STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY

GUIDELINE 101G1: Information Technology Dictionary

VERSION NUMBER	Guideline 101G1-01
VERSION DATE	December 31, 2018
STANDARD TITLE	Information Technology (IT) Dictionary
GOVERNING POLICY	This guideline is governed by Policy 101: IT Governance, regardless of revision.
OBJECTIVE	The objective of this guideline is to define the abbreviations, acronyms, and other terms used in the State of Alabama IT governance documents (policies, standards, guidelines, procedures, etc.).
GUIDELINE	This guideline is a reference document. It defines the terms, abbreviations, and acronyms used in the State of Alabama IT governance documentation (policies, standards, guidelines, procedures, etc.). It contains no agency requirements. Agencies may use these terms as they are defined herein, or may (if required) use a revised definition when creating agency policies and procedures. This is a living document. Minor changes will be made frequently without advancing the version number, but the version date will be updated with every change. Keeping a local copy of this document is not recommended. Always refer to the version posted in the IT Governance Library (at http://oit.alabama.gov/governance-library/) to access the current version.

ACRONYMS AND ABBREVIATIONS

A B C D E F G H I J K L M N O P Q R S T U V W XYZ DEFINITIONS

- A -	
AAA	Authentication, Authorization, and Accounting
ACEE	Accessor Environment Element
ACL	Access Control List
AES	Advanced Encryption Standard
ALEA	Alabama Law Enforcement Agency
AO	Authorizing Official
AP	Access Point
AS	Authentication Server
ASP	Application Service Provider
AV	Anti-Virus

- B -	
BEM	Bid Evaluation Matrix
BIOS	Basic Input Output System
BYOD	Bring Your Own Device

- C -	
CA	Certification Authority
CAPTCHA	Completely Automated Public Turing tests to tell Computers and Humans Apart
CASB	Cloud Access Security Broker
CCB	Configuration Control Board
CDE	Cardholder Data Environment
CERT	Computer Emergency Response Team
CFR	Code of Federal Regulations
CHAP	Challenge Handshake Authentication Protocol
CI	Configuration Item
CIDR	Classless Inter-Domain Routing
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
CMDB	Configuration Management Database
CMVP	Cryptographic Module Validation Program
CPE	Customer Premise Equipment
CPU	Central Processing Unit
CSIRT	Cyber Security Incident Response Team

D -	
DAC	Discretionary Access Control
DBA	Database Administrator
DBMS	Database Management System
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DNS	Domain Name System (or Service)
DNSSEC	Domain Name System Security Extensions
DOS	Denial of Service
DSMON	Data Security Monitor
DSS	Data Security Standard

BACK TO TOP

- E -	
EFI	Extensible Firmware Interface
EPROM	Erasable Programmable Read-Only Memory

- F -	
FAR	False Acceptance Rate
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
FR	Frame Relay
FRR	False Rejection Rate
FSP	File Security Packet
FTP	File Transfer Protocol
FWSM	Firewall Services Module
FY	Fiscal Year

BACK TO TOP

- G -	
GAL	Global Access List
GDG	Generation Data Group
GID	Group Identifier

- H -	
HFS	Hierarchical File System
HIPAA	Health Information Portability and Accountability Act
HSSI	High-Speed Serial Interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transmission Protocol, Secure

BACK TO TOP

- I -	
IA	Information Assurance
ICAC	Internet Crimes Against Children
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force

IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	IP Security
IPT	IP Telephony
ISA	Internet Security and Acceleration
ISDN	Integrated Services Digital Network
ISN	Initial Sequence Number
ISO	Information Security Officer
ISP	Internet Service Provider
IT	Information Technology
ITB	Invitation to Bid
IV&V	Independent Verification and Validation

BACK TO TOP

- J -

- K -

- L -

LAN	Local Area Network
LU	Logical Unit

- M -

MAC	Mandatory Access Control
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MPLS	Multi-Protocol Label Switching
MS-ISAC	Multi-State Information Sharing and Analysis Center

BACK TO TOP

- N -

NA	Network Administrator
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NSA	National Security Agency

