Information Technology and Data Security - Glossary

I. Definitions

Abuse - The deliberate misuse of privileges which results in a threat to the confidentiality, availability, or integrity of information.

Account - A unique electronic identifier composed of, at minimum, a username and password.

Administrator (server) - The individual responsible for installing, maintaining, hardening, logging and reporting on the services running on a server.

Auditable Lock - A lock with logging functionality which facilitates the tracking of access and associates an individual to an unlock event.

Authentication - The act of identifying or verifying the eligibility of a user or process to access specific categories of information.

Authorization - Following authentication, the granting of access to a resource.

Availability - The property of being accessible and usable upon demand by an authorized user or system.

CISP - PCI (Cardholder Information Security Program - Payment Card Industry) –Information Security specifications developed and used by credit card companies for the purpose of ensuring and enhancing the privacy and security of financial data.

Class "A" Server - A server or technology resource which predominately provides enterprise level services to either the administrative or academic operation of the University. The failure of a Class A resource would have an immediate and adverse impact on the overall administrative or academic mission of the University. These servers and systems are listed as “Critical Systems” and managed on the critical systems list.

Class "B" Server - A server or technology resource which predominately provides either administrative or academic operation to a school or college unit within the University. The failure of a Class B resource would have an immediate and adverse impact on the overall academic or administrative operation of a school or college unit within the University.

Class "C" Server - All other servers or technology resources as listed within the ASU DNS operations. It is not likely that the failure of any Class C server or service would have an immediate and adverse impact on either the administrative or academic mission of a school or college unit within the University or otherwise impact the overall mission of the University.

Class "D" Server - A server or technology resource which has not entered a production status and is being used for testing & evaluation purposes only. Class D resources may have static IP addresses, which will be audited bi-annually. No firewall exceptions can be associated with Class D resources, with the exception of those services in which testing cannot occur without a rule (which will be evaluated on a case-by-case basis). The failure of a Class D resource would have no impact on the overall administrative or academic mission of the University.

Client (systems) - A workstation on a network.

Compromise - Unauthorized disclosure or loss of sensitive information, unauthorized information or system integrity change, or system availability interruption.

Confidential Data - Confidential data includes data that the University is required to protect under the following legal or regulatory provisions: Family Educational Rights and Privacy Act of 1974, Payment Card Industry Security Standards Council, and State of Georgia Personal Information. This includes non-public proprietary or confidential information or documents containing such information as social security number, driver's license number or state identification card number, banking account number, credit card number, debit card number, account passwords or personal identification numbers (excluding ASU IDs), education records, grades, and data defined as "restricted" and "sensitive" by the University System of Georgia Data Handling and Storage Policy.

Confidentiality - The quality or state of information that prevents disclosure or exposure to unauthorized individuals or systems.

Connectivity - The uninterrupted availability of electronic information paths.

Critical Systems - See Class "A" Server.

Data User - ASU employees who use or combine data elements in the course of their job responsibilities and/or external constituents who consume informational or data reports produced using ASU institutional data and analytics and intelligence tools. In some instances, data trustees, stewards, and managers are also data users. In other instances, ASU personnel who do not have data management responsibilities are also data users. ASU's analytic and intelligence specialists typically serve multiple roles in the data governance structure as data trustees, stewards, and managers as well as data users.

Degauss - The destruction of magnetic media through the use of a strong alternating magnetic field.

Email - Short for electronic mail, the transmission of messages over electronic communications networks.

Encryption - The use of algorithms to encode data in order to render the message or file readable only for the intended recipient.

Enterprise Network - All devices, cabling, and software which constitute the backbone network, all Local Area and Wireless Networks, and telephone networks at Albany State University.

FERPA (Family Educational Rights and Privacy Act) - A Federal law which protects the privacy of student educational records, and affords specific rights regarding the release of such records. Specific information is available from the ASU Office of the Registrar's website located here: **https://www.asurams.edu/enrollment-management/office_of_the_registrar/registrar_faq.php**

Firewall - A device or software application which forms a barrier between a secure environment and an untrusted environment.

Harden - The act of configuring a server or client, through the disabling of unnecessary services and application of safeguards, to reduce the likelihood of a system compromise.

Incident - An event that has the potential to compromise the security of a computer system or business process.

Information – Data (electronic, paper, etc.) which holds value to the organization.

Information Security - The safeguarding of information against unauthorized disclosure

Information Technology - The hardware and software operated by an organization that processes information on behalf of its stakeholders in order to accomplish a function of the organization.

Integrity - The accuracy, completeness, and validity of information in accordance with organizational values and expectations.

Interference - The degradation of a communication signal. Such interference can either slow down a transmission or completely eliminate it.

Logging - The recording of data & events for the purpose of auditing access to systems & services.

Malware - Software designed to compromise the confidentiality, availability, or integrity of the system in which it is executed. Viruses and worms are both examples of malware.

Misuse - The accidental or deliberate (abuse) use of privileges which results in a threat to the confidentiality, availability, or integrity of information.

Mitigation - The introduction of safeguards to counter a potential or actual incident.

NetID - The most common account type at Albany State University. Short for "Network Identification".

Network - An integrated, communicating aggregation of computers and peripherals linked through communication facilities.

Network Access - Connectivity which includes the backbone network, all local area and wireless networks, as well as telephone networks at Albany State University.

New Server - A server which has recently been installed and hardened, but has not entered into production status due to pending system scans or firewall rule requests.

