



Cyber Security Policies, Standards and Guidelines Definitions & Acronyms

Original Publication Date: February 12, 2010

Revision Date: September 24, 2010

**Thomas D. Smith
Director
New York State
Office of Cyber Security
30 South Pearl Street
Albany, N.Y. 12207-3425**

DEFINITIONS & ACRONYMS

Approved Storage Facility: Office for Technology (OFT) *data* centers, *SE* physically secured central servers/*data* centers, and other facilities as approved in writing by *SE* executive management, upon recommendation of the *SE ISO*. These facilities include their internal *data* communication networks.

Authentication: The process to establish and prove the validity of a claimed *identity*.

Authorization: The granting of rights, which includes the granting of access based on an authenticated *identity*.

Availability: The extent to which *information* is operational, accessible, functional and usable upon demand by an authorized entity (e.g., a *system* or *user*).

Biometric Data: Unique physical or behavioral characteristics, such as fingerprints or voice patterns, used as a means of verifying personal *identity*.

Botnet: A collection of compromised computers centrally controlled by an attacker.

Business Risk: This is the combination of *sensitivity*, *threat* and *vulnerability*.

CIO: Chief Information Officer.

Classification: The designation given to *information* from a defined category on the basis of its *sensitivity*.

Compensating Controls: Alternative safeguards or countermeasures that accomplish the intent of the original security control.

Confidentiality: The property that *information* is not made available or disclosed to unauthorized individuals, entities, or processes.

Consumer Reporting Agency: Any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit *information* or other *information* on consumers for the purpose of furnishing consumer reports to *third parties*, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the *State* Attorney General and furnished upon request to *State Entities* required to make a notification under this Policy.

Controls: Countermeasures or safeguards that are the devices or mechanisms that are needed to meet the requirements of policy.

Copyright: A property right in an original work of authorship fixed in any tangible medium of expression, giving the holder the exclusive right to reproduce, adapt, distribute, perform and display the work (*Black's Law Dictionary, 7th ed. 1999*).

CPE: Continuing Professional Education.

Cryptographic: Relating to a method of storing and transmitting *data* in a form that only those it is intended for can read and process.

Cryptographic Key: A binary number used by an *encryption* algorithm to perform calculations.

Data: See *Information*.

Data at Rest: A term used to describe *data* stored on electronic media but excludes any *data* while traversing a network. *Data at rest* includes but is not limited to archived *data*, files stored on a disc, DASD, or hard drives, USB thumb drives, files stored on backup tape and disks and also files stored off-site or on a storage area network (SAN).

Data in Transit: A term used to describe *data* that is being transferred on a network, either on wire, fiber, air waves or any other network connection not involving storage media.

Denial of Service (DoS): An attack that takes up so much of the company's business resource that it results in degradation of performance or loss of access to the company's business services or resources.

Disaster: A condition in which *information* is unavailable, as a result of a natural or man-made occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of the *SE's* business objectives as determined by *SE's* management.

DMZ: Demilitarized zone; a semi-secured buffer or region between two networks such as between the public *Internet* and the trusted private *State* network.

DNS: An internet service that translates domain names into IP addresses.

Electronic Storage Media: Media used to record and store *data*, including, but not limited to hard drives, tapes, removable drives of any kind, flash drives or other USB storage media, CDs, diskettes, etc..

Encryption: The *cryptographic* transformation of *data* to render it unintelligible through an algorithmic process using a *cryptographic key*.

Field Level Encryption: Protects *data* by encrypting *data* in certain fields of a database.

File Level Encryption: Protects *data* by encrypting *data* on a file by file basis.

Firewall: A security mechanism that creates a barrier between an internal network and an external network.

Folder Level Encryption: Protects *data* by encrypting *data* on a folder by folder basis.

Full Disk Encryption: Software or hardware which encrypts all user *data* that resides on a disk along with sensitive operating system files.

Guideline: Non-mandatory suggested course of action.

Host: A *system* or computer that contains business and/or operational software and/or *data*.

Identity: A set of attributes for a person.

Incident: Any adverse event that threatens the *confidentiality*, *integrity* or *availability* of *information* resources.

Incident Response: The manual and automated *procedures* used to respond to reported network intrusions (real or suspected); network failures and errors; and other undesirable events.

Information: Any representation of facts, concepts or instructions created, stored (in temporary or permanent form), filed, produced or reproduced, regardless of the form or media. This may include, but is not limited to the *data* contained in reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic or hard copy.

Information Assets: All categories of *information* (automated and non-automated), including (but not limited to) *data* contained in records, files, and databases. See *Information*.

Information Custodian: An individual, organizational unit (e.g., IT, Operations, *Systems*, Network) or entity (e.g., Office for Technology) acting as caretaker of *information* on behalf of its owner.

Information Owner: An individual or a group of individuals that has responsibility for making *classification* and *control* decisions regarding use of *information*. See Part 2 of Information Security Policy P03-002, Organizational and Functional Responsibilities.

Information Security: The concepts, techniques and measures used to protect *information* from accidental or intentional *unauthorized access*, modification, destruction, disclosure or temporary or permanent loss (See *Availability*).

Information Security Architecture: A framework designed to ensure *information security*. Principles are defined and integrated into business and IT processes in a consistent manner.

Information Technology Equipment: Includes, but is not limited to, personal computer workstations, laptops, *PDA*s, mainframes, servers, fax machines, copiers, printers and other electronic devices used to input, store, process and output *information*.

Integrity: The property that *data* has not been altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.

Intranet: An internal (i.e., non-public) network that uses the same technology and protocols as the *Internet*.

Internet: A *system* of linked computer networks, international in scope, that facilitate *data* transmission and exchange, which all use the *standard Internet* protocol, TCP/IP, to communicate and share *data* with each other.

Intrusion Detection: The monitoring of network activities, primarily through automated measures, to detect, log and report upon actual or suspected unauthorized access and events for investigation and resolution.

ISO: Information Security Officer.

Least Privilege: *User*, program or process is granted only the access they specifically need to perform their business task and no more.

Malicious Code: *Malicious code* refers to code that is written intentionally to carry out annoying, harmful actions or use up the resources of a target *host*. They sometime masquerade as useful software or are embedded into useful programs, so that *users* are induced into activating them. Types of *malicious code* include *Trojan horses* and *viruses*.

Media Access Control (MAC) address: A hardware address that uniquely identifies each node of a network.

Merging: The process of combining different sources of *information* into a new source of *information*.

Multi-User System: Refers to computer *systems* that support two or more simultaneous *users*. All mainframes, servers and microcomputers are *multi-user systems*, but most personal computers, laptops and workstations are not.

Need to Know/Need to Do: see *Least Privilege*.

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 (e.g., betty was smoking tires and playing tuna fish).

PDA: see *Personal Digital Assistant*.

Penetration Testing: The portion of security testing in which evaluators attempt to exploit physical, network, *system* or application weaknesses to prove whether these weaknesses can be exploited by gaining extended, unauthorized or elevated privileged access to protected resources.

Personal Digital Assistant (PDA): A small portable device, such as a Palm Pilot or Blackberry, which combines computing, telephone/fax and networking features. Also called palmtop, handheld and pocket PC.

Personal, Private, or Sensitive Information (PPSI): Any *information* where *unauthorized access*, disclosure, modification, destruction or disruption of access to or use of such *information* could severely impact the *SE*, its critical functions, its employees, its customers, *third parties*, or citizens of New York . This term shall be deemed to include, but is not limited to, the *information* encompassed in existing statutory definitions¹.

PPSI includes, but is not limited to:

- *Information* concerning a person which, because of name, number, personal mark or other identifier, can be used to identify that person, in combination with:
 - Social Security Number;
 - driver's license number or non-driver identification card number;
 - mother's maiden name; or
 - financial account identifier(s) or other *information* which would permit access to a person's financial resources or credit.
- *Information* used to authenticate the *identity* of a person or process (e.g., PIN, password, *passphrase*, *biometric data*). This does not include distribution of one-time-use PINs, passwords, or *passphrases*.

¹ General Business Law §§399-dd; 399-h(1)(c),(d),(e); 899-aa(1)(a)(b);
Public Officers Law, §§86(5); 92(7), (9);
State Technology Law §§202(5); 208(1)(a).

- *Information* that identifies specific structural, operational, or technical *information*, such as maps, mechanical or architectural drawings, floor plans, operational plans or *procedures*, or other detailed *information* relating to electric, natural gas, steam, water supplies, nuclear or telecommunications *systems* or infrastructure, including associated facilities, including, but not limited to:
 - training and security *procedures* at sensitive facilities and locations as determined by the Office of Homeland Security (OHS);
 - descriptions of technical processes and technical architecture;
 - plans for *disaster* recovery and business continuity; and
 - reports, logs, surveys, or audits that contain sensitive *information*.
- Security related *information* (e.g., *vulnerability* reports, *risk assessments*, security logs).
- Other *information* that is protected from disclosure by law or relates to subjects and areas of concern as determined by *SE* executive management.

Physical Security: The protection of *information* processing equipment from damage, destruction or theft; *information* processing facilities from damage, destruction or unauthorized entry; and personnel from potentially harmful situations.

PPSI: *See Personal, Private, or Sensitive Information.*

Privacy: The right of individuals and organizations to control the collection, storage, and dissemination of *information* about themselves.

Privileged Account: The *user-ID* or account of an individual whose job responsibilities require special *system authorization*, such as a network administrator, security administrator, etc. Special *authorizations* are allocated to this account such as RACF Administrator, auditor, Special, UNIX root or Microsoft Administrator.

