INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

Multi-Tiered Cloud Security Standard for Singapore (MTCS SS584:2015) Gap Analysis Report

For harmonisation of MTCS SS with ISO/IEC 27018:2014

October 2015

Revision History

Revision Date	Version	Updated by	Description
October 2015	1.0	IDA	Initial release

Disclaimer

The information provided in this Gap Analysis Report is for general information purposes only. The Gap Analysis Report is provided "AS IS" without any express or implied warranty of any kind. Whilst the Working Group (defined below), Infocomm Development Authority of Singapore (IDA) and / or individual contributors thereof have made every reasonable effort to ensure that the information contained herein are obtained from reliable sources and that any opinions and / or conclusions drawn there from are made in good faith, to the extent not prohibited by law, the Working Group and IDA, and their respective employees, agents and / or assigns shall not be responsible or liable for reliance by any person on the information, opinions and / or conclusions contained herein. The Working Group and IDA, and their respective employees, agents and / or assigns shall not be liable for any direct, indirect, incidental or consequential losses arising out of the use of the Gap Analysis Report. The Working Group and IDA are entitled to add, delete or change any information in the Gap Analysis Report at any time at their absolute discretion without giving any reasons.

The Multi-Tiered Cloud Security Harmonisation Working Group was a joint project by the Infocomm Development Authority (IDA) and Microsoft Singapore to assist in the preparation of this report. It comprises the following members:

	Name	
Project Sponsors		
	Dr. Hing-Yan Lee	IDA
	Erick Stephens	Microsoft
Facilitator	Tao Yao Sing	IDA
Secretary	Dr. Aaron Thor	IDA
Members	Darryn Lim	Microsoft
	Gary Lim	Microsoft
	Alfred Wu Hoi	Microsoft
	Antony Ma	IDA

The Multi-Tiered Cloud Security Harmonisation Focus Group on harmonisation of ISO27018 with MTCS SS584:2015 was appointed by IDA to assist in providing professional insights, verification and endorsement of this report. It comprises the following experts:

Dave Cheng	Certification International (Singapore)
Ros Oh	DNV Business Assurance Singapore
Lee Lai Mei	SGS International Certification Services Singapore
Christian Weidinger	TÜV Rheinland Singapore
Chris Ng	TÜV SÜD PSB
James Liu	Amazon Web Services
Alex Ng/Alan Ng	ClearManage
Edmund Tan	Acclivis Tech
Kenneth Yeo	Ascenix
Terence Ang	M1
Alan Woo	NewMedia Express
David Loke	ReadySpace
Septika/Sendang	Telin Singapore
Michael Mudd	Open Computing Alliance
Dr. Lam Kwok Yan	Association of Information Security Professionals
Aloysius Cheang	Cloud Security Alliance
John Lim	Information Systems Audit and Control Association
Dr. Chen Yuan Yuan	National University of Singapore
Prof. Anwitaman Datta	Nanyang Technological University
Jeffrey Tan	Deloitte
Tan Shong Ye	PricewaterhouseCoopers

Please send questions and feedback to IDA_cloud@ida.gov.sg.

Contents

1 Normative References

The following source documents were referenced for the purpose of this report:

- Singapore Standard for Multi-Tiered Cloud Computing Security (MTCS SS). MTCS SS aims to encourage the adoption of sound risk management and security practices for cloud computing. MTCS SS provides relevant cloud computing security practices and controls for cloud users, auditors and certifiers to understand cloud security requirements, and for public Cloud Service Providers (CSPs) to strengthen and demonstrate the cloud security controls in their cloud environments.
- ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. ISO/IEC 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect PII in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. In particular, ISO/IEC 27018:2014 specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

2 Purpose of Document

This Gap Analysis Report is the first report in the set of three (3) documents to support the harmonisation between MTCS SS584:2015 and ISO/IEC 27018:2014. The purpose of each document is described in the diagram below.

