CYBER SECURITY STANDARD

Transported Asset Protection Association

Cyber Security Standard
CSS 2025

TAPA Standards

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

CSS Table of Contents

1. Introduction

1.1. Purpose of this Cyber Security Standard (CSS) Document

This Cyber Security Standard (CSS) document is the official TAPA Standard to provide a minimum baseline for Cyber Security. It is a common global Standard that can be used in business/ security agreements between Buyers and Logistics Service Providers (LSPs) and/or other Applicants seeking Certification.

In developing this Standard, TAPA recognizes the cyber threats that Buyers and Logistics Service Providers must acknowledge and against which they *must develop and implement robust defense systems.* The CSS would apply to all of the services an LSP/Applicant provides.

1.2. Scope

- This Standard is intended to be a single-level standard framework.
- The aim is to provide a tool for companies to understand the minimum requirements in IT management in the company's supply chain operations to protect digital assets from cyber-attacks and operation lapses.
- The TAPA Cyber Security Standard is not absolute. Using this standard is not a substitute for regularly checking your national, regional, and international governmental reference websites.

1.3. Audience

Typical users of the TAPA Standards include:

- Buyers
- LSPs/Applicants
- Law Enforcement or other government organizations
- Professional Supply Chain Organizations
- Insurers

1.4. Resources to Implement the TAPA CSS

The resources necessary to meet the requirements of the CSS shall be the responsibility of the LSP/Applicant and at the LSP's/Applicant's own expense, unless negotiated or otherwise agreed upon by Buyer and LSP/Applicant.

1.5. Protecting LSP Policies and Procedures

Copies of security policies and procedures documents will only be submitted to Buyer in accordance with signed disclosure agreements between LSP/Applicant and Buyer and shall be handled as confidential information.

2. About TAPA

2.1. TAPA's Purpose

Cargo crime is one of the biggest supply chain challenges for manufacturers of valuable, high-risk products and their logistics service providers.

The threat is no longer only from opportunist criminals. Today, organized crime rings are operating globally and using increasingly sophisticated attacks on vehicles, premises, and personnel alongside non-tangible assets in the supply chain such as intellectual property and digital assets to achieve their aims.

TAPA is a unique forum that unites global manufacturers, logistics providers, freight carriers, law enforcement agencies, and other stakeholders with the common aim of reducing losses from international supply chains. TAPA's primary focus is theft prevention through the use of real-time intelligence and the latest preventative measures.

2.2. TAPA's Mission

TAPA's mission is to help protect members' assets by minimizing cargo losses from the supply chain. TAPA achieves this through the development and application of global Security Standards, recognized industry practices, technology, education, benchmarking, regulatory collaboration, and the proactive identification of crime trends and supply chain security threats.

3. TAPA Standards

3.1. TAPA Security Standards

The following global TAPA Security Standards have been created to ensure secure transportation and storage of high-value theft-targeted cargo:

- The Facility Security Requirements (FSR) represents minimum standards specifically for secure warehousing, or in-transit storage, within a supply chain.
- The Trucking Security Requirements (TSR) focuses exclusively on transport by truck and represents minimum standards specifically for transporting products via road within a supply chain.
- Cyber Security Standard (CSS) represents a minimum standard and a baseline for cyber security within a supply chain.

TAPA global Security Standards are reviewed and revised as needed every three years.

3.2. Implementation

Successful implementation of the TAPA Security Standards is dependent upon LSPs (Logistics Service Providers)/Applicants, Buyers (owners of the cargo), and TAPA Authorized Auditors working together.

4. Notices and Disclaimers

The TAPA Cyber Security Standard (CSS) 2025 (the "TAPA CSS") are made available for use subject to the important notices and legal disclaimers provided below. Access to and use of the TAPA CSS is subject to these notices and disclaimers.

4.1. Notice and Disclaimer of Liability Concerning the Use of the TAPA CSS

The TAPA CSS is developed by and within all three regions of TAPA – The Americas, Asia Pacific (APAC), and EMEA. TAPA develops its standards through a consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. TAPA CSS is developed by volunteers with industry-based expertise in technical working groups. Volunteers participate without compensation from TAPA. While TAPA administers the process and establishes rules to promote fairness in the consensus development process, TAPA does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

TAPA makes no warranties or representations concerning its standards and expressly disclaims all warranties, express or implied, concerning the TAPA CSS, including but not limited to the warranties of merchantability, fitness for a particular purpose, and non-infringement. In addition, TAPA does not warrant or represent that the use of the material contained in its standards is free from patent infringement. The TAPA CSS is supplied “AS IS” and “WITH ALL FAULTS”.

