Management Protocol (SNMP) is an application-layer protocol designed to facilitate the exchange of management information between network devices.

Simulation Testing describes a method of testing the BRP in which a business disruption is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in a simulation test. Extensive travel, moving equipment, and eliminating voice or data communications may not be practical or economically feasible during a simulated test.

Single Sign-on (SSO) is mechanism whereby a single action of user authentication and authorization can permit an authorized user to access all computers and systems where they have access permission, without the need to enter multiple logon ids/operator ids and/or passwords.

Smart Card is any plastic card (like a credit card) with an embedded integrated circuit for storing information or verifying access identity.

Spamming refers to the sending of unwanted e-mail messages to a large quantity of recipients. Spamming unduly slows down a network.

Specific is a retention designation assigned to records that will be kept for a specified number of years.

Staff refers to all non-student (faculty, professional, classified), temporary, part-time, full-time, contracted and consultants who are paid from University funds and require access to electronic data to perform their job function.

Structured Walkthrough Testing describes a method of testing the BRP in which the Resumption Team members verbally "walk through" the specific steps as documented in the plan to confirm effectiveness of the plan and identify gaps, bottlenecks or other weaknesses in the plan.

Students are all individuals enrolled at the University of Massachusetts and its programs. This includes individuals attending day, continuing education, graduate and/or undergraduate sessions who may be part-time or full-time students. (NOTE: While performing job functions related to student employment with the University, students are considered employees and must therefore abide by employee related policies).

Student Data refers to data that is created by University students.

Student Records are records related to courses, grades, housing, admissions, student disciplinary actions, non-disbursement financial aid or other academic records.

Surrogacy refers to a situation in which an authorized e-mail user has given another authorized e-mail user permission to access certain features of their mail account. The surrogate uses their own mail id to access the other user's mail features, they DO NOT use the other user's mail id. For example, a Department Head or Director may give their assistant surrogate access to their mailbox so that the assistant may screen the Department Head's or Director's mail. The assistant would access the mail system using their own electronic mail id but would be able to view the Department Head's/Director's mail.

Systems Development Life Cycle refers to the standard steps/tasks (e.g., problem definition, business plan, conceptual design, detailed design, program coding & testing, systems testing, documentation, implementation and post-implementation review) that should be followed when developing a new or modifying an existing application system.

Temporary Records are records that do not fall into the other retention designations (i.e., Permanent, Until Superseded or Specific). These records should be disposed of after 6 months from the last date of entry on the record.

Terminal refers to a device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry.

A **Third Party** in an email system refers to any individual, group of individuals, bulletin board, conference or newsgroup either within the University or at any other location worldwide who is not originally addressed in the e-mail message.

Third Party Data is any data supplied by and/or maintained for a Third Party.

Time-out or Idle Time refers to a capability within computer systems to disconnect an authorized user if that user is logged on and has not communicated with the computer for a specified period of time (e.g., 15 minutes).

Token Security refers to a network access procedure in which a token (i.e., a group of bits that serves as a symbol of authority) passes from one computer to another computer and the only computer allowed to transmit information is the one with the token.

Trace Facilities refers to methods that provide a historical record of specified events occurring in a computer system(s).

A **Transfer** is an employee “move” from one campus to another, one department/unit to another, external temp to University employee, consultant to University employee, student employee to non-student employee or a “move” from one function to a different function within the same department/unit.

Transmission Control Protocol/Internet Protocol (i.e., TCP/IP) refers to the suite of communications protocols used to connect computer systems on the Internet.

Transportable Computers refers to computer equipment that is "light weight" and easily moved. Transportable computers include laptop, notebook computers, PDAs and palm computers.

Trojan Horse, Virus, or Worm is computer code designed to self-replicate, damage, or otherwise hinder the performance of a computer's memory, file system, or software.

Tunnel refers to a protected channel that allows individuals in one organization to go through the Internet or other public network, and reach a computer in another organization in a relatively unfettered way.

Unauthorized User is any individual accessing data which is other than non-classified to which they have not been given explicit approval by a Data Custodian.

Unclassified Data is University data that does not fall into any of the other data classifications (i.e., Operational or Confidential). This data maybe made generally available without specific Data Custodian approval.

Uninterruptible Power Supply (UPS) is a device that protects computing equipment from the effects of transient power spikes/drops or temporary electrical outages.

University Data is data created, executed or received by an University employee (i.e., full or part time, temporary, professional, classified or faculty) in connection with the transaction of University business. Categories of University data are Financial, General, Medical, Personnel, Student, etc.

University Data System refers to any computerized or manual system which stores or processes University data.

University E-mail Users are all individuals who have accounts on electronic mail systems under the control and administration of the University of Massachusetts.

University of Massachusetts World-Wide Web Site or University Web Site consists of all informational pages and web based applications/databases or communications which reside on computers either purchased, leased or administered from University resources or resources managed by the University.