Gap Analysis Report	Implementation Guideline Report	Audit Checklist Report
The purpose of the Gap Analysis Report is to provide an overview of the differences between the requirements listed in MTCS SS and the ISO/IEC 27018:2014 Standard. The information provided in this document aims to assist entities that are MTCS SS certified to adopt the ISO/IEC 27018:2014 Standard. CSPs that are MTCS SS certified will have to comply with the requirements stated in ISO/IEC 27018:2014 Standard that are not fully covered in MTCS SS.	The purpose of the Implementation Guideline Report is to assist CSPs that are MTCS SS certified to implement the ISO/IEC 27018:2014. The guidelines in the report will include recommendations on how to address or the close the gaps. However, the guidelines are generic and need to be tailored to each CSP's specific requirements.	The purpose of the Audit Checklist Report is to guide auditors, including internal audit function, ISO/IEC 27018:2014 Certification Bodies and external audit bodies in understanding additional requirements beyond MTCS SS. From the CSPs' perspective, this document serves as a general guide for them to understand the scope covered in ISO/IEC 27018:2014 certification audit when the scope of MTCS SS audit overlaps with scope of the ISO/IEC 27001:2013 audit.

3 Intended Audience

This Gap Analysis Report is intended for CSPs that are MTCS SS Level 2 or Level 3 certified who are interested in complying with ISO/IEC 27018:2014.

It is also intended to guide auditors, including internal audit function, ISO/IEC 27001:2013 Certification Bodies and external audit bodies on the differences between ISO/IEC 27018:2014 Standard and MTCS SS.

4 Document Structure

This document has the following structure from this section onwards. Sections 6, 7 and 8 have introduction statements that will explain the section's background and context in more details.

- Section 5 – Terms and Definitions
- Section 6 – Approach
- Section 7 – Summary of Findings
- Section 8 – Gap Analysis

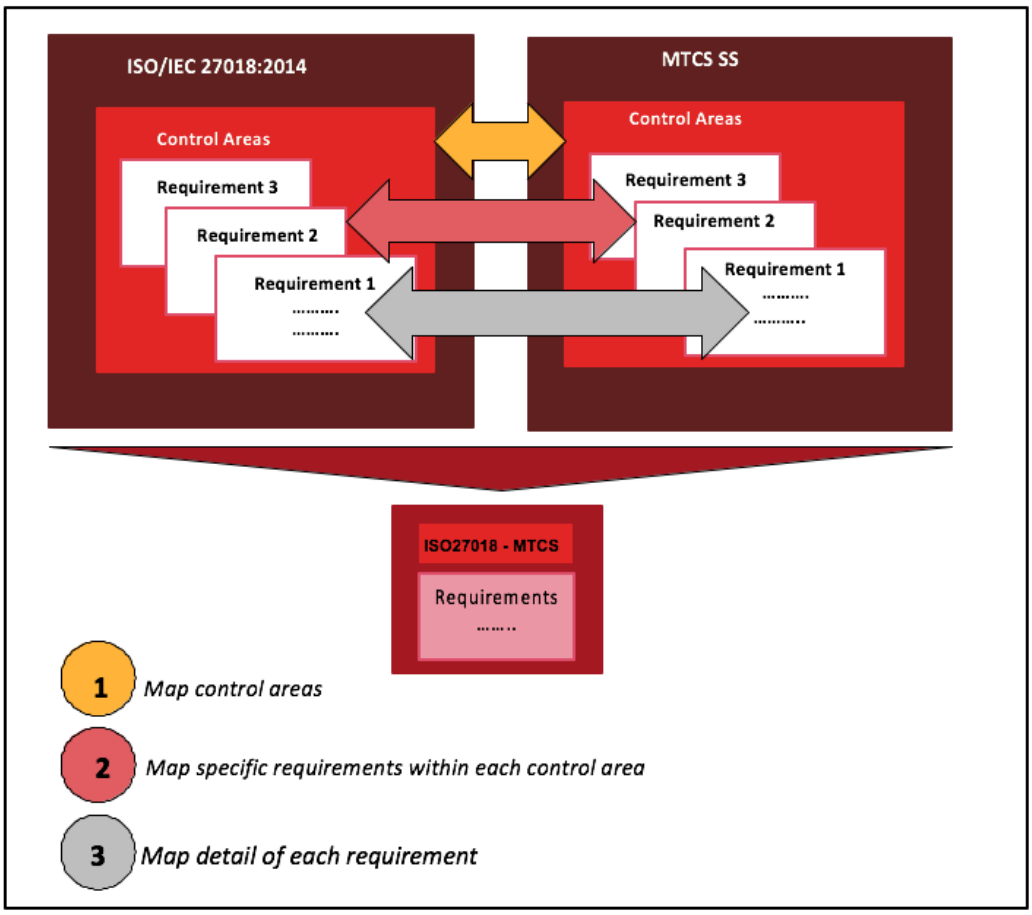
5 Terms and Definitions

PII-related terms used in this report are defined in ISO/IEC 27018:2014, and cloud-related terms used in this report are defined in MTCS SS.

