

Access-Controlled Environment – A physically secured location with appropriate environmental controls accessible only to authorized personnel with a legitimate business need.

Affiliates – Select individuals from institutions, hospitals and clinics who have been afforded contractual affiliate status by the Office of the Provost. *Affiliates* do not receive a salary from the University for the duties and services they perform.

Anti-Virus Software – Software specifically designed for the detection and prevention of known viruses. See also *Anti-Virus Updates*.

Anti-Virus Updates – Frequently released definitions that identify new viruses. These definitions are used to keep *anti-virus software* effective.

Application Administration Account – An account for the administration of an application (e.g., Oracle database administrator, MS-SQL SA administrator).

Associates – Individuals such as unpaid faculty, principal investigators, visiting scholars, dissertation special members and others who are regularly engaged in activities that directly support the teaching and research mission of the University, but are not compensated by the University by salary.

Attack – An attempt to gain unauthorized access or deny authorized access to a *university resource*.

Attacker – An entity that attempts to gain unauthorized access or deny authorized access to a *university resource*.

Authentication – The process for verifying that someone is who they claim to be. In private and public computer networks (including the Internet), authentication is commonly performed through the use of logon usernames and passwords (e.g., UANetID).

Authorization – The process of granting a person, computer process, or device access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access, which is verified through authentication.

Availability – The degree to which information and vital services are assessable for use when required.

Business Continuity – The ability to carry out vital business services in a timely manner despite loss or damage to *university resources*.

CIO – The University’s Chief Information Officer.

Compromise – An unauthorized intrusion into a *university resource* where unauthorized disclosure, modification or destruction of *confidential university data* may have occurred.

Confidentiality – The degree to which *confidential university data* are protected from unauthorized disclosure.

Confidential University Data - Personally Identifiable Information, Proprietary Information, Confidential Non-Personally Identifiable Information, and any other data the disclosure of which could cause significant harm to the University or its constituents.

- **Confidential Non-Personally Identifiable Information** - Summary information about people where the identities of individual people cannot be determined and information about University-related activities. The protection of Confidential Non-Personally Identifiable Information is governed by the University's own policies. Examples may include detailed information about some University buildings, activities or events, information about future University development plans, and grant information.
- **Personally Identifiable Information** - Information relating to an individual that reasonably identifies the individual, except where such information is public by operation of University policy or applicable law (e.g., past or present employees' names, titles, positions, fact of employment, salaries or other "directory" information pursuant to ABOR Policy 6-912 or University policy; student names, local/residence hall addresses and telephone numbers, email addresses and other "directory" information under FERPA, unless such student has requested nondisclosure consistent with FERPA and University policy). Examples may include, but are not limited to: Social Security numbers, payment card numbers, financial account information, Arizona driver license number, Arizona nonoperating identification license number (State ID card), student grades or disciplinary information, all FERPA non-directory information about students and former students, including home address and home telephone numbers, citizenship, income tax withholdings, personnel records, relatives' names and addresses, student and employee identification numbers, donations, patient health information, human subject data, information the University has promised to keep confidential, and account passwords or encryption keys used to protect access to Confidential University Data. Confidentiality of Personally Identifiable Information is largely governed by law or contract (e.g., HIPAA, FERPA, GLBA, PCI DSS, and laws governing human subject data).

- **Proprietary Information** - Data, information, or intellectual property in which the University has an exclusive legal interest or ownership right, which, if compromised could cause significant harm to the University. Examples may include, but are not limited to, business planning, financial information, trade secret, copyrighted material, and software or comparable material from a third party when the University has agreed to keep such information confidential.

Data – Information that has been translated into a form that is more convenient to move or process.

Data Facilities – Controlled facilities with a primary focus of housing servers, networking equipment and other *devices*.

Devices – Any apparatus used to access, store, transmit or interface with a university resource. This includes but is not limited to computers (servers, workstations and laptops), PDA's, printers, network appliances, devices situated behind firewalls, Network Address Translation devices, or use of Virtual Private Networks.

Disaster Recovery – The ability to restore lost or damaged data or systems in a timely manner.

Electronic Communication – Transmitting data electronically with or without human interaction (i.e. email, web, instant messaging, etc.).

Encrypted – Transformed using an algorithm to make information unreadable to anyone other than those with special knowledge, usually referred to as a key.

Encryption – The process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Firewall – A hardware or software device that limits access to a computer or network to help prevent unauthorized access. Also see *Firewall Appliance* and *Host-based Firewall Software*.

Firewall Appliance – A physical device that provides firewall protection for a network. Also see *Firewall* and *Host-based Firewall Software*.

Host-based Firewall Software – A software program that provides firewall protection for only the system that it is running. Also see *Firewall* and *Firewall Appliance*.

Incident(s) - Any event that threatens the confidentiality, integrity, or availability of university resources.

Information Security Liaison – An individual designated by Vice Presidents, Deans, Directors, Department Heads or Heads of Centers to serve as the primary contact between

the respective unit and the Information Security Office for all matters relating to information security.

Integrity – The degree to which the accuracy and completeness of information and computer software is safeguarded to protect the business process for the university.

Log – Electronic information about activity recorded by a computer during the course of operation.

NAT- Network Address Translation.

Network – A logical collection of devices and communication paths.

Networked Device – Any equipment that resides on a network.

Network Manager – See *System Administrator*.

Non-Compliance – Failure to meet or exceed standards or recommendations set by the University or by individual units.

NTS SecOps – Network Technology Solutions Security Operations.

Offsite – Located in a University-approved secure location other than in the building in which backups are performed.

Patches – Updates to operating systems and application software that enhance security and/or operability.

Personally Identifiable Information – See *Confidential University Data*.

Personal Information – An individual's first name or first initial and last name in combination with any one or more of the following data elements:

- The individual's social security number
- The individual's Arizona driver license number or non-operating identification license
- The individual's financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to the individual's financial account

Scan – A series of messages or transmissions attempting to access a device to learn what network services and information the device provides in order to identify potential weaknesses.

Security Breach – See *Compromise*.

Server - A system that provides services to others outside their local network.

Site-licensed –Licensed for use by the University at low or no cost to the user.

System Administrator - A generic term referring to any person who performs those IT administrator duties, not just those with that primary job duty. Students, faculty, staff members may be the system administrators for their own machines.

Technical Support Person – See *System Administrator*.

UIISO – University Information Security Officer.

Unit - Any university college, department, school, program, research center, business service center or other operating unit.

University – The University of Arizona.

University Network – The collection of central and outlying data, voice, and other networks that provides direct access to *university resources*.

University Resource – Data in any form and recorded in any matter and computer-related resources operated, owned or leased by the University, including but not limited to:

- Networks and network appliances
- Computers (servers, workstations and laptops)
- Printers
- Software and applications
- Thumbdrives, paper, etc.
- Any other computer-related equipment, device or hardware used to access, store, transmit or interface with another university resource

University Employee – An individual who is employed by the University under classifications "faculty," "classified staff," or "academic professional," "administrative professional," "administrative personnel," "administrator," "service professional" or "student employee" as those terms are defined in Arizona Board of Regents' Policy Manual, the University Handbook for Appointed Personnel, Classified Staff Employee Handbook or Student Employee Manual.

University-Related Persons – University students and applicants for admission, *University Employees* and applicants for employment, *Affiliates*, *Associates*, *Volunteers*, alumni, temporary employees of agencies who are assigned to work for the University, and third party contractors engaged by the University and their agents and employees.

Volunteer – An individual such as a docent, 4-H worker, event coordinator and any other individual who does not meet the criteria for affiliate or associate appointments and is not

a *university employee*. *Volunteers* perform services for the University without coercion or expectation of compensation, benefits or future employment.

VPN or Virtual Private Network –An encrypted communication channel between two computers or networks which is intended to prevent eavesdropping between the endpoints. The university offers a free sitelicensed *VPN* to all faculty, staff and students.

Vulnerability – Any flaw in the software, hardware, or configuration of a computing device that can be used to compromise the security of a *university resource*.

Vulnerability Assessment – An audit by a responsible party that is intended to identify potential vulnerabilities in a computer system or network.

Related Guidance

Information Security Policy (IS-100) and all supporting standards, procedures and guidelines

Initial Draft	5/25/06
Effective Date	5/27/08