- O -

OIDCARD	Operator Identification Card
OIT	Office of Information Technology
OS	Operating System
OSS	Open Source Software

BACK TO TOP

- P -

PBX	Private Branch Exchange
PCI	Payment Card Industry
PDA	Personal Digital Assistant
PED	Personal Electronic Device
PHI	Protected Health Information

PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMWG	Project Management Work Group
POA&M	Plan of Action and Milestones
POMD	Personally-Owned Mobile Device
POS	Point of Sale

BACK TO TOP

- Q -

- R -

RACF	Resource Access Control Facility
RAID	Redundant Array of Independent Disks
RAS	Remote Access Server
RCP	Remote Copy; command on the Unix OS
RDA	Records Disposition Authority
RDP	Remote Desktop Protocol
RFP	Request for Proposal
RMF	Risk Management Framework
ROM	Read-Only Memory
RRMP	Residual Risk Mitigation Plan
RSA	An encryption algorithm named after its creators: Rivest, Shamir, and Adleman;
RSA	Retirement Systems of Alabama
RSH	Remote Shell
RSN	Robust Security Network
RTU	Root of Trust for Update

BACK TO TOP

- S -

SA	System Administrator
SAISO	Senior Agency Information Security Officer
SAN	Storage Area Network
SCP	Secure Copy; command on the Unix OS
SCSI	Small Computer System Interface
SDLC	System Development Life Cycle
SE	Secure Erase®
SFTP	Secure FTP
SIP	Session Initiated Protocol
SME	Subject Matter Expert
SP	Software Programmer
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SSLF	Specialized Security – Limited Functionality
STIG	Security Technical Implementation Guide
SYN	Synchronize (packet in TCP)

BACK TO TOP

- T -	
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSIG	Transaction Signature
TSO	Time Sharing Option

- U -	
UCE	Unsolicited Commercial Email
UEFI	Unified Extensible Firmware Interface
UID	User Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus

- V -	
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRF	VPN Routing and Forwarding
VTC	Video Tele-Conferencing

- W -	
WAN	Wide Area Network
WD	Web Developer
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

- X -	
XML	Extensible Markup Language

- Y -

- Z -

BACK TO TOP

DEFINITIONS

A B C D E F G H I J K L M N O P Q R S T U V W XYZ ACRONYMS

- A -

ACCESS CONTROL: Enable authorized use of a resource while preventing unauthorized use or use in an unauthorized manner.

ACCOUNTABILITY: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

ADVANCED ENCRYPTION STANDARD (AES): AES is a symmetric block cipher algorithm using cryptographic key sizes of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. WPA2 is an implementation of AES.

AGENCY: Includes departments, agencies, offices, boards, commissions, bureaus, authorities and authorized individuals in the employment of the state.

ASSURANCE: Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. “Adequately met” includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass.

ASYMMETRIC CRYPTOSYSTEM: A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (public-key encryption).

AUTHENTICATION: Verifying the identity of a subject requesting the use of a system and/or access to a resource.

AUTHORIZATION: The granting or denying of access rights to a user, program, or process.

AVAILABILITY: The property of being accessible and usable upon demand by an authorized entity.

BACK TO TOP

- B -

BIOMETRIC TEMPLATE: The digital representation of information captured during enrollment.

BIOS: Refers collectively to boot firmware based on the conventional BIOS, Extensible Firmware Interface (EFI), and the Unified Extensible Firmware Interface (UEFI).

BYPASS: When someone circumvents one or more components of the biometric system, most probably the capture device because it is outside the perimeter of the protected system or area. An attacker might compromise the capture hardware or wiring to send electronic or digital representations of biometric data directly to the comparator without first presenting a sample to the capture device.

BACK TO TOP

- C -

CAPTCHA: Completely Automated Public Turing tests to tell Computers and Humans Apart; a type of challenge-response test used in computing as an attempt to ensure that the response is generated by a person.