6 Approach

In order to assist CSPs that are MTCS SS-certified to adopt ISO/IEC 27018:2014, requirements listed in MTCS SS were mapped against equivalent requirements in ISO/IEC 27018:2014. This followed a structured and systematic 3-step approach.

Note that the mappings to ISO/IEC 27018:2014 were only made for MTCS SS Level 2 and Level 3 requirements, as MTCS SS Level 1 requirements are only applicable for hosting of public information that does not include any PII.



7 Summary of Mapping

Of the 98 clauses in ISO27018:2014, only 39 clauses were found to include public cloud PII protection implementation guidance. Hence, only these 39 PII related clauses with breakdowns of the extent of coverage by MTCS SS are shown in table below, were considered for mapping between ISO27018:2014 and MTCS SS.

However, for completeness of mapping to other clauses, please refer to the Gaps Analysis Report on cross-certification from MTCS SS to ISO/IEC 27001:2013, available from https://www.ida.gov.sg/programmes-partnership/small-and-medium-enterprises/initiatives/MTCS-Certification-Scheme

Coverage description	Number of PII clauses	Percentage of PII clauses (%)
The requirements in ISO27018 are not covered in MTCS SS	4	10.3
The requirements in ISO27018 are partly covered in MTCS SS, i.e. some gaps exist	19	48.7
The requirements in ISO27018 are fully covered in the MTCS SS, i.e. no gap exists.	16	41
Total:	39	100

8 Gap Analysis

CSPs that are MTCS SS Level 2 or Level 3 certified, and are interested in complying with ISO/IEC 27018:2014 can view the key areas that need to be addressed in Tables 1 and 2, where the requirements of ISO27018 are partly covered or not covered in MTCS SS. Table 3 shows requirements in ISO27018 that are fully covered in MTCS SS.

Table 1: The following requirements in ISO27018 are not covered in MTCS SS.

ISO 27018 clause number	Clause title	Description of key controls	Reference to matching MTCS clauses	Reference to matching MTCS sub-clauses	MTCS SS Level 2 coverage	MTCS SS Level 3 coverage
A1.1	Obligation to cooperate with rights of PII principals	The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principal's rights to access, correct and/or erase their PII. Where the PII controller depends on the cloud PII processor for information or technical measures to facilitate the exercise of PII principals' rights, the relevant information or technical measures should be specified in the contract.	-	-	Not specifically covered in the MTCS.	
A2.1	Purpose limitation	PII processed under contract should not be processed for any purposes independent of the instructions of the cloud service customer.	-	-	Not specifically covered in the MTCS.	
A2.2	No commercial use	PII processed under contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without consent.	-	-	Not specifically covered in the MTCS.	
A5.1	Disclosure notification	Notify the cloud service customer of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.	-	-	Not specifically covered in the MTCS.	

Table 2: The following requirements in ISO27018 are partly covered in MTCS SS.

