Cyber Security Standard (CSS) Master Glossary & Definitions CSS 2025

TAPA Standards

TAPA Copyright © Do Not Copy

TAPA Americas	TAPA Asia Pacific	TAPA EMEA
1353 Riverstone Pkwy Ste 120-320, Canton, GA 30114 USA	10 Anson Road, International Plaza #05-01, Singapore 079903	Proostwetering 18A 3543 AE Utrecht The Netherlands
www.tapaonline.org Tel. (561) 617-0096	www.tapa-apac.org Tel. (65) 6911 6800	www.tapaemea.org Tel. +31 1957 3461

© TAPA 2025 – All Rights Reserved

Term	Definition
IT - Information Technology	Information Technology, this could include both hardware and software.
Acceptable Use	A policy which is given to employees on what is acceptable regarding use of company owned equipment, including internet access.
Administrative access	Refers to accounts with the ability to modify computer hardware and operating system settings, which are above the level of a regular user's abilities on the given system. Some systems may refer to this as “root”, “administrator”, or “elevated” access.
Anti-Virus	Software designed to detect and protect against computer viruses.
Backup	In information technology, a backup, or data backup is a copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event.
BIA (Business Impact Analysis)	A method of identifying the effects of failing to perform a function or requirement.
Buyer owned IT assets	Computing devices and hardware which are placed at a LSP's location specifically by the Buyer for use only for Buyer's business.
Cloud Service Provider	A third-party company that offers a platform and hardware that is accessed remotely via an internet connection. Services can include infrastructure applications or storages services (example Azure or AWS.)
Data Breach	An incident wherein information is stolen or taken from a system without the knowledge of authorization of the system's owner.
DRP (Disaster Recovery Plan)	A documented process or set of procedures to execute an organization's disaster recovery processes and recover and protect a business IT infrastructure in the event of a disaster.
Encryption	The process of converting information or data into a code, especially to prevent unauthorized access.
External Party	3rd party provider / service provider. Examples many include people who come into work on any IT connected device (servers, laptops, printers, video monitoring equipment, alarms, HVAC, any IOT device, etc.).
Firewalls	A security appliance / software capable of monitoring, blocking or allowing network traffic.

Term	Definition
Information systems	An integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products.
IT Network Asset	A piece of software or hardware within information systems environment. Such as servers, routers, switches, etc.
Logical access control	A process or set standard which involves authenticating and authorizing users into the information systems. This is different than physical access control.
LSP (Logistics Service Provider)	A forwarder, a carrier, a trucking company, a warehouse operator, or any other company that provides direct services handling freight within the supply chain.
Malware	Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
MFA (Multi Factor Authentication)	Using more than one method of authentication from independent categories of credentials to verify the user’s identity for a login or other transaction.

TAPA Copyright © Do Not Copy

© TAPA 2025 – All Rights Reserved

NDA (Non-Disclosure Agreement)	A contract by which one or more parties agree not to disclose confidential information that they have shared with each other as a necessary part of doing business together.
PII (Personal Identifiable Information)	Information that, when used alone or with other relevant data, can identify an individual. Sensitive personally identifiable information can include your full name, Social Security Number, driver's license, financial information, and medical records.
Penetration Testing	An authorized simulated cyberattack or detailed analysis on a computer system, performed to evaluate the security of the system.
Phishing	The fraudulent attempt to obtain sensitive information or data by impersonating oneself as a trustworthy entity in a digital communication.
Physical access control	The restriction of access to a physical space within the business or organization. This type of access control limits access to rooms, buildings, and physical IT assets. In addition, physical access control keeps track of who is coming and going in restricted areas.
Router	Network device creating connection between multiple networks.
Social Engineering	Manipulating people into performing actions or divulging confidential information.
Spyware	Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly.
Term	**Definition**
SSID (Service Set Identifier)	The primary name associated with an 802.11 wireless local area network (WLAN), including home networks and public hotspots. Client devices use this name to identify and join wireless networks.
Switch	A network device creating connections between multiple devices.
UPS (Uninterrupted Power Supply)	An electrical apparatus that provides emergency power to a load when the input power source or mains power fails. This is usually a battery or series of batteries to allow for "soft" shutdown of critical systems or as a bridge until auxiliary power generation systems can be engaged.
Username (individual identifier)	An identification used by a person with access to a computer, network, or online service.
WLAN (Wireless Local Area Network)	Wireless Local Area Network Local area networks (LANs) that send and receive data without a physical connection between individual nodes and a hub, such as through radio transmission.
Zero-Day vulnerability	A zero-day (also known as 0-day) is a computer-software vulnerability unknown to those who should be interested in its mitigation (including the vendor of the target software). Until the vulnerability is mitigated, hackers can exploit it to adversely affect programs, data, additional computers, or a network.

TAPA Copyright © Do Not Copy

© TAPA 2025 – All Rights Reserved

TAPA Copyright © Do Not Copy

Publishing and copyright information

The TAPA copyright notice displayed in this document indicates when the document was last issued.

© TAPA 2025-2028

No copying without TAPA permission except as permitted by copyright law.

Publication history

First published in January 2021

Current edition published in January 2025

This Publicly Available Specification comes into effect on 1st January 2025.

 © TAPA 2025 – All Rights Reserved