Use of the TAPA CSS is entirely voluntary. The existence of the TAPA CSS does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the TAPA CSS. Furthermore, the viewpoints expressed at the time the TAPA CSS is approved and issued are subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making the TAPA CSS available, TAPA is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is TAPA undertaking to perform any duty owed by any other person or entity to another. Any person utilizing the TAPA CSS should rely upon his or her independent judgment in the exercise of reasonable care in any given circumstance or, as appropriate, seek the advice of a competent professional in determining the appropriateness of the TAPA CSS.

IN NO EVENT SHALL TAPA BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

4.2. Translation

The TAPA consensus standards development process involves the review of documents only in the English language. In the event that the TAPA CSS is translated, only the English version published by TAPA is the approved TAPA standard.

4.3. Laws and Regulations

Users of the TAPA CSS should consult all applicable local laws and regulations. Compliance with the provisions of the TAPA CSS does not constitute compliance with any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. TAPA does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

4.4. Not Legal Advice

The TAPA CSS does not include or constitute legal advice and is not intended to serve as a substitute for legal advice. Users of the TAPA CSS should consult with their own legal counsel if they desire to incorporate or refer to the standard in legal agreements.

4.5 Updating of the TAPA CSS

Users of the TAPA CSS should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official TAPA document at any point in time consists of the current edition of the document together with any amendments or errata then in effect. Users are cautioned to determine that they have the latest edition of any TAPA standard.

IMPORTANT NOTICE

The TAPA CSS does not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. The TAPA CSS development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during the implementation of the standard. Implementers and users of the TAPA CSS documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

4.6. Copyrights

The TAPA CSS is copyrighted by TAPA under US and international copyright laws. They are made available by TAPA and are adopted for a wide variety of both public and private uses. These include both uses, by reference, in-laws, and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, TAPA does not waive any rights in copyright to the documents. Subject to payment of the appropriate licensing fees, TAPA will grant users a limited, non-exclusive license to copy portions of the TAPA CSS for company or organizational internal use or individual, non-commercial use only.

“TAPA” is a registered trademark of the Transported Asset Protection Association and may not be used without the express written permission of TAPA through its officially recognized regions. TAPA Standards and associated material are published through, and by TAPA, and may not be revised, edited, or changed by any party without the express written permission of TAPA. Misuse of the TAPA brand may result in the removal of certification or legal action.

5. Contracts and Subcontracting

5.1. Contracts

The safe and secure transportation, storage, and handling of the Buyer’s assets is the responsibility of the LSP/Applicant, its agents and subcontractors throughout the collection, transit, storage, and delivery, as specified in a release or contract.

Where the CSS is referenced or included in the contract between the LSP/Applicant and Buyer, it shall also be referenced in the LSP's/Applicant's security program.

LSP shall provide Buyer with evidence of CSS Certification and, where appropriate, evidence that CSS requirements have been met. Further, any alleged failure by the LSP/Applicant to implement the CSS requirements shall be resolved according to the terms of the contract negotiated between the Buyer and the LSP/Applicant.

5.2. Subcontracting

Subcontracting contracts include a requirement that the subcontractors of the LSP/Applicant meet all noted CSS Requirements.

6. TAPA CSS Certification

6.1. Self-Certification

Self-Certification option is not applicable in this Standard. All certification audits must be executed by properly trained TAPA approved IAB Authorized Auditors (IAB AA).

6.2. General Information

6.2.1. Even though the CSS is intended for entity certification (single or multi-site), the following conditions must be met:

6.2.1.1. The sites/facilities that shall be included in the certification must be owned/ operated by the entity requesting certification.

6.2.1.2. The sites/facilities that shall be included in the certification must be explicitly listed in the certification application and the certificate issued by the IAB.

6.2.1.3. All the sites/facilities included in the certification request must use the same IT infrastructure.

6.2.1.4. The sites/facilities that shall be included in the certification must have a common IT Security Management System.

6.2.1.5. The sites/facilities included in the entity certification must comply with the CSS requirements. This compliance must be confirmed by a properly TAPA trained internal Authorized Auditor (AA) that should have audited the sites (remotely or onsite) and be able to present related CSS audit reports.

6.2.1.6. Inclusion of new sites can be executed provided the LSP/Applicant submits to the IAB the relative AA CSS audit reports and requests the addition on a new site or a group of new sites into the certification scheme. The IAB will examine the info received and re-issue the entity (multi-site) certificate with the new sites included.

