

Glossary

* **Access Point** – an electronic device that serves as a common connection point for devices seeking to use radio frequency waves to connect to a wired network. Wireless access points provide shared bandwidth such that as the number of users connected to an access point increases, the bandwidth available to each user decreases.
* **ACL** - a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject and an operation. For instance, if a file object has an ACL that contains (Alice: read, write; Bob: read), this would give Alice permission to read and write the file and Bob to only read it.
* **Chain Letter –** Chain letter (Email) is a term used to describe Emails that encourage you to forward them onto someone else
* **CHD** - Cardholder Data, which refers to data related to a credit card transaction.
* **CVSS** - Common Vulnerability Scoring System is a free and open industry standard for assessing the severity of computer system security vulnerabilities. As of April 2005 the Forum of Incident Response and Security Teams (FIRST) is the custodian of CVSS for future development.   
  Scoring is the process of combining all the metric values according to specific formulas. Base Scoring is computed by the vendor or originator with the intention of being published and once set, is not expected to change. It is computed from the big three confidentiality, integrity and availability. This is the foundation which is modified by the Temporal and Environmental metrics. The base score has the largest bearing on the final score and represents vulnerability severity. More information about CVSS you can find at FIRST <http://www.first.org/cvss/use-design>
* **Demilitarized Zone** **(DMZ)** - is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network.
* **Dual Homing** - A computer with two or more network interfaces. A dual-homed host can act as a simple firewall on a small network as long as there is no direct IP traffic between the Internet and the internal network. In such a case, all Internet applications are run only on the dual-homed host.
* **PHI** - Personal Health Information, is individually identifiable health information, as defined by 45 CFR 160.103, known as HIPAA.
* **PII** - is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.
* **Ponzi –** A Ponzi scheme is a fraudulent investment operation that involves paying returns to investors out of the money raised from subsequent investors.
* **Pyramid Scheme –** A fraudulent scheme in which people are recruited to make payments to the person who recruits them while expecting payments from the persons they recruit.
* **RPO** - A Recovery Point Objective is the maximum acceptable amount of data loss measured in time. It is the age of the files or data in backup storage required to resume normal operations if a computer system or network failure occurs.
* **RTO** - Recovery Time Objective is the maximum desired length of time allowed between an unexpected failure or disaster and the resumption of normal operations and service levels. The RTO defines the point in time after a failure or disaster at which the consequences of the interruption become unacceptable.
* **Spam** – The unauthorized and/or unsolicited electronic mass mailings
* **Split Tunneling** - A computer networking concept which allows a VPN user to access a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same physical network connection. This connection service is usually facilitated through a program such as a VPN client software application.
* **System owner -** The system owner is responsible for every stage in the lifecycle of an information system including procurement, integration, modification, operation, maintenance, retirement.
* **Rogue Access Point** - A Rogue Access Point is any device that adds an unauthorized (and therefore unmanaged and unsecured) Wireless LAN (WLAN) to the organization’s network. A rogue AP could be added by inserting a WLAN card into a back office server, attaching an unknown WLAN router to the network, or by various other means.
* **VPN** – extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, and thus benefit from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption.