2021
Cyber Security Standards

Transported Asset Protection Association

Cyber Security Standards Requirements
CSS 2021

TAPA - The Americas
5030 Champion Blvd, G-11 #226
Boca Raton, Florida 33496 USA
Tel. (561) 617-0096
www.tapaonline.org

TAPA – Asia Pacific
70 Shenton Way
Eon Shenton, #16-02
Singapore 079118
Tel. (65) 6980 0584
www.tapa-apac.org

Table of Contents

1. Introduction

Purpose of this Cyber Security Standards (CSS) Document

This Cyber Security Standards (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 the development of this Standard, TAPA recognizes the cyber threats which 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 provided by an LSP/Applicant.

Scope

- This Standard is intended to be single-level standards framework, (not A, B, C; or 1, 2, 3).
- The TAPA Cyber Security Standards are not absolute. Using these standards is not a substitute for regularly checking your national, regional, and international governmental reference websites.

Audience

Typical users of the TAPA Standards include:

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

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.

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

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 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.

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

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 Standards (CSS) represent a minimum standards and a baseline for cyber security within a supply chain.

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

This document addresses the CSS requirements only.

- The certification process for TAPA CSS is documented in the TAPA CSS document.

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

Important Notices and Disclaimers Concerning TAPA CSS Standards Documents
The TAPA Cyber Security Standards Requirements CSS 2021 (the "TAPA CSS Standards") are made available for use subject to the important notices and legal disclaimers provided below. Access to and use of the TAPA CSS Standards is subject to these notices and disclaimers.

Notice and Disclaimer of Liability Concerning the Use of the TAPA CSS Standards
The TAPA CSS Standards are developed by and within TAPA – The Americas and TAPA – Asia Pacific. 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 Standards are 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 Standards, 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 Standards are supplied "AS IS" and "WITH ALL FAULTS."

Use of the TAPA CSS Standards is entirely voluntary. The existence of the TAPA CSS Standards 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 Standards. Furthermore, the viewpoint expressed at the time the TAPA CSS Standards are approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standards.

In publishing and making the TAPA CSS Standards 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 Standards should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of the TAPA CSS Standards.

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.

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

Laws and Regulations
Users of the TAPA CSS Standards should consult all applicable laws and regulations. Compliance with the provisions of the TAPA CSS Standards does not constitute compliance to 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.

Not Legal Advice
The TAPA CSS Standards do not include or constitute legal advice and are not intended to serve as a substitute for legal advice. Users of the TAPA CSS Standards should consult with their own legal counsel if they desire to incorporate or make reference to the standards in legal agreements.

Updating of the TAPA CSS Standards
Users of the TAPA CSS Standards 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 Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. The TAPA CSS Standards 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 implementation of the standard. Implementers and users of the TAPA CSS Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Copyrights
The TAPA CSS Standards are copyrighted by TAPA – The Americas 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 use, 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 Standards for company or organizational internal use or individual, non-commercial use only.

Trademarks
"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.

5. Contracts and Subcontracting

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.

Subcontracting

Subcontractors of storage includes a contractual requirement that the subcontracting LSP/Applicant meets all noted CSS Standards.

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/Applicant expense. If the LSP/Applicant fails the audit, or refuses to comply with this process, their certificate may be withdrawn.

6.0 Waivers

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.

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 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 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.

Cyber Security Standards (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 Standards (CSS). This includes scheduling compliance checks, communications with relevant parties, changes to the CSS, etc. Note: These persons can be an employee or 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 fulfill 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 b) Scope c) Roles & Responsibilities to include IT / Cyber security owners responsible and accountable for protecting overall Information security and the key areas of identification, detection, and response 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 IT security yearly and updated at least on an annual basis based on risk or as circumstances dictate.
Data Protection	2.0	2.1	The LSP/Applicant must have a policy and procedure regarding computer systems containing LSP / APPLICANT assets which must leave the LSP / Applicant's facility for repair or disposal, any data or devices containing Buyer information must be removed or destroyed first, to NIST standard 800-88.