6.2.1.7. Removal of existing site(s) can be executed provided the LSP/Applicant removes the site(s) form the listing of sites and formally informing the IAB. The IAB shall revoke the individual site certification and adjust and re-issue the entity (multi-site) certificate.

6.2.2. An informal summary of the findings/ results should be shared with the LSP/Applicant during the audit closing conference. The IAB AA shall inform the LSP/Applicant of audit results within ten (10) business days following the completion of the audit. Any delays in issuing the audit results must be promptly communicated to the LSP/Applicant and negotiated between the IAB AA and LSP/Applicant.

6.2.3. Costs for TAPA certification are the responsibility of the LSP/Applicant unless otherwise negotiated with the Buyer(s).

6.3. Re-certification

The TAPA CSS certificate shall be valid for a period of three (3) years with no extension permitted.

To prevent any lapse in certification, a re-certification audit must be performed prior to the expiration date of the current certificate. Completion of any SCARs must also occur within the original 60-day allotted period and prior to the current certificate's expiration date (see Corrective Action/SCAR in Section 7).

Therefore, to assure adequate planning and preparation, it is recommended that the LSP/Applicant schedule the re-certification audit three (3) months before the current certificate expiration date. If the TAPA CSS certificate is issued within the aforementioned three-month period, the date of the new certificate will be the expiration date of the current certification. If corrective actions are not closed prior to the expiration date, and there is no waiver granted, the certification will expire.

7. Audit Follow Up

7.1. Corrective Action/SCAR

If CSS requirements are not met, as discovered during the audit, the IAB AA submits a Security Corrective Action Requirement (SCAR) to the relevant LSP/Applicant. The LSP/Applicant shall respond to the IAB AA within ten (10) business days, documenting the action to be taken and the date the action will be completed. SCAR completion dates may be negotiated between the IAB AA and the LSP/Applicant. However, unless the Regional TAPA Waiver Committee approves a waiver, corrective action implementation shall not exceed sixty (60) days from notification to the LSP/Applicant.

In all cases, the LSP/Applicant shall submit progress updates/reports on all outstanding SCARs to the IAB AA. Any SCAR not completed before its due date shall be escalated by the LSP's/Applicant's Security Representative to the LSP's/Applicant's Management. The reason(s) for non-compliance shall be documented and communicated to the IAB AA. LSP's/Applicant's failure to address a SCAR may result in the withholding of the TAPA certification. The LSP/Applicant has the right to appeal directly to TAPA if the certification is withheld. TAPA shall arbitrate the dispute between the LSP/Applicant and the IAB AA and retains the right to issue a binding resolution to the dispute.

Note: It is not necessary for the IAB AA to re-audit the facility in order to close a SCAR. Evidence of SCAR closure (i.e., achieving compliance) may be presented to the IAB AA in the form of written correspondence, web meetings, conference calls, photographs, etc.

7.2. Compliance Monitoring

7.2.1. Self-Audits

The LSP/Applicant will ensure they have an internal process in place in order to monitor compliance, in years two and three, in between formal audits conducted by an AA. (the responsible person for monitoring the TAPA Cyber Security Standard (CSS) or any other individual properly qualified and trained).

7.2.2. Interim Self-Audits

7.2.2.1. The interim Self-Audits must reflect the CSS requirements.

7.2.2.2. Interim Self Audit's must be carried out by LSP's/Applicant's own or subcontracted AA individual properly qualified and trained.

7.2.2.3. The interim Self-Audit must be documented on the TAPA audit form and submitted to the IAB within 30 days of the anniversary date of the original IAB certification.

7.2.2.4. Failure to comply will result in suspension of the original certification until the interim Self-Audit is properly completed. Gaps identified must be documented, assigned a due date for completion of corrective action(s), and tracked to closure within 60 days.

Table 1: Audit & Compliance Monitoring Schedule

Action	Frequency
Certification Audit (IAB AA Certification Audit)	Every three (3) years
Self-Audits (interim compliance checks)	Annually at 1st and 2nd Anniversary
LSP/ Applicant Subcontractor Audit	In accordance with Buyer- LSP/ Applicant contract

7.2.3. Buyer Visits to LSP/Applicant

The Buyer and the LSP/Applicant recognize the importance of working in partnership to reduce risk within the supply chain. Both parties agree to schedule Buyer visits with reasonable notice, e.g., 10 business days, with scope and parameters mutually agreed upon in advance and/or in accordance with the Buyer-LSP/Applicant contract. Loss investigations: i.e., thefts, damage, etc., shall be performed in accordance with the Buyer-LSP/Applicant contract.