CAPTURE: Biometric technology is used to record a user's physical characteristic or behavior. The hardware performing the reading is called the *capture device*. Capture devices typically are designed to capture one biometric characteristic such as a finger print, retina pattern or keyboard dynamic.

CHAP: Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function.

CLASSLESS INTER-DOMAIN ROUTING (CIDR): An IP addressing scheme that replaces the scheme based on classes A, B, and C. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations. CIDR was created to help reduce problems associated with IP address depletion.

CLEAR: Clearing is the process of eradicating the data on media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing.

CLOUD-BASED FILE STORAGE AND SHARING SERVICE: A commercial service in which a user is allotted storage space on a remote server where access to the server is carried out over a network, such as the Internet.

COLLATERAL INFORMATION: Information that is in the workspace that is not meeting or conference related but can be seen by the camera or heard by the microphone. Collateral information can also be non-meeting/conference related information on a PC workstation that is used to participate in, or present to, a conference.

CONFIDENTIALITY: A concept that applies to data that must be held in confidence and describes the status or degree of protection that must be provided for such data.

CONFIGURATION ITEM (CI): A product that is placed under configuration management. Such products may include hardware components, software components, documentation, or any other item that needs to be controlled.

CONFIGURATION MANAGEMENT (CM): From an information security point of view, configuration management is a process that provides assurance that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications,

CONTAINER SOLUTION: A software solution that can separate personal applications and data from state applications and data.

COOKIES: Small text files which a web server may ask the web browser to store and send back to the web server when needed. Cookies may be used to store a transaction identifier or other information a user may provide.

CUSTOM SOFTWARE: Software that is developed for a specific user, a group of users, or for an organization. Typically, custom software does not require a license to use, but may require a maintenance agreement for modifications or upgrades.

CYBER SECURITY INCIDENT: An assessed occurrence having actual impact (i.e., damage is done, access is achieved by an intruder, loss occurs, or malicious code is implanted), or potentially adverse effects on an information system (e.g., when detecting something noteworthy or unusual such as a new traffic pattern, new type of malicious code, a source of persistent attacks, or evidence of inappropriate use having the potential to impact the organization).

BACK TO TOP

- D -

DENIAL OF SERVICE (DOS): The prevention of authorized access to resources or the delaying of time-critical operations (time-critical may be milliseconds or it may be hours, depending upon the service provided).

DENIAL OF SERVICE ATTACK: Multiple service requests sent to a victim's computer until it eventually overwhelms the system causing it to freeze, reboot, and ultimately not be able to carry out regular tasks.

DES: Cryptographic algorithm designed for the protection of unclassified data and published by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standard (FIPS) Publication 46. DES only supports key lengths of 56 bits which is considered inadequate.

DIGITAL FORENSICS: The application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.

DOMAIN NAME: A domain name is all the text that follows the first period '.' in a host name. A host name is used to locate an entity on the Internet. A host name is part of a Uniform Resource Locator (URL), which is the address of a site or document on the Internet.

DUAL HOMING: Network topology in which a device is connected to the network by way of two independent access points.

BACK TO TOP

- E -

ELECTRONIC DEVICE: Any device that requires software for it operation, and has the capability to transfer, transmit, capture, receive, or stare data. Examples include, but are not limited to, desktops, personal computers, laptops, notebooks, notepads, handhelds, and smart phones.

EMPLOYEE: Individual in the employment of the State of Alabama, to include contract staff.

ENCRYPTION: The translation of data into a secret code; the process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge (usually referred to as a key).

END OF SUPPORT: Refers to the time in a product's lifecycle when the vendor no longer provides automatic fixes, updates, security patches, and other technical assistance.

ENROLLMENT: The initial association of an identity with a biometric characteristic.

EXTENSIBLE FIRMWARE INTERFACE (EFI): A specification for the interface between the operating system and the platform firmware. [see BIOS]

BACK TO TOP

- F -

FILE: Includes, but is not limited to, word processing documents, spreadsheets, email, office productivity application, images of reports, screens, and all other forms of electronic data.

FIRMWARE: Software that is included in read-only memory (ROM).

FREEWARE (or SHAREWARE): A variety of software typically available on the Internet that is available free-or-charge to can be downloaded to your computer. May also include other software available from

other electronic sources; however, it may require the user to obtain a license for its use, sometimes for a fee.

BACK TO TOP

- G -

GAMBLING: Sites that cater to gambling activities such as betting, lotteries, casinos, including gaming information, instruction, and statistics.

GAMES: Sites that provide information about or promote electronic games, video games, computer games, role-playing games, or online games. Includes sweepstakes and giveaways. Sport games are not included in this category, but time consuming mathematic game sites that serve little education purpose are included in this category.

GOVERNANCE: The set of responsibilities and practices exercised by executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that organization's resources are used responsibly.

GUIDELINE: A collection of system specific or procedural specific "suggestions" for best practice; not required, but strongly recommended.

BACK TO TOP

- H -

HASH ALGORITHM (or HASH FUNCTION): A function that maps a bit string of arbitrary length to a fixed length bit string.

HOSTED: A computer, an application, or data running on another computer (the host) and accessible by means of a network connection.

HYPERTEXT LINK: Element on a Web page (text, image, or file) that when clicked opens another Web page or jumps to another location.

BACK TO TOP

- I -

IDENTIFYING INFORMATION: Any information used either alone or in conjunction with other information that specifically identifies a person or a person's property, and includes, but is not limited to, any of the following information related to a person:

- Name
- Date of birth
- Social Security number
- Driver's license number
- Financial services account numbers, including checking and savings accounts
- Credit or debit card numbers
- Personal identification numbers (PIN)
- Electronic identification codes
- Automated or electronic signatures
- Biometric data
- Fingerprints
- Passwords
- Parent's legal surname prior to marriage

- Any other numbers or information that can be used to access a person's financial resources, obtain identification, act as identification, or obtain goods or services

[SOURCE: *The Code of Alabama, Section 13A-8-191 (Act 2001-312, p. 399, §2)*]

IEEE 802.11i: The security specification of the 802.11 standard consisting of two components: IEEE 802.1x and Robust Security Network (RSN). RSN is used to establish a secure wireless connection between wireless devices. RSN uses dynamic negotiation of authentication and encryption algorithms between access points and wireless devices. The authentication schemes are based on IEEE 802.1x and EAP with Advanced Encryption Standard (AES) as the encryption algorithm

INDIVIDUAL ACCESS CONTROLS: Methods of electronically protecting files from being accessed by people other than those specifically designated by the owner.

INDIVIDUAL IDENTIFIER: Information associated with a single individual and used to distinguish him or her from other individuals.

INFORMATION OWNER: Individual, or group of individuals, responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be. Responsibility for implementing security measures may be delegated, though accountability remains with the identified owner of the asset.

INTEGRATED SERVICES DIGITAL NETWORK (ISDN): A circuit-switched telephone network system that allows digital transmission of voice and data over ordinary telephone copper wires.

INTEGRITY: The property that data or information has not been modified or altered in an unauthorized manner.

IP SCANNING: Searching a range of computer addresses to identify which are active; useful for mapping a network but also a common precursor to an attack.

IP SPOOFING: Forging the source IP address on a TCP/IP packet in order to hide the source of a message; can be used to exploit applications that use authentication based on IP addresses.

IPSEC: Internet Protocol Security (IPSEC) is a framework for a set of protocols for security at the network or packet processing layer of network communication designed to provide private communications over public networks.

BACK TO TOP

- J -

- K -

KEY: In cryptography, a sequence of symbols that is used with a cryptographic algorithm for encrypting or decrypting data. See PRIVATE KEY and PUBLIC KEY.

BACK TO TOP

- L -

LEAST PRIVILEGE: The security principle of granting users only those accesses they need to perform their official duties.

LICENSED SOFTWARE: Software for which the end-user or organization is granted permission to use one or more copies of software in ways where such a use would otherwise potentially constitute copyright infringement of the software owner's exclusive rights under copyright law.

LIVE SAMPLE: The digital representation of information captured during verification.

LOG: A record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network.