ISO 27018 clause number	Clause title	Description of key controls	Reference to matching MTCS clauses	Reference to matching MTCS sub-clauses	MTCS SS Level 2 coverage	MTCS SS Level 3 coverage
5.1.1	Policies for information security	The information security policies should be augmented by a privacy policy containing a statement concerning support for and commitment to managing compliance with applicable PII protection legislation and the contractual terms agreed between the cloud PII processor and its clients (cloud service customers). Contractual agreements should clearly allocate responsibilities between the public cloud PII processor, its sub-contractors and the cloud service customer. A mechanism to ensure the cloud PII processor is obliged to support and manage compliance is provided by the contract between the cloud service customer and the cloud PII processor. The contract could call for independently audited compliance, acceptable to the cloud service customer	9.2 9.3 10.1	9.2.2 9.3.3 10.1.2	MTCS clauses 9.2.2(a), 9.3.3(a), and 10.1.2(a) address the roles & responsibilities as between the CSP and 3rd party service providers, and also the CSP's compliance with applicable statutory, regulatory and contractual requirements including data protection, privacy of PII. However, there is no express requirement in the MTCS for the CSP's contractual agreements to allocate responsibilities between the CSP and the CSP's customer.	
6.1.1	Information security roles and responsibilities	The public cloud PII processor should designate a point of contact for use by the cloud service customer regarding processing of PII under the contract.	6.7	6.7.3	(MTCS SS Level 2 and above) MTCS clauses 6.7.1 and 6.7.3(a) require the CSP to designate information security liaison personnel for customers to contact. However, it is unclear whether the responsibilities of the ISL would include attending to issues regarding the processing of PII in accordance to applicable statutory, regulator and contractual requirements.	
10.1.1	Cryptography	The public cloud PII processor should provide information to the cloud service customer regarding the circumstances in which it uses cryptography to protect the PII it processes and provide information about any capabilities it provides that may assist the cloud service customer in applying its own cryptographic protection.	17.1 17.2 17.3 17.4	17.1.2 17.2.2 17.3.2, 17.3.3 17.4.2	(MTCS SS Level 1 and above) The use of cryptography by CSP to protect PII is clearly stated in MTCS (clause 17). However, MTCS does not explicitly require the CSP to provide (i) information on the circumstances in which it uses cryptography to protect PII or (ii) information that may assist the CSP's customer in applying its own cryptographic protection.	

11.2.7	Secure disposal or re-use of equipment	For the purposes of secure disposal or re-use, equipment containing storage media that may possibly contain PII should be treated as though it does.	12.8 12.9	12.8.2 12.9.3	Although MTCS clauses 12.8.2 and 12.9.3 cover secure disposal and removal of data in media (MTCS SS Level 1 and above) and the entire cloud environment (MTCS SS Level 2 and above), MTCS does not cover the specific situation with regard to the re-use of equipment.
12.1.4	Separation of development, testing and operation environments	Where the use of PII for testing purposes cannot be avoided, a risk management assessment should be undertaken and measures implemented to minimise the risks identified.	16.3	16.3.2 16.3.3	MTCS clauses 16.3.2 (MTCS SS Level 1 and above) and 16.3.3 (MTCS SS Level 2 and above) prohibit the use of production data for testing/development unless certain safeguards are met. MTCS does not specifically require a risk management assessment to be undertaken where PII needs to be used for testing purposes.
12.3.1	Information backup	Multiple copies of data in physically and/or logically diverse locations should be created or maintained for the purposes of backup and/or recovery. Restoration should be possible within a specific, documented period after a disruption event. Backup procedures should be reviewed at a specific, documented frequency. The cloud PII processor should have a policy which addresses the requirements for backup of information and any further requirements (e.g. contractual and/or legal requirements) for the erasure of PII which backed up information may contain.	12.7 12.9	12.7.2 12.9.3	MTCS clause 12.7.2 requires CSPs to establish and implement backup procedures in alignment with the committed services and scope of recovery, and to determine the frequency of testing and the access and storage locations of the backups (MTCS SS Level 1 and above). MTCS clause 12.9.3 also requires CSPs to verify the deletion of backup data (MTCS SS Level 2 and above). However, MTCS does not have an explicit requirement for the CSP to (i) create multiple copies of data in physically and/or diverse locations, (ii) have a specific, documented period within which data should be restored, or (iii) review the backup procedures at a specific documented frequency.
13.2.1	Information transfer policies and procedures	Record incoming and outgoing physical media containing PII, including the type of physical media, the authorized sender/recipients, the date and time, the number of physical media, and the types of PII they contain.	12.4 12.5	12.4.3 12.5.2, 12.5.3	Although MTCS clauses 12.4 and 12.5 cover data labelling/handling and data protection (MTCS SS Level 1 and above), MTCS does not specifically require incoming/outgoing physical media containing PII to be recorded (or the details required under ISO 27018).
16.1.1	Responsibilities and procedures for security incidents	Any security incident should trigger a review by the public cloud PII processor, as part of its information security incident management process, to determine if a data breach involving PII has taken place.	11.1 11.2 11.3 11.4	11.2.2, 11.2.3	MTCS clause 11 requires CSPs to implement, maintain and periodically test and update information security incident response plans and procedures (MTCS SS Level 1 and above). However, MTCS does not specifically require a review / examination / analysis of security incidents to determine if a data breach involving PII has taken place.

18.2.1	Independent review of information security	Where individual cloud service customer audits are impractical or may increase risks to security, independent evidence that information security is implemented and operated in accordance with the public cloud PII processor's policies and procedures should be made available.	10.2	10.2.2	Although MTCS clause 10.2.2 requires the CSP to have independent reviews and assessments performed for policies and standards that have bearing on the relevant cloud service (MTCS Level 1 and above), MTCS does not specifically require the CSP to make available independent evidence of the CSP's implementation and operation of information security in accordance with the CSP's policy and procedures.	
A4.1	Erase temporary files	Temporary files and documents should be erased or destroyed within a specified, documented period.	12.6 12.8	12.6.4 12.8.2	MTCS clause 12.6.3 require CSPs to have secure deletion or removal procedures when data is no longer needed (MTCS SS Level 2). Additionally, MTCS clause 12.8.2 requires CSPs to ensure that media that is no longer required is securely wiped or disposed of (MTCS SS Level 1 and above). However, MTCS does not require the CSP to specifically erase or destroy temporary files and documents or that such erasure or destruction should be within a specified, documented period.	MTCS clauses 12.6.3 and 12.6.4 require CSPs to have secure deletion or removal procedures when data is no longer needed (MTCS SS Level 2 and above), and to provide mechanisms for cloud users to remove or destroy all data (including backups) in the event of contract termination either on expiry or prematurely (MTCS SS Level 3 and above). Additionally, MTCS clause 12.8.2 requires CSPs to ensure that media that is no longer required is securely wiped or disposed of (MTCS SS Level 1 and above). However, MTCS does not require the CSP to specifically erase or destroy temporary files and documents or that such erasure or destruction should be within a specified, documented period.
A7.1	Disclosure of subcontracted PII processing	The use of sub-contractors should be disclosed to the cloud service customers before their use.	9.1 9.4	9.1.1 9.4.3	MTCS clause 9 requires CSPs to have in place an effective control framework over its third-party service providers (MTCS SS Level 1 and above). Additionally, under MTCS clause 5 and Annex A, the CSP can, but is not required to, indicate whether consent from the user is required before sub-contractors are used. However, MTCS does not specifically require the CSPs to actually disclose the use of sub-contractors to its cloud service customers before their use.	

A9.2	Retention of security policies and guidelines	Copies of security policies and operating procedures should be retained for a specified, documented period upon replacement (including updating)			MTCS sets out in a lot of detail what policies must be in place and what must be in these policies but it does not expressly require copies of the policies to be retained for a period upon replacement (Requirements throughout MTCS).	
A9.3	PII return, transfer and disposal	There should be a policy in respect of return, transfer and/or disposal of PII and this policy should be made available to the cloud service customer.	12.4 12.6 12.8 12.11 18.2	12.4.3(b) 12.6.3 12.6.4 12.8.2(c) 12.11.3(a) 18.2.3(a)	Although MTCS has all necessary controls for data handling (clauses 12.4, 12.11, 18.2) including clause 12.6.3 requiring CSPs to have secure deletion or removal procedures when data is no longer needed (MTCS SS Level 2 and above). Additionally, MTCS clause 12.8.2 requires CSPs to ensure that media that is no longer required is securely wiped or disposed of (MTCS SS Level 1 and above). However, MTCS does not require the CSP to make the disposition of PII policy available to its cloud service customers.	Although MTCS has all necessary controls for data handling (clauses 12.4, 12.11, 18.2) including clauses 12.6.3 and 12.6.4 requiring CSPs to have secure deletion or removal procedures when data is no longer needed (MTCS SS Level 2 and above), and to provide mechanisms for cloud users to remove or destroy all data (including backups) in the event of contract termination either on expiry or prematurely (MTCS SS Level 3 and above). Additionally, MTCS clause 12.8.2 requires CSPs to ensure that media that is no longer required is securely wiped or disposed of (MTCS SS Level 1 and above). However, MTCS does not require the CSP to make the disposition of PII policy available to its cloud service customers.
A10.1	Confidentiality agreements	Individuals under the public cloud PII processor's control with access to PII should be subject to a confidentiality obligation.	6.1 7.3 6.4	6.1.3 7.3.2 (a), (b), (d) 6.4.2 (a)	Although MTCS (clause 7) requires CSPs to have signed contracts with their employees and relevant third parties covering compliance with the CSPs responsibilities for information security, MTCS does not specifically require the employees or third parties to be subject to a confidentiality obligation.	
A10.2	Restriction on hard copy material	The creation of hardcopy material displaying PII should be restricted.	12.8	12.8.1 12.8.2 (c)	Although MTCS clauses 12.4 and 12.5 cover data labelling/handling and data protection (MTCS SS Level 1 and above), and MTCS clause 12.8 covers the secure destruction of hardcopy materials, MTCS does not specifically require the CSP to have any restrictions on the creation of hardcopy materials displaying PII.	

A10.3	Log of data restoration	There should be a procedure for, and log of, data restoration efforts.	12.7 13.3 19.6 21.2	12.7.1, 12.7.2 13.3.1, 13.3.2 19.6.3 21.2.2(c)	Although MTCS (clause 13) requires CSPs to track and monitor all access to network resources and system component, it does not explicitly require the CSP to have a procedure for, or log of, data restoration efforts.
A10.9	Records of authorized users	An up-to-date record of the users or profiles of users who have authorized access to the information should be maintained.	23.1	23.1.1	Although MTCS (clause 23) requires the CSP to establish a formal user registration process to grant, modify and restrict user access to the cloud services (MTCS SS Level 1 and above), there is no specific requirement for user records or profiles to be kept up-to-date.
A10.10	User ID management	De-activated or expired user IDs should not be granted to other individuals.	7.3 23.1	7.3.2 (c) 23.1.1	Although MTCS (clause 23) requires the CSP to establish a formal user registration process to grant, modify and restrict user access to the cloud services (MTCS SS Level 1 and above), there is no specific requirement to ensure that de-activated or expired user IDs are not to be granted to other individuals.
A10.11	Contract measures	Contracts between the cloud service customer and the public cloud PII processor should specify the minimum technical and organisation measures to ensure that the security measures are in place and that data is not processed for any purpose independent of the instructions of the customer. These measures should not be subject to unilateral reduction by the public cloud PII processor.	10.1 12.2	10.1.2 12.2.1, 12.2.3	MTCS clause 10.1 requires CSPs to identify, create and maintain documentation pertaining to applicable statutory requirements (based on applicable laws where CSP's data centres are located), regulatory requirements and contractual requirements (including data protection, privacy of personal information and intellectual property rights) (MTCS SS Level 1 and above). However, MTCS does not actually impose any: (i) requirement for the CSP to have a contract with the cloud service customer, or to ensure that the contract includes minimum technical and organisation measures to ensure that the CSP has security measures are in place and ensure that data is not processed for any purpose independent of the instructions of the customer; or (ii) restriction against the CSP unilaterally reducing its security measures.

Table 3: The following requirements in ISO27018 are fully covered in MTCS SS.

ISO 27018 clause number	Clause title	Description of key controls	Reference to matching MTCS clauses	Reference to matching MTCS sub-clauses	MTCS SS Level 2 coverage	MTCS SS Level 3 coverage
7.2.2	Information security awareness, education and training	Measures should be put in place to make relevant staff aware of the possible consequences of breach of privacy or security rules and procedures, especially those addressing the handling of PII			MTCS requires the CSP to develop and implement a training programme on information security incident management procedures and instil individuals' responsibility to report all information security events or incidents in a timely manner (Requirement 7.6).	
9.2	User access management	The public cloud PII processor should enable the cloud service customer to manage access by cloud service users under the cloud service customer's control, such as by providing administrative rights to manage or terminate access.	23.9	23.9.1 23.9.2 23.9.3	CSP has a self-service portal for management of user accounts (with provisions to manage access and specify restrictions for users). (MTCS SS Level 1 & Level 2) (Requirements 23.9.1, 23.9.2, 23.9.3)	
9.2.1	User registration and de-registration	Procedures for user registration and de-registration should address the situation where user access control is compromised, such as the corruption of password or other user registration data	22.4		MTCS requires the CSP to implement a formal process to ensure that unauthorised access attempts are detected and terminated in a timely manner (Requirement 22.4).	
9.4.2	Secure log-on procedures	The public cloud PII processor should provide secure log-on procedures for any account requested by the cloud service customer for cloud service users under its control.	23.2	23.2.3	MTCS has detailed requirements about the login process (clause 23.2), and specifically requiring the implementation and making available a 2FA mechanism (secure login) for users. (MTCS SS Level 2) (Requirement 23.2.3)	
12.4.1	Event logging	A process should be in place to review event logs to identify irregularities and propose remediation measures. Event logs should record whether or not PII has been changed and by whom. The public cloud PII processor should define how log information can be made available to the cloud service customer. The cloud service customer should only be able to access records that relate to that cloud service customer's activities	13.1		MTCS requires the CSP to capture audit trails of user identification, event type and origination, data and time stamp, attempt status and affected data. Access to audit trails must be restricted using physical and logical user access controls (Requirement 13.1).	