7.3. TAPA Complaint Investigation and Resolution

If TAPA receives a formal complaint concerning the performance of a certified LSP/Applicant, TAPA (subject to validation) may require that the LSP/Applicant contract for a re-audit at the LSP's/ Applicant's expense. If the LSP/Applicant fails the audit, or refuses to comply with this process, their certificate may be withdrawn.

8. Waivers

8.1. Overview

A waiver is a written approval granted to either exempt a facility from a specific TAPA requirement or to accept an alternative compliance solution. A waiver may be requested if an LSP/Applicant cannot meet a specific requirement in the CSS and can justify alternative measures. Waivers are valid for the period of the certification.

All waiver requests for a specific security requirement (either in part or whole) must be submitted via a TAPA Waiver Request form to the Independent Audit Body (IAB)/Authorized Auditor (AA) by the LSP/Applicant (to be found on the TAPA website). The requesting LSP/Applicant takes full responsibility for the accuracy of information provided in the waiver request.

Each waiver request must then be submitted through the IAB/AA to the TAPA Regional Waiver Committee for approval. It is the responsibility of the IAB/AA to decide if the request is complete and justifies processing by TAPA; this includes verification of mitigating factor(s) and/or alternative security controls.

Should TAPA officials and/or Buyers challenge that waiver conditions have changed, TAPA will complete a formal investigation and LSP/Applicant understands that the waiver may be revoked by TAPA.

8.2. Waiver Business Process

If an LSP cannot meet a specific requirement in the CSS, the waiver process below is implemented:

Table 1: Responsibilities: Waiver Application / Evaluation

Step	Responsibility	Action
1.	LSP/Applicant	Establishes and verifies mitigation measures.
2.	LSP/Applicant	Completes TAPA Waiver Request form and submits to the IAB/AA.
3.	IAB/AA	Reviews and verifies integrity of the information contained in the TAPA Waiver Request form.
4.	IAB/AA	Submits TAPA Waiver Request form to the TAPA Regional Waiver Committee.
5.	TAPA Regional Waiver Committee	Reviews the request and either grants or denies the waiver.

If a Waiver Is Denied

If the TAPA Regional Waiver Committee does not approve the waiver request, the LSP/Applicant is required to implement the full security requirements of the CSS.

If a Waiver Is Granted

If the TAPA Regional Waiver Committee approves the waiver request, the following actions will be taken:

Table 2: Waiver Approval

Step	Responsibility	Action
1.	TAPA Regional Waiver Committee	Documents and signs the waiver specifics.
2.	TAPA Regional Waiver Committee	Specifies the waiver lifespan (up to a maximum of three years) and sends a copy to the AA.
3.	AA	Notifies the LSP/Applicant of the outcome of the Waiver Request.
4.	LSP/Applicant	Complies with the waiver requirements. Failure to do so shall void the waiver approval.

9. Cyber Security Standard (CSS)

Section	Section #	Requirement #	Requirement
Security Policy	1.0	1.1	LSP/Applicant management must have formally appointed a person who is responsible for maintaining cyber security and information protection. The supplier must also have a person (can be the same) responsible for monitoring the TAPA Cyber Security Standard (CSS). This includes scheduling compliance checks, communications with relevant parties, changes to the CSS, etc. Note: This person can be an employee or an outsourced person under contract to perform this role. This person can be the same person responsible for the other TAPA standards but must have relevant qualifications or training to fulfil the role.
Security Policy	1.0	1.2	LSP/Applicant must have Information security policies and procedures that address the following areas: a) Purpose & objectives (Example: Govern, Identify, Protect, Detect, Respond, Recover); b) Scope; c) Roles & Responsibilities to include OT/IOT/Cyber security owners responsible and accountable for protecting overall Information security and the key areas of identification, detection and response and; d) Clearly defined security levels and priorities.
Security Policy	1.0	1.3	Cybersecurity policies and procedures must be reviewed by an appropriate person responsible for cybersecurity and updated at least on an annual basis based on risk or as circumstances dictate.