Open Computer Lab - An Albany State University lab with computing resources available in an open environment. Open lab environments are defined as, but not limited to, those labs which are available for use by students, alumni, staff, and faculty. In addition, open computer labs are rarely used for regularly scheduled instructional courses.

Password - A word or string of characters that authenticates a user, a resource, or an access type.

Personally Identifiable Information - Per The Georgia Personal Identity Protection Act (O.C.G.A. § 10-1-911, 2010), "Personal information is an individual's first name or first initial and last name, in combination with any one or more of the following data elements:

1) Social security number
2) Driver's license number or state identification card number
3) Account number, credit card number, or debit card number, if circumstances exist
4) wherein such a number could be used without additional identifying information, access codes, or passwords;
5) Account passwords or personal identification numbers or other access codes; or
6) Any of the items contained in subparagraphs (A) through (D) of this paragraph when
7) not in connection with the individual´s first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised."

Physical Security - An aspect of information security that addresses the design, implementation, and maintenance of countermeasures that protect the physical resources of an organization. Examples include various locks, fire suppression devices, video cameras, etc.

Privacy - The condition of inaccessibility as it relates to personally identifiable information.

Process (data) - State of data in which it is being manipulated/changed by an individual, system, or application.

Public Space - Any property under control of the University. This includes but is not limited to, buildings, entrances, exits, lobbies, corridors, library shelving areas, loading docks, special storage areas, laboratories, bookstores, cashier windows, circulation desks, athletic facilities, leased properties, or help desks.

Remote Access - The ability to remotely connect into a computer via a service running on the device, versus physically at the console.

Safeguard - Protective measures prescribed to meet the security requirements of an information system. Safeguards may include technology features, management constraints, awareness training, physical security, personnel security, among other mitigating factors. Synonymous with security controls and countermeasures.

Safety and Security Function - Includes but is not limited to protection of buildings and physical grounds and monitoring and recording restricted access transactions at entrances to buildings and other areas. Usage includes but is not limited to verification of security alarms, intrusion alarms, exit door and gate controls, or panic and holdup alarms. Other usage includes but is

not limited to monitoring transit stops, parking areas, public streets, driveways, walkways, vehicle intersections, and vending areas.

Security Breach - See "compromise."

Server - A physical or virtual device which carries out some task (i.e. provides a service) on behalf of yet another piece of software called a client. This includes (but is not limited to) network-aware devices (SNMP, SMB, etc.), web servers, proxy servers, file servers, print servers, email servers, etc.

Service - A specific functionality offered/hosted by a server.

Social Media - Social media are media for social interaction, using highly accessible and scalable communication techniques. Social media is the use of web-based and mobile technologies to turn communication into interactive dialogue. Albany State University recognizes that online communication tools increasingly serve as channels for direct interaction with students, stakeholders, the public, the media and supporters of the University. The organization's commitment to transparency and collaboration encourages open and responsible communication by employees, and other University representatives by employing the use of social media providing such communications are professional, ethical and accurate, and adhere to the current campus policies for IT acceptable use and security and copyright/fair use. Students enrolling at Albany State University assume a responsibility to abide by the University's Student Code of Conduct.

Store (data) - State of data in which it is not in use, but rather it is in storage on media such as (but not limited to) hard drives, backup tapes, USB Drives, or optical media.

Tablet Computer - Mobile computer that can execute programs, has internet syncing/browsing capability, and is integrated into a flat touch screen interface display. These devices include (but are not limited to) palmtops, Apple iPads, and Android tablets such as the Motorola Xoom and Dell Streak

Technology Classroom - An Albany State University classroom with individual computing resources available to the majority of the students in the class. Technology Classrooms are used for scheduled instructional courses.

Transmit (data) - State of data while it is in route between a server and a client.

Un-cataloged Server - A server which is not included in the ongoing vulnerability scans, the upcoming risk assessment database, or does not have a documented Administrator.

User - Individuals who have been granted access to specific information assets. Users include, but are not limited to, faculty and staff, trainees, students, vendors, volunteers, contractors, or other affiliates of the institution.

Username - A unique alpha-numeric identifier associated with a specific user.

Video Monitoring Equipment - Any and all systems that are utilized in the surveillance of public spaces with the intention to capture criminal activity. Due to federal and state regulations

regarding evidence handling, these systems are required to be centrally managed by the Department of Public Safety in cooperation with the Information Security Office. This may include but is not limited to cameras, servers, storage devices, media, and reporting points.

Virtual Private Network - A private network which uses encryption and authentication to create a secure channel over untrusted networks.

Vulnerability - A weakness in a system which can be exploited to violate the system's intended behavior relative to safety, security, reliability, availability, integrity, etc.

II. Contacts

Office of Vice President of Information Technology Services & Chief Information Officer (CIO)

Information Technology Services Office of Information Security
Phone: 229-500-4357 (HelpDesk) or 229-500-2027 (Information Technology Services main office)

III. References

O.C.G.A. § 10-1-911. (2019). *Georgia Personal Identity Protection Act*. Retrieved from Code of Georgia: http://www.lexisnexis.com/hottopics/gacode/Default.asp

O.C.G.A. § 16-9-90. (2019). *Georgia Computer System Protection Act*. Retrieved from Code of Georgia: http://www.lexisnexis.com/hottopics/gacode/Default.asp

USG Information Technology Handbook, version 2.5, section 5.1, 2019:
http://www.usg.edu/information_technology_services/it_handbook/

NIST Special Publication 800-53 (Rev. 4): https://nvd.nist.gov/800-53/Rev4#

NIST Special Publications 800-171:
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

Last Update

Aug 2019