12.4.2	Protection of log information	Log information may contain PII. Measures such as controlling access should be in place to ensure that log information is only used for its intended purposes	13.1		MTCS requires the CSP to restrict access to audit trails using physical and logical user access controls (Requirement 13.1).
A5.2	Recording of PII disclosures	Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time.	13		MTCS requires the CSP to ensure that activities performed and events occurred in the cloud environment are being tracked and maintained for a period of time to detect any unauthorised activities and to facilitate investigation and resolution in the event of security incidents (e.g. access violations) (Requirement 13).
A9.1	Notification of data breach involving PII	Unauthorised access to PII should be promptly notified to the cloud service customer.	11.1	11.1.2	MTCS requires CSPs to have in place internal and external communication and contact procedures in the event of a security breach (including information cloud users and relevant third parties). CSPs shall disclose any security breach to potentially affected customers within reasonable time after the detection of the security breach (Requirement 11.1.2).
A10.4	Storage media leaving the premises	PII on media leaving the premises should be subject to an authorisation procedure	18.2		MTCS requires that no equipment, information or software is taken off-site without prior authorisation (Requirement 18.2).
A10.5	Unencrypted portable storage media and devices	Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any used of such portable media and devices should be documented.	12.5 17.1	12.5.3 (c) 17.1.1, 17.1.2(b)	All end point devices (including portal physical media and portable devices) handling customer data should be protected with strong encryption in place and be restricted to certain authorised personnel (MTCS SS Level 2). Such situation (use of portable media and devices) does not arise.
A10.6	Encryption over public networks	PII transmitted over public data-transmission networks should be encrypted prior to transmission.	17.1 17.2	17.1.2(b), 17.2.2	MTCS clauses 17.1 and 17.2 require CSPs to ensure that encryption policies apply to sensitive information in-transit and in-storage (MTCS SS Level 1 and above), and that e-commerce and online transactions are also encrypted (MTCS SS Level 1 and above).
A10.7	Disposal of hardcopy materials	Hardcopy materials that are destroyed must be destroyed using methods such as cross-cutting, shredding, incinerating, pulping etc.	12.8	12.8.2	MTCS requires CSPs to securely dispose of hardcopies by shredding, incinerating or pulping (Requirement 12.8.2).
A10.8	Unique use of user IDs	If more than one individual has access to stored PII, then they should each have distinct user IDs.	22.1		MTCS requires CSPs to assign each user with a unique username (Requirement 22.1).
A10.12	Sub-contracting PII processing	Contracts between the public cloud PII processor and any sub-contractors that process PII should specify the minimum technical and organisation measures that meet the information security and PII protection obligations of the public cloud PII processor. These measures should not be subject to unilateral reduction by the sub-contractor	10.5	10.5.2	Not specifically covered but MTCS requires CSPs to have data protection regulatory requirements specified in third party contractual agreements (Requirement 10.5.2).

A10.13	Data on pre-used storage space	Whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer	12.8	12.8.2	MTCS requires CSPs to ensure media is wiped or destroyed of securely and safely when no longer required, using formal procedures. Equipment and storage media containing any sensitive data must be security overwritten and/or forensically erased. Data shall not be retrievable using forensic mechanisms (Requirement 12.8.2).
A11.1	Geographic location of PII	Specify and document the countries in which PII must possibly be stored.	12.4 12.10	12.4.3 (c) 12.10.3	CSP should clearly specify the location where data is stored and as per agreement with customers (MTCS SS Level2). Information on locations of all data in production and backup environments is available (MTCS SS Level 2).

<End of Gap Analysis Report>