BACK TO TOP

- M -

MALICIOUS WEBSITES: Sites that host software that is covertly downloaded to a user's machine to collect information and monitor user activity, and sites that are infected with destructive or malicious software, specifically designed to damage, disrupt, attack, or manipulate computer systems without the user's consent, such as virus or Trojan horse.

MALWARE: Short for malicious software (such as a virus or Trojan horse); software designed specifically to damage or disrupt a system.

MEDIA: Refers to different types of data storage options including but not limited to paper, microforms, hand-held devices (cell phones, personal digital assistants, palm devices), networking devices, floppies, hard drives, USB removable devices with or without hard drives (including pen drives, thumb drives, flash drives, memory sticks), ZIP disks, magnetic tapes, optical disks, and memory.

MOBILE CODE: Software obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient.

MOBILE DEVICE: Any portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g. wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile device may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in feature for synchronizing local data with remote locations. Examples include smart phone and tablets

BACK TO TOP

- N -

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST): A non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

NON-DISCLOSURE AGREEMENT (NDA): A legal contract between at least two parties outlining sensitive or confidential materials the parties wish to share with one another for certain purposes, but wish to restrict from generalized use. In other words, it is a contract through which the parties agree not to disclose information covered by the agreement.

NON-REPUDIATION: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity so neither can later dent having processed the data.

BACK TO TOP

- O -

OFFICE OF INFORMATION TECHNOLOGY (OIT): An office of the State of Alabama, formed through the passage of Senate Bill 117, to focus on three statutory mandates: IT Strategic Planning, IT Governance, and IT Resource Utilization.

BACK TO TOP

- P -

PACKET SNIFFING: A form of wire-tap applied to computer networks; a technique for collecting information that can be used to attack the network.

PASSPHRASE: A sequence of words or other text used to control access to a computer system, program or data; similar to a password in usage, but generally longer for added security and easier to remember because it's based on words or a phrase that means something to the user.

PEER-TO-PEER FILE SHARING: Websites that allow users to share files and data storage between each other.

PERSONAL DIGITAL ASSISTANT (PDA): Small handheld devices combining computing, telephone/fax, Internet and networking features (see PORTABLE DEVICE).

PERSONAL ELECTRONIC DEVICE (PED): Any device that requires software for its operations. Examples include, but are not limited to, laptops, notebooks, notepads, handhelds, and smart phone.

PERSONALLY IDENTIFIABLE INFORMATION (PII): Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

PERSONALLY-OWNED MOBILE DEVICE (POMD): Any Mobile Device owned and used by a State of Alabama employee or contractor to conduct state business and/or access the state network.

PERSONNEL SECURITY: A family of operational safeguards that consider an individual's background, qualifications, and operational restrictions prior to granting the individual access to protected information and information systems.

PHISHING: Counterfeit web pages that duplicate legitimate business web pages for the purpose of eliciting financial, personal or other private information from the users.

PICONET: An ad-hoc computer network of devices using Bluetooth technology protocols to allow one master device to interconnect with up to seven active slave devices.

PII ELECTRONIC RECORD: Any item, collection, or grouping of information in electronic form that associates personal information such as education, financial transactions, medical history, criminal or employment history, with an individual identifier. Also any item, collection, or grouping of information in electronic form that associates two or more individual identifiers. Electronic records that contain information about education, financial transactions, medical history, or criminal or employment history but do not include individual identifiers are not considered PII electronic records.

POLICY: The overall expression of management's intention on how security should be implemented, maintained, and enforced. Policies are usually point-specific, covering a single area, and outline specific responsibilities that must be met.

PORT SCANNING: Examining a range of computer ports to identify which are open; a common precursor to an attack.

PORTABLE DEVICE: Transportable or hand-held communication or smart phone device (such as Blackberry, Treo, iPhone, iPad) and any other type of device with similar inherent features. Could also refer to portable *storage* devices such as USB drives, thumb drives, digital cameras, etc.

PRIVATE KEY: In public key cryptography, a key that is known only to its owner. Contrast with public key.

PROCEDURE: A set of instructions or methods for performing a specific task or function. One or more procedures may support the implementation of a security policy.

PROJECT (IT PROJECT): a temporary endeavor undertaken to create a product, service, or result that is IT enabled. A project may be staffed by state or contract personnel.

PROJECT BUSINESS CASE: captures the reason and justification for a project. The business case will demonstrate the business need, explain the proposed resolution, and consider the strategic alignment with the state's goals and policies. The cost benefit analysis is included in the business case.

PROJECT CLOSURE REPORT: An instrument prepared by the project manager or his/her designee at the conclusion of an IT project; contains key metrics, best practices, lessons learned, and other valuable information about the project; the IT Project Closure Report must be prepared and submitted to OIT as a part of project cessation.

PROJECT INITIATION PACKET: a packet consisting of one or more documents including the Project Request Form and the Business Case and Cost Benefit Analysis. This packet is to be submitted to OIT for project governance.

PROJECT MANAGEMENT WORK GROUP (PMWG): A committee of state agency IT professionals tasked with developing an IT governance framework for the state.

PROJECT REQUEST: provides basic information and description about the project.

PROJECT STATUS REPORT: An assessment report during a project that conveys details such as what tasks have been accomplished, what resources have been expended, what issues and risks have been encountered, and whether the project is expected to be completed on time and within budget. Project Status Reports are used by OIT to determine whether changes are necessary to an ongoing effort.

PROXY: A server or device that acts as an intermediary between systems (between a user and the Internet for example, as a way to hide the IP address and other data of the user by replacing it with that of the proxy).

PROXY AVOIDANCE: Websites that provide information or tools on how to bypass Internet access controls and browse the Web anonymously, includes anonymous proxy servers.

PUBLIC KEY: In public key cryptography, a key that is made available to everyone. Contrast with private key.

PUBLIC KEY CRYPTOGRAPHY: Cryptography in which public keys and private keys are used for encryption and decryption. One party uses a common public key and the other party uses a secret private key. The keys are complementary in that if one is used to encrypt data, the other can be used to decrypt it.

PURGE: Purging is the process of removing the data from media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was on the media before purging. The goal is to destroy the data beyond forensic recovery.

PUSH EMAIL: A delivery system with real-time capability to "push" email through to the client device as soon as it arrives, rather than requiring the client to poll and collect or pull mail manually.

BACK TO TOP

- Q -

- R -

RADIUS: Remote Authentication Dial-In User Service, RADIUS, is an authentication, authorization, and accounting (AAA) protocol for network access application.

REDUNDANT ARRAY OF INDEPENDENT DISKS (RAID): A method of storing data on multiple hard disks. When disks are arranged in a RAID configuration, the computer sees them all as one large disk. Placing data on multiple disks improves input/output performance and increases fault tolerance.

REPLAY ATTACK: When someone is able to capture a valid user's biometric data and then use it at a later time for authorized access. The attacker may obtain the biometric data from the stored biometric template or as it is being transmitted from one element of the biometric system to another.

REMEDIATION DATABASE: A database of vulnerability patches, instructions, workarounds, etc. that need to be applied within the organization. Enterprise patch management tools usually supply such a database, but there may be a need to manually maintain a separate one for IT technologies not supported by the patch management tool.

RISK: The net mission/business impact considering (1) the likelihood that a particular threat source will exploit or trigger a particular information system vulnerability and (2) the resulting impact if this should occur. IT-related risks arise from legal liability or mission/business loss due to, but not limited to:

- Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information.
- Non-malicious errors and omissions.
- IT disruptions due to natural or man-made disasters.
- Failure to exercise due care/diligence in the implementation and operation of the IT resource.

RISK ANALYSIS: The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.

RISK MANAGEMENT: The ongoing process of assessing the risk to mission/business as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate, cost-effective controls to achieve and maintain an acceptable level or risk.