Section	Section #	Requirement #	Requirement
Data Protection	2.0	2.1	The LSP/Applicant must have a policy and procedure regarding computer systems containing LSP's/Applicant's assets which must leave the LSP's/Applicant's facility for repair or disposal. Any data or devices containing the Buyer information must be removed or destroyed first, according to NIST standard 800-88, ISO, or similar standards.
Data Protection	2.0	2.2	LSP/Applicant must have a policy and procedure regarding computer systems containing Buyer information. They must not have removable storage devices, or USB ports to which portable devices could be attached and/or must have them disabled. a) In the case that they can't be physically removed or disabled, a use policy must be in place and applied consistently. b) In the event that a portable drive is required for the shipping/receiving process (i.e. use of digital cameras) or other production-related activities, the LSP/Applicant must: i) Protect with a password and encryption; ii) Perform an anti-virus/malware/spyware scan on the device prior to entry into the secure environment; and, iii) Have any such portable drive (USB) owned and registered by LSP/Applicant, with use controlled by management. c) Must have a documented written policy controlled and enforced by management.
Data Protection	2.0	2.3	When on-site repairs are made to computer systems containing Buyer information, LSP's/Applicant's IT personnel should be present at all times. LSP/Applicant must: a) Maintain a log providing repair details, individuals involved, and disposition of disposed equipment as a result of repairs; b) Have a valid, active NDA obligating the service providers to retain as confidential LSP's/Applicant's IP and confidential information of LSP's/Applicant´s Buyers; and, c) Policy and procedures must cover repair during emergency circumstances and non-business hours.

Section	Section #	Requirement #	Requirement
Data Protection	2.0	2.4	LSP/Applicant must have a data classification policy/program. All Buyer Information and/or PII must be designated as such and protected as required by the most restrictive data classification level utilized by LSP/Applicant.
Data Protection	2.0	2.5	For LSP's/Applicant's facilities that have return operations involving stored data (customer returns), the following would apply: a) The LSP/Applicant must have policies and practices in place to protect any information that may have been inadvertently retained on any returned devices (such as computers, drives, memory boards, etc.) b) All such devices should be segregated within the facility until resolution of any issues identified above or unless the entire facility is dedicated to these functions.
Network Security	3.0	3.1	When Buyer-owned IT Network Assets are placed and utilized at LSP's/Applicant's facility*, such Buyer-owned IT equipment (e.g. network components and/or servers) located at LSP's/Applicant's facility(is) must be stored in physically secured and access-controlled IT room(s) that: a) have active alarms (if the door is held open, or opened without proper access); b) have a solid ceiling (or some similar mitigation); c) have a motion detector in the room (attached to the alarm system); d) must be covered by video monitoring and recording. * i.e.: Placed by Buyer to house Buyer's inventory WMS
Network Security	3.0	3.2	LSP/Applicant must identify and maintain an inventory of: a) all IT/OT/IOT assets b) the exact location of device(s) within the facility c) Identification of all devices upon which Buyer data resides d) Asset Description e) Asset Owner

Section	Section #	Requirement #	Requirement
Network Security	3.0	3.3	LSP/Applicant must use practices in line with current industry standards that protect their enterprise network on to which Buyer information is stored and processed, for example, NIST, ISO 27001, IEC 62443, or other relevant cyber security standards.
Network Security	3.0	3.4	LSP/Applicant must employ execute an annual cyber external security audit and/or penetration testing of their IT/OT/IOT systems, which includes the LSP's/Applicant's network access control systems. Testing should be conducted by a qualified independent 3rd party properly certified. LSP/Applicant must address and/or close any gaps identified from the penetration testing. This process should be documented, and records kept for the certification validity period.
Network Security	3.0	3.5	LSP/Applicant must have a policy/procedure that specifies, at least every 90 days, a review of allowed access to LSP's/Applicant's Information Systems. Upon completion of the review, management approval must-revalidate all employees'/contractors' access. Access must be terminated immediately for any employees/contractors who do not have a valid need for revalidation.

Section	Section #	Requirement #	Requirement
Wireless Networks	4.0	4.1	Wireless networks must be secured with at least WPA2 security protocol and be limited to LSP's/Applicant's personnel. Only devices on the approved MAC address list can access the corporate network. Guest wireless networks must be for guest temporary use only and not have any LSP's/Applicant's/buyer's devices or systems connected through them. Guest or visitors must not be allowed access to LSP's/Applicant's employees network(s). Recommendation • SSID should be hidden.
Remote Access	5.0	5.1	The LSP/Applicant must define and document the risks that remote access can expose in their different environments.
Remote Access	5.0	5.2	LSP/Applicant must complete a review every 90 days of accounts which have remote access to LSP's/Applicant's systems. This review will cover at least the following topics: a) Decide who shall have remote access, when, where, and how; b) Includes employees, vendors/suppliers, and business partners; c) Create policies and procedures for remote access to whom, when, where, and how; d) Have a system for documenting, logging access, and denying access (i.e.an essential supply chain software vendor or a partner LSP); and, e) Have measures for securing remote access due to external cyber threats (for example: two factor authentication). Note: If user accounts have remote access capability via VPN (or similar) this review must be done at the same time as Control 3.5. Records of these reviews shall be kept for the certification validity period.