Procedures: Specific operational steps that individuals must take to achieve goals stated in this Policy.

Remote Access: Any access coming into the *SE's* network from off the *SE's* private, trusted network. This includes, but is not limited to, dialing in from another location over public lines by an employee or other authorized individual.

Risk: The probability of suffering harm or loss. It refers to an action, event or a natural occurrence that could cause an undesirable outcome, resulting in a negative impact or consequence.

Risk Assessment: The process of identifying *threats* to *information* or *information systems*, determining the likelihood of occurrence of the *threat*, and identifying *system vulnerabilities* that could be exploited by the *threat*.

Risk Management: The process of taking actions to assess *risks* and avoid or reduce *risk* to acceptable levels.

Role-Based Access Control: An approach to restricting *system* access where permissions to perform certain operations are assigned to specific job functions.

SE: See *State Entity(ies)*.

Security Administration: The actions and responsibility for administering the security mechanisms including identification and *authentication* establishment and *authorization* maintenance.

Security Management: The responsibility and actions required to manage the security environment including the *security policies* and mechanisms.

Security Policy: The set of criteria for the provision of security services based on global rules imposed for all *users*. These rules usually rely on a comparison of the *sensitivity* of the resources being accessed and the possession of corresponding attributes of *users*, a group of *users*, or entities acting on behalf of *users*.

Sensitivity: The measurable, harmful impact resulting from disclosure, modification, or destruction of *information*.

Sniffing: Monitoring network traffic.

Spamming: Blindly posting something to a large number of groups.

Spoofing: Representing yourself as someone else.

Standard: Sets of rules for implementing policy. *Standards* make specific mention of technologies, methodologies, implementation *procedures* and other detail factors.

State: The State of New York.

State Entity(ies): *State Entity* for the purpose of this Policy, shall include all *State* agencies, departments, offices, divisions, boards, bureaus, commissions and other entities over which the Governor has executive power, the State University of New York Central Administration and the City University of New York Central Administration.

System(s): An interconnected set of *information* resources under the same direct management control that shares common functionality. A *system* may include hardware, software, *information*, applications or communications infrastructure.

Technical Security Review: A *technical security review* would consist of reviewing the *controls* built into a *system* or application to ensure they still perform as designed and are in compliance with documented security policies and *procedures*. It would also include reviewing security patches to ensure they have been installed and are operational, reviewing security rules such as access control lists for currency, testing of *firewall* rules, etc. This type of testing includes intrusion and/or *penetration testing* of *controls*.

Third Party: Any non-*SE* employee such as a contractor, vendor, consultant, intern, another *SE* (e.g., Office for Technology), etc.

Threat: A force, organization or person, which seeks to gain access to, or compromise, *information*. A *threat* can be assessed in terms of the probability of an attack. Looking at the nature of the *threat*, its capability and resources, one can assess it, and then determine the likelihood of occurrence, as in *risk assessment*.

Trojan Horse: *Malicious code* hidden in a legitimate program that when executed performs some unauthorized activity or function.

Unauthorized Access: Insider or outsider who gains access to network or *information technology equipment* resources without permission or without valid *authorization*.

User: Any *State Entity(ies)*, federal government entity(ies), political subdivision(s), their employees or *third party* contractor(s) or business associates, or any other individual(s) who are authorized by such entities to access a *system* for a legitimate government purpose.

Value: A measure of worth which can be expressed in monetary terms or in terms of importance to the *SE*.

Virus: A program that replicates itself on computer *systems* by incorporating itself into other programs that are shared among computer *systems*. Once in the new *host*, a *virus* may damage *data* in the *host's* memory, display unwanted messages, crash the *host* or, in some cases, simply lie dormant until a specified event occurs (e.g., the birth date of a historical figure).

Volume Level Encryption: Protects *data* by encrypting the entire partition of a disk or, in the case of a single partition hard drive, the entire drive.

Vulnerability: A weakness of a *system* or facility holding *information* which can be exploited to gain access or violate *system integrity*. *Vulnerability* can be assessed in terms of the means by which the attack would be successful.

Vulnerability Scanning: The portion of security testing in which evaluators attempt to identify physical, network, *system* or application weaknesses to discover whether these weaknesses may be exploited by persons or machines seeking to gain either unauthorized or elevated privileged access to otherwise protected resources.

Workforce: *State* employees, and other persons whose conduct, in the performance of work for the *SE*, is under direct control of the *SE*, whether or not they are paid by the *SE*.

World Wide Web (WWW): A hypertext-based *system* designed to allow access to *information* in such a way that the *information* may physically reside on locally or geographically different servers. This access was greatly improved through the introduction of a graphical interface to the *World Wide Web* called a web browser. Netscape and *Internet Explorer* are two of the most popular web browsers.

Worm: A program similar to a *virus* that can consume large quantities of network bandwidth and spread from one network to another.