Section	Section #	Requirement #	Requirement
Data Protection	2.0	2.2	LSP / APPLICANT must have a policy and procedure regarding computer systems containing Buyer information. They must not have disk drives, writable CD-R or DVD-R disc drives, 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 b) In the event that a portable drive is required for shipping / receiving process (ex. use of digital cameras) or other production-related scenarios, the LSP / APPLICANT must: • Encrypt with a password • Perform an anti-virus/malware/spyware scan on the device prior to entry into the secure environment • 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 by management
Data Protection	2.0	2.3	When on-site repairs are made to computer systems containing Buyer information, LSP / APPLICANT IT personnel should be present at all times. LSP / APPLICANT Must: a) Maintain a log providing repair details, individuals involved, disposition of disposed equipment as result of repairs. b) Have a valid, active NDA obligating the service providers to retain as confidential LSP / APPLICANT IP and confidential information of LSP / Applicant's Buyers c) Policy and procedures must cover repair during emergency circumstances and non-business hours
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 and protected as required by most restrictive data classification level.

Section	Section #	Requirement #	Requirement
Data Protection	2.0	2.5	For LSP / Applicant facilities which have return operations (customer returns), the following would apply: a) The LSP / Applicant must have policies and practices in place to protect any information which 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 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 / APPLICANT facility (*), such Buyer owned IT equipment (e.g., network and server) located at LSP / Applicant's facility(is) must be stored as follows: a. in physically secured and access-controlled IT room(s) b. have active alarms (if door held open, or opened without proper access) c. have a solid ceiling (or some similar mitigation) d. have a motion detector in the room (attached to the alarm system) e. must be covered by video monitoring * 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 assets b. the location of device(s) c. Identification of all devices upon which Buyer data resides.
Network Security	3.0	3.3	LSP / APPLICANT must use practices in line with current industry standards which protect their enterprise network on to which Buyer information is processed. i.e., NIST, ISO 27001

Section	Section #	Requirement #	Requirement
Network Security	3.0	3.4	LSP / APPLICANT must employ an external security audit or penetration testing which includes the LSP / Applicant's access control systems. This should be done on an annual basis. Testing should be conducted by an independent 3rd party. LSP / APPLICANT must address and / or close any gaps identified from the penetration testing. This process should be documented
Network Security	3.0	3.5	LSP/ APPLICANT must have a policy / procedure which specifies, at least every 90 days, a review of access to LSP / APPLICANT's Information Systems. Upon completion, access for all employees / contractors must be revalidated by management approval. Access must be terminated for any employees / contractors who do not have a valid need for revalidation.
Wireless Networks	4.0	4.1	Wireless networks must be secured with at least WPA2 and be limited to LSP / APPLICANT personnel. Guest networks must be for guest use only and not have any LSP/Applicant or buyer's devices or systems connect through them Guest or visitors must not be allowed access to LSP / APPLICANT'S network. 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. The LSP / APPLICANT must train employees and contingent staff of these risks and it must be documented in training materials. Formal training must complete an annual review quarterly via memoranda, virtual meeting or in-person training.

Section	Section #	Requirement #	Requirement
Remote Access	5.0	5.2	LSP/Applicant must complete a review every 90 days of accounts which have remote access to LSP/Applicant systems. This review will include: 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 e) For example: an essential supply chain software vendor or a partner LSP f) Have plans for securing remote access due to external cyber threat Note: If user accounts have remote access capability via VPN (or similar) this review should be done at the same time as Control 3.5
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 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 access should be done every 180 days d) Termination of admin rights must be done immediately upon termination or change in role within the company

Section	Section #	Requirement #	Requirement
User Account Management	6.0	6.2	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. e) Users must be required to change passwords on initial login.
User Account Management	6.0	6.3	LSP/Applicant must have a documented policy / procedure which outlines the steps regarding an employee's/contractor's termination or change of role. LSP / APPLICANT must immediately terminate physical and logical access to LSB / APPLICANT'S information systems as applicable.

Section	Section #	Requirement #	Requirement
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: ● 8-11 characters: mixed case letters, numbers and symbols. ● 12-15 characters: mixed case letters and numbers. ● 16-19 characters: mixed case letters. ● 20+ characters: no restrictions. 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 (e.g.,!@#$%^&*()_+|~-=\`{}[]:";'<>?,./) 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 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. They must have a documented policy.

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. Consequences for sharing passwords should be outlined in policies 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). This must be documented in a policy
Identification, Authentication, and Access	7.0	7.5	LSP / APPLICANT must have in place an appropriate use policy regarding information systems. Consequences for violating use policy should 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. Any failed access attempts must be investigated. Investigations must be conducted in accordance with the incident handling policy. Review must be done by IT Management. This must be documented in a policy.

Section	Section #	Requirement #	Requirement
Information Security Awareness Training	8.0	8.1	The LSP / APPLICANT must provide information security awareness training to employees. The training must include the roles and responsibilities computer users play in maintaining cyber security for the LSP / APPLICANT. a. Training to provide employee basic knowledge and training to execute their day-to-day responsibilities in a secure manner and in accordance with LSP / APPLICANT policies and procedures to include: • Protection practices against social engineering, phishing, malware, etc. • Access requirements to the LSP / APPLICANT's Information Systems • How to report a suspected security incident (phishing email for example) • How to report suspected or inadvertent sharing of Buyer confidential information b. Training be done as part of orientation, with focus as appropriate depending upon job responsibilities, and repeated a at least annually for all personnel with IT access. (The above is not an exhaustive list of subjects to include in the training) *This must be a documented policy.*
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 for a minimum of 4 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 effectiveness and understanding of cyber security training. This should be done at a minimum on a quarterly basis

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. Portable computer devices, such as tablets, laptops, phones, computers, must be access locked (screen locked, with a password) when not in use. This must be a documented policy.
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). Encryption level should be TLS 1.2 or a comparable or higher standard. *This must be a documented policy.*
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 from emails, external storage devices etc.) This must be a documented policy.
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
Configuration Management	12	12.2	The LSP / APPLICANT must apply and maintain documentation for the current configuration (imaging), and change-management procedures to the following systems, utilizing a change management board / process: a) All computer systems containing Buyer's information b) The centralized computing resources upon which these systems depend 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 which would involve patching of vulnerable systems and/or applying other controls. a) Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. b) The patch policy must state a time frame for review and implementation of issued patches by software provider. c) If a patch or an update for a critical flaw, i.e., zero-day vulnerability, is announced, a policy should be placed to immediately implement the patch.
Intrusion Detection and Prevention Systems	14	14.1	The LSP / APPLICANT'S 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. This must be a documented policy.
Intrusion Detection and Prevention Systems	14	14.2	The LSP / APPLICANT must establish a written process 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 1 year. Note: 1 year retention is the TAPA requirement. Local laws / regulations may require a longer 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. If the breach is a confirmed breach, notification to Buyer must be immediate. The LSP/Applicant must review perform an annual review which includes a tabletop exercise on the incident management policies and procedures.
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.
Environmental Controls	16	16.1	LSP / APPLICANT must ensure that clean, reliable electrical power is provided for critical computing infrastructure and computer equipment containing Buyer assets. a) Un-Interrupted Power Supply (UPS) must be capable of providing adequate power until (i) alternate power systems, such as a generator or secondary circuit, are activated, or (ii) computer systems are shut down according to manufacturer specifications. 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. b) The UPS should be tested annually to confirm the UPS system is operating at levels per the UPS specification.
Environmental Controls	16	16.2	The LSP / APPLICANT data center or computer room should be equipped with a fire suppression mechanism and maintained in accordance with applicable state / regional laws and regulations.

Section	Section #	Requirement #	Requirement
Third-party Service Delivery Management	17	17.1	LSP / APPLICANT must have a documented process 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 should include the requirements on allowing access by external parties to information process facilities and follow up checks.
Third-party Service Delivery Management	17	17.2	LSP / APPLICANT must annually audit third parties, who have any electronic transactions (access, have visibility of, house or receive data for the LSP), to ensure compliance with TAPA cyber security information security requirements. This must include review of processes and procedures for integrations and remote access into systems.
Cloud Services Security	18	18.1	A 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 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. Ability to provide proof that Buyer information has been security deleted upon termination of services or at Buyer's request. *This must be a documented policy.*
Security in Business Continuity Planning	19	19.1	The LSP / APPLICANT must have appropriate business continuity plans (BCP) for recovering from compromised system attacks, including but not limited to, all necessary data and software back-up and recovery arrangements. This must be a documented policy.

Section	Section #	Requirement #	Requirement
Back-up 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 if transferred to a secondary location. If backed-up onsite 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. 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 This must be a documented policy.