Section	Section #	Requirement #	Requirement
Remote Access	5.0	5.3	The LSP/Applicant must train employees and contingent staff on these risks. Training material(s) must be documented, and training records must be kept for at least one year. Formal training must be delivered annually via memoranda, virtual meeting, online training, or in-person class-room training.
User Account Management	6.0	6.1	LSP/Applicant must have documented policies/procedures regarding administrative privileges on Information Systems; they must be individually assigned and restricted to personnel who need such privileges. a) Privileged access rights must be allocated to users on a need-to-know basis and in accordance with the network access control policy; b) Privileged access rights should be assigned to a user ID different from those used for regular business activities. Regular business activities should not be performed from privileged ID; c) Review of Admin/root access should be done every 90 days; and, d) Termination of admin rights must be done immediately upon termination or change in role within the company.
User Account Management	6.0	6.2	Documented procedures must require that new user accounts meet the following conditions: a) An initial password must be assigned to each new account at the time of creation; b) The initial password must be unique for each new user. Default, standard, or blank initial passwords must not be used; c) Initial passwords cannot contain the user's name, identification number or otherwise follow a standard pattern based on user information; d) Passwords will be communicated to users in a secure manner, and only after validating the identity of the user; and, e) Users must be required to change passwords on initial login.

Section	Section #	Requirement #	Requirement
User Account Management	6.0	6.3	LSP/Applicant must have a documented policy/procedure which outlines the cybersecurity related steps regarding an employee's/contractor's termination or change of role. LSP/Applicant must immediately terminate physical and logical access to LSP/Applicant's information systems as applicable.
Identification, Authentication, and Access	7.0	7.1	LSP/Applicant must implement access controls on Information Systems via individual identifiers that are not shared among multiple users. These guidelines must be documented in a policy. Password Parameters: • Eight (8) characters or more when possible, following this sliding scale: ○ 8-15 characters: mixed case letters, numbers, and special characters; ○ 16+ characters: mixed case letters and special characters; Based on the sliding scale above, choose characters from three or more of the following character classes, particularly if the system prohibits long passphrases: • Alphabetic lower-case (a-z); • Alphabetic upper-case (A-Z); • Numeric (0-9); • Punctuation and other characters (for example: !@#$%^&*()_+|~-=\`{}[]:";'<>?,./) when permitted. Note: Where technically feasible, create a long and easy-to-remember passphrase (at least 16 characters, using a series of words that can include spaces). The following practices must also be adhered to, at a minimum: a) passwords must be changed at least every 90 days; b) after 5 failed login attempts a system alert must be created; c) Information Systems must prevent the re-use of the last 10 passwords and of passwords used in the last 30 days; and, d) passwords must not be shared.
Identification, Authentication, and Access	7.0	7.2	The LSP/Applicant must employ multi factor authentication (MFA) for access to the internal network from an external source. There must be a documented policy/procedure in place.

Section	Section #	Requirement #	Requirement
Identification, Authentication, and Access	7.0	7.3	User accounts and/or passwords to computer systems cannot be shared, posted, or otherwise distributed. Each employee must not share their individual user ID and password or any other network access user credentials. Consequences for sharing passwords or other network access user credentials must be outlined in policies/procedures and training.
Identification, Authentication, and Access	7.0	7.4	All files or folders containing Buyer confidential information must be protected by an Access Control List (ACL). There must be a documented policy/procedure in place.
Identification, Authentication, and Access	7.0	7.5	LSP/Applicant must have in place an appropriate use policy regarding information systems. The policy must include artificial intelligence/machine learning services. Consequences for violating use policy must be outlined in policies and training.
Identification, Authentication, and Access	7.0	7.6	LSP/Applicant access logs and admin access logs must be reviewed at least every 90 days. Each review must be documented and retained for a minimum of 6 months. 5+ failed/rejected access attempts must be investigated. Investigations must be conducted in accordance with the incident handling policy and outcomes must be documented. Records must be kept for the duration of the certification validity. Members of IT & Security Management must review the result of the investigation. There must be a documented policy/procedure in place.