RISK MANAGEMENT FRAMEWORK (RMF): a structured process that integrates risk management activities into the system development life cycle (SDLC). [see NIST Special Publication 800-37]

RSA: An asymmetric key encryption algorithm based on factoring very large integers. Asymmetric algorithm keys must be longer for equivalent resistance to attack than symmetric algorithm keys. 1024-bit RSA keys are equivalent in strength to 80-bit symmetric keys, 2048-bit RSA keys to 112-bit symmetric keys and 3072-bit RSA keys to 128-bit symmetric keys. RSA are the initials of the three algorithm creators: Rivest, Shamir, and Adleman.

BACK TO TOP

- S -

SCATTER-NET: A set of piconets connected through sharing devices.

SECURE ERASE (SE): A data-destroy command amounting to “electronic data shredding.” SE is built into the hard disk drive itself and is implemented in all ATA interface drives with capacities greater than 15 GB manufactured after 2001. Executing the SE command causes a drive to internally completely erase all possible user data record areas by overwriting with binary zeroes. On solid state drives, cells are marked as empty, restoring the drive to factory default.

SECURE SHELL (SSH): A computer program and an associated network protocol designed for logging into and executing commands on a networked computer; providing secure encrypted communications between two untrusted hosts over a non-secure network. SSH is most commonly used in combination with SFTP, as a secure alternative to FTP or in combination with SCP, as a secure alternative to RCP file transfers in Unix environments.

SECURITY CONTROLS: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Security controls are defined in NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems.

SECURITY PLAN: A document identifying the system, the sensitivity of information handled by the system, and system security measures including operational, technical, and management controls, system rules of behavior, risk assessment, and any security awareness and training requirements.

SEPARATION OF DUTIES: Dividing roles and responsibilities so that a single individual cannot subvert a critical process.

SHAREWARE: (see FREEWARE)

SOCIAL ENGINEERING: The art of getting people to do things they would not ordinarily do for someone they do not know (such as giving someone their password). Common social engineering methods include posing as a new employee seeking help or as a vendor or employee of a partner company. Common targets of social engineers are receptionists and administrative assistants because they are predisposed to being helpful.

SOFTPHONE: Systems which implement VoIP using an ordinary PC with a headset and special software.

SPAM: Spam is any kind of unwanted online communication, most commonly in the form of unwanted or unsolicited email.

SPAM URLs: Websites or web pages whose URLs are found in spam emails.

SPLIT TUNNELING: Term used to describe a multiple-branch networking path. In a VPN context, a secure tunnel is established to the VPN concentrator and other traffic is sent directly to different remote locations without passing through the VPN concentrator. This can expose the state’s networked resources to attack and can make state resources accessible to anyone from non-trusted networks.

SPYWARE: Secret code hidden in an otherwise harmless program. Spyware permits unauthorized access to a computer, allowing someone else to observe the user, read data, or even control the computer.

SQL INJECTION: A type of security exploit in which the attacker adds Structured Query Language (SQL) code to a Web form input box to gain access to resources or make changes to data.

SSL VPN: Secure Sockets Layer (SSL) Virtual Private Network (VPN) is a form of VPN that can be used with a standard Web browser. In contrast to the IPSEC VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer.

STANDARD: A collection of system-specific or subject-specific requirements that must be met by everyone subject to the source policy. For example, a policy may address the high-level responsibilities for network/system authentication, whereas one or more standards would address the specific requirements for different methods of authentication.

STATEFUL: Having the capability to maintain the last-known or current status or condition of a process or application.

STATE NETWORK: Any compute, data, wireless, or telecommunications network provided or operated by any agency of the State of Alabama, which allows electronic devices to transmit or receive electronic media or data. Internet access and email service networks are included.

SUPPORTED SOFTWARE: Software products that receive automatic fixes, updates, security patches, and/or technical assistance from the vendor.

SYMMETRIC CRYPTOSYSTEM: A method of encryption in which the same key is used for both encryption and decryption of the data (secret key encryption).

SYSTEM INTERCONNECTION: The direct connection of two or more IT systems for the purpose of sharing data and other information resources.