University or Campus Computing Infrastructure refers to the underlying technology (e.g., hardware, cabling, telecommunications and software) required to support the primary University/Campus computing and data communications environments which are usually maintained by computing centers. This does NOT include departmental computing resources (e.g., a department level computing system or network).

University Guidelines/Standards are statements designed to achieve the requirements of University Policies by establishing specific criteria that must be met in Campus Procedures.

University Policies are concise statements of direction and required action issued only by the Board of Trustees.

University Records are any records created, executed or received by an University employee (i.e., full or part time, temporary, professional, classified or faculty) in connection with the transaction of University business. Categories of University Records are Financial, General, Medical, Personnel, and Student, etc.

University Standards/Guidelines are statements designed to achieve the requirements of University Policies by establishing specific criteria that must be met in Campus Procedures.

Unofficial web pages/publications - All web pages/publications that are not official web pages/publications are unofficial web pages/publications.

Until Superseded is a retention designation assigned to records that are routinely updated or revised and where the previous version has no continuing value.

User Authentication Or Authentication is the process by which the identity of an individual and their right to access specific categories of data are verified.

User Customizability refers to the computer user's ability to tailor different software options to their specific preferences (e.g., web home page, language of choice, reply messages sent, message sorting, etc.)

Virus, Worm or Trojan Horse is computer code designed to self-replicate, damage, or otherwise hinder the performance of a computer's memory, file system, or software.

Vital Records are University records which are essential to the protection of the rights of individuals or the University's rights and assets, and/or the execution of the University's public or contractual obligations.

Web Application/Database is any computer application or database that is accessible through the Internet.

Web Application/Database Developer is any individual who is creating/developing an application and/or database on the Internet.

Web Based Communication is communication or conversation through the Internet such as "chat groups", on-line conferencing, or class discussions.

Web Browsers or Browsers are software applications that which enable a user to display and interact with text, images, videos, music and other information typically located on a Web page at a website on the World Wide Web or a local area network.

Web Consortium (W3C) is an international industry consortium whose purpose is to lead the WWW to its full potential by developing common protocols that promote its evolution and ensure its interoperability.

Web Page refers to a page of information available on the Worldwide web network.

Web Page/Publications Administrator is any individual who is responsible for the day to day monitoring and maintenance of web pages or publications. This may be the same person as the Web Page/Publications Developer.

Web Page/Publications Developer is any individual who is creating/developing a page/publication for the WWW. This may be the same person as the Web Page/Publications Administrator.

Web Page Sponsor is the head of the entity for which the web page/publication is being developed (e.g., President, Chancellor, Dean, Department Head, committee chairperson, etc.).

Web Site - a set of interconnected webpages, usually including a homepage, generally located on the same server, and prepared and maintained as a collection of information by a person, group, or organization.

Web Site/Server Administrator is any individual responsible for the support of a server attached to the Internet.

Web Server refers to a computer(s) that provides WorldWide Web (WWW) access to other computers.

Wide Area Network (WAN) refers to a geographically dispersed computer network that links multiple Local Area Networks (LANs). WANS usually cover an area larger than a single building or campus.

Wi-Fi is an industry trade name for 11 Meg 802.11b standards.

Windows registry file is a database used by the Windows operating system (e.g., Windows 2000, NT) to store configuration information.

Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks defined in the standard 802.11b. WEP is designed to provide the same level of security as that of a wired network and protect wireless communication from eavesdropping.

Wireless refers to technology that permits the transfer of information between separate points using electromagnetic waves rather than a physical connection.

Wireless Access Point (i.e., WAP) - is a piece of network hardware that serves as a communications “hub” for wireless connectivity typically providing connection to the wired local area network (i.e., LAN) and therefore transmitting data between the wireless and wired networks. Access points can be connected to the wired network allowing wireless access to the campus network and connecting via radio frequency to networked devices such as laptop computers and PDAs.

Wireless Area Network (i.e., WLAN) in essence, provides the functionality of a wired local area network without the physical constraints of the wire.

Wireless Client refers to electronic equipment such as a notebook computer or handheld PDA that use wireless radio signaling to reach a network. Wireless clients work in association with wireless access points.

Wireless Infrastructure refers to wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network.

Wireless Networking Infrastructure refers to wireless access points (i.e., WAPs), antennas, cabling, power and network hardware associated with the deployment of a wireless communications network.

Workstation is a general-purpose computer designed to be used by one person at a time and which offers higher performance than normally found in a personal computer (PC), especially with respect to graphics, processing power and the ability to carry out several tasks at the same time.

Worldwide Web (i.e., the Web or WWW) is a distributed information system that can be accessed to retrieve data in text, video or audio format.

Worm, Virus or Trojan Horse is computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software.

802.11x refers to wireless networking standards developed by the Institute of Electrical and Electronics Engineers (i.e., IEEE).