Section	Section #	Requirement #	Requirement
Information Security Awareness Training	8.0	8.1	The LSP/Applicant must provide information security awareness training to employees and contractors. The training must include the roles and responsibilities computer users play in maintaining cyber security for the LSP/Applicant. a) Training to provide employees and contractors basic knowledge and training to execute their day-to-day responsibilities in a secure manner and in accordance with LSP's/Applicant's policies and procedures including: i) Protection practices against social engineering, phishing, malware, ransomware, spyware, etc; ii) Access requirements to the LSP / APPLICANT's Information Systems; iii) How to report a suspected security incident (phishing email for example); iv) How to report suspected or inadvertent sharing of Buyer confidential information; and, v) How to manage remote access risks and potential information exposure. b) Training must be done as part of orientation and within 30 days from the hiring date, with focus as appropriate depending upon job responsibilities, and repeated at least annually for all personnel with IT access. (The above is not an exhaustive list of subjects to include in the training.) There must be a documented policy/procedure in place.
Information Security Awareness Training	8.0	8.2	The LSP/Applicant must document the training in 8.1, including content provided, dates, and the personnel trained, and retain that documentation/training records for a minimum of 3 years.
Information Security Awareness Training	8.0	8.3	Practical measures, such as phishing test emails and random interviews of employees must be employed to gauge the effectiveness and understanding of cyber security training. This should be done at a minimum on a quarterly basis. Outcome of these regular tests must be reviewed for follow up. Additional mitigation measures must be applied, if necessary.

Section	Section #	Requirement #	Requirement
Laptops and Portable Devices	9.0	9.1	Portable storage media, such as thumb drives, must be in personal custody during business hours, otherwise, they must be secured in a locked location. LSP/Applicant computer devices, such as tablets, laptops, phones, and computers, must be immediately access-locked (screen locked, with a password or biometric ID) when not in use. There must be a documented policy/procedure in place.
Cryptographic Controls	10	10.1	Encryption must be used for protecting Buyer information in storage or while in transit over connected or wireless networks (including transmission over the internet). The encryption level should be TLS 1.2 or a comparable higher standard. There must be a documented policy/procedure in place.
Information Infrastructure Security	11	11.1	LSP/Applicant must use anti-virus software to scan for malware, viruses, worms, or other maliciously intended software at the following points in real time and must contain the latest updates: a) network entry/exit points; and, b) download of files from external sources (including emails, external storage devices, etc.). There must be a documented policy/procedure in place.
Configuration Management	12	12.1	All IT equipment used throughout the network must have legitimate/properly licensed software. The LSP/Applicant must have a documented process to ensure secure sourcing of software and be able to show up-to-date licensing evidence.

Section	Section #	Requirement #	Requirement
Configuration Management	12	12.2	The LSP/Applicant must apply and maintain documentation and records for the current configuration (imaging), and change-management procedures to the following systems, utilizing a change management board/process for the following items: a) All computer systems containing Buyer's information and/or LSP/Applicant's data that has the most restrictive data classification level utilized by LSP/Applicant; b) The centralized computing resources upon which these systems depend; and, c) Firewalls, routers, or network switches that are used to control LSP/Applicant assets.

Section	Section #	Requirement #	Requirement
Technical Vulnerability Management	13	13.1	The LSP/Applicant must have in place an ongoing patch process/policy that must involve patching of vulnerable systems and/or applying other controls. This must include: a) Security-relevant software updates include, for example, patches, service packs, hotfixes, and anti-virus signatures; b) The patch policy must state a time frame for the review and implementation of issued patches by the software provider. If a patch or an update for a critical flaw, i.e. zero-day vulnerability, is announced, a policy should be in place to immediately implement the patch.
Intrusion Detection and Prevention Systems	14	14.1	The LSP/Applicant must have an intrusion detection, monitoring and prevention mechanism which provides alerts regarding: a. attacks and indicators of potential attacks. b. unusual transactions that could indicate unauthorized access to information. c. unexpected changes to system configurations and privileges; and d. unauthorized local, network and remote connections. e. unusual data transfer patterns There must be a documented policy/procedure in place.
Intrusion Detection and Prevention Systems	14	14.2	The LSP/Applicant must establish a written process/procedure for documenting, reporting, and escalating security events, and weaknesses. The LSP/Applicant must retain investigation documentation of actions taken and improvements made in response to the event for a minimum of one (1) year. Note: One (1) year retention is the TAPA requirement. Local laws/regulations may require an alternate retention time.