SYSTEM DEVELOPMENT LIFE-CYCLE: A circular process model based on the concept that a mission need is defined and translated into an advantageous solution, which goes through a continuous loop of evolution and improvement until it is retired. There are five basic phases of the system development life cycle:

- Initiation,
- Development/acquisition,
- Implementation,
- Operation/maintenance, and
- Disposition.

See NIST Special Publication 800-14: *Generally Accepted Principles and Practices for Securing Information Technology Systems*)

BACK TO TOP

- T -

THREAT: Any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats arise from human actions and natural events.

THREAT SOURCE: Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) the situation and method that may accidentally trigger a vulnerability.

THRESHOLD: the minimum requirements for establishing OIT governance.

TRACEABILITY: The ability to chronologically interrelate uniquely identifiable entities in a way that is verifiable.

TRIAL (or EVALUATION) SOFTWARE: Software products for which there is a specified timeframe in which the user has to evaluate the program before deciding to purchase. These may be either limited function versions of a program, or in some cases, fully functional versions of the program.

TRIPLE DES: Block cipher formed from the DES cipher by using it three times. Triple DES is also known as TDES or 3DES, however, there are variations of TDES which use two different keys (2TDES) and three different keys (3TDES) therefore the non-standard abbreviation 3DES is considered confusing and should be avoided. In general TDES with three different keys (3TDES) has a key length of 168 bits: three 56-bit DES keys (with parity bits 3TDES has the total storage length of 192 bits), but due to the meet-in-the-middle attack the effective security it provides is only 112 bits. 2TDES is weaker and not recommended because two of the three keys used are identical.

BACK TO TOP

- U -

UNIFIED EXTENSIBLE FIRMWARE INTERFACE (UEFI): A possible replacement for the conventional BIOS that is becoming widely deployed in new x86-based computer systems. The UEFI specifications were preceded by the EFI specifications. [see BIOS]

UNSUPPORTED SOFTWARE: Software products that no longer, or never, received automatic fixes, updates, security patches, and online technical assistance for the vendor.

USER: A person who requires the services of a computing system.

BACK TO TOP

- V -

VIRTUALIZATION: The creation of a virtual (rather than actual) version of something, such as a hardware platform, operating system (OS), storage device, or network resource.

VIRTUAL PRIVATE NETWORK (VPN): Protected information system link utilizing tunneling, security controls, and end-point address translation giving the impression of a dedicated line.

VOICE OVER INTERNET PROTOCOL (VoIP): Also referred to as IP Telephony, Internet telephony, Broadband telephony, Broadband Phone, and Voice over Broadband, is the routing of voice conversations over the Internet or through any other IP-based network.

VULNERABILITY: A weakness in system security requirements, design, implementation, or operation, that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.

BACK TO TOP

- W -

WAIVER: a request to omit or delay a requirement in the IT project governance process, granted by the Secretary of Information Technology.

WIRED EQUIVALENT PRIVACY (WEP): A security protocol used for encrypting wireless network transmissions; superseded by WPA, WEP is regarded as being insufficiently secure and should not be used.

WPA2: Wi-Fi Protected Access (WPA) is used to secure wireless computer networks. WPA2 implements the full IEEE 802.11i standard and replaces WEP.

BACK TO TOP

- X -

- Y -

- Z -

ZEROIZATION: A method of erasing electronically stored data, cryptographic keys, and critical security parameters by altering or deleting the contents of the data storage to prevent recovery of the data.

BACK TO TOP

SUPPORTING DOCUMENTS

The following document supports this guideline:

- Policy 101: IT Governance

EFFECTIVE DATE

This guideline shall be effective upon its approval by the Secretary of Information Technology, as evidenced by the signature of the Secretary being affixed hereto.

SUPERSEDES

This guideline supersedes ISD reference document ITD-07: IT Dictionary, which is hereby rescinded.

The undersigned, as Acting Secretary of Information Technology of the State of Alabama, exercising the power vested in that Office by the laws of this state, declares this guideline to be adopted as of the 29th day of January, 2019.

Jim Purcell
Acting Secretary of Information Technology

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
101G1-01	12/31/2018	Initial version