Section	Section #	Requirement #	Requirement
Security Incident Management	15	15.1	If LSP/Applicant becomes aware of a Data Breach, LSP/Applicant will notify Buyer(s) within 24 hours and promptly take reasonable steps to minimize harm and secure Buyer data. In case the breach is a confirmed breach, notification to the Buyer must be immediate. The LSP/Applicant must perform an annual review which includes a tabletop exercise on the incident management policies and procedures. The outcome of these annual reviews and tabletop exercises must be reviewed for follow up on the results by management. Additional mitigation measures must be applied, if necessary.
Security Incident Management	15	15.2	If an unauthorized user obtains access to LSP/Applicant's computer systems or networks containing Buyer information, the LSP/Applicant must immediately investigate the incident to determine if Buyer information has been copied, altered, or destroyed as a result of the unauthorized access. Records of these investigation reports must be kept for the duration of the certification validity. Members of IT & Security Management must review the result of the investigation. There must be a documented policy/procedure in place.

Section	Section #	Requirement #	Requirement
Environmental Controls	16	16.1	The LSP/Applicant must ensure that clean, reliable electrical power is provided for critical computing infrastructure and computer equipment containing Buyer assets. a) Uninterrupted Power Supply (UPS) must be capable of providing adequate power until: (i) Alternative power systems, such as a generator or secondary circuit, are activated; or, (ii) Computer systems are shut down according to manufacturer specifications. b) Systems containing Buyer information must be configured to shut down before the UPS battery runs out, to prevent a “hard stop,” which results in potential data loss or system corruption. c) The UPS should be tested annually to confirm the UPS system is operating at actual necessary levels.
Environmental Controls	16	16.2	The LSP's/Applicant's data centre or computer room should be equipped with a fire alarm/smoke detection system and a fire suppression mechanism and that is maintained in accordance with applicable state/regional laws and regulations. It is recommended the fire suppression systems for the data centre use specific agents such as inert gases or clean agents to avoid damage to the expensive electronic equipment.
Third-party Service Delivery Management	17	17.1	The LSP/Applicant must have a documented process/procedure to assess the risk whenever there is a business need for an external party to have access to secure information or information processing facilities. This policy/procedure must include the requirements for allowing access by external parties to information process facilities, any specific restrictions regarding access, and follow-up checks. Approval must be documented and records of these approvals must be kept for the duration of the certification validity.

Section	Section #	Requirement #	Requirement
Third-party Service Delivery Management	17	17.2	The LSP/Applicant must annually audit third parties, who have any electronic transactions (any kind of access, house, or receive data for the LSP/Applicant), to ensure compliance with TAPA CSS requirements. This must include a review of processes and procedures for integrations and remote access into systems.

Section	Section #	Requirement #	Requirement
Cloud Services Security	18	18.1	An LSP/Applicant who engages with one or more Cloud Service Providers must ensure such Cloud Service Providers adhere to the following: a. Protect Buyer information in accordance with the applicable security requirements specified in the CSS; b. Buyer information must be protected during the disruption of cloud service providers' business; c. Have a Disaster Recovery Plan (DRP) in place; and perform a yearly tabletop exercise to evaluate the effectiveness of the DRP d. Have the ability to provide proof that Buyer information has been securely deleted upon termination of services or at Buyer's request. There must be a documented policy/procedure in place.
Security in Business Continuity Planning	19	19.1	The LSP/Applicant must have appropriate business continuity plans (BCP) including a Disaster Recovery Plan (DRP) for recovering from compromised system attacks, including but not limited to, all necessary data and software backup and recovery arrangements. Recovery Time Objectives (RTO) must be defined in the BCP. There must be a documented policy/procedure in place.
Security in Business Continuity Planning	19	19.2	Complete BCP/DRP exercises must be executed at least annually by the LSP/Applicant. The outcomes of these annual exercises must be reviewed by the management. The BCP/DRP must be reviewed and updated at least annually. Additional mitigation measures must be applied, if necessary.
Backup and Restoration	20	20.1	Information Systems must be backed-up at least weekly. Such backups must be tested at least monthly and backup data must be encrypted. The LSP / APPLICANT must define a back-up strategy that includes encrypting and testing back-up files, and must document all back-up, rotation, and restore procedures There must be a documented policy/procedure in place.

Section	Section #	Requirement #	Requirement
Backup and Restoration	20	20.2	If backed up onsite, the backup files must be stored in another building or a secondary off-site location, with Buyer information in electronic format, must be protected by appropriate physical and logical access controls, and be accessible only to personnel whose job function requires such access.

Publishing and copyright information

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

Publication history

First published in January 2021

Current edition published in January 2025

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