MCMC MTSFB TC G030:2021

TECHNICAL CODE

INFORMATION AND NETWORK SECURITY - PERSONAL INFORMATION MANAGEMENT SYSTEM

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date : 24 August 2021

MCMC MTSFB TC G030:2021

Development of technical codes

The Communications and Multimedia Act 1998 ('the Act') provides for Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirement for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd (MTSFB) as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8688 8000
Fax: +60 3 8688 1000
http://www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
MCMC Centre of Excellence (CoE)
Off Persiaran Multimedia
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8320 0300
Fax: +60 3 8322 0115
http://www.mtsfb.org.my

Contents

Committee representation

This technical code was developed by Trust and Privacy Sub Working Group under the Security, Trust and Privacy Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB) which consists of representatives from the following organisations:

Celcom Axiata Berhad

Maxis Broadband Sdn Bhd

MEASAT Broadcast Network Systems Sdn Bhd

Provintell Technologies Sdn Bhd

Telekom Malaysia Berhad

Foreword

This technical code for Information and Network Security - Personal Information Management System (‘this ‘Technical Code’) was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd (MTSFB) via its Trust and Privacy Sub Working Group under the Security, Trust and Privacy Working Group.

This Technical Code is an extension to the MCMC MTSFB TC G009, *Information and Network Security - Requirements.*

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

INFORMATION AND NETWORK SECURITY - PERSONAL INFORMATION MANAGEMENT SYSTEM

0. Introduction

Most organisations are processing Personal Identifiable Information (PII) and the quantity and types of PII processed are increasing. In the business collaborations, there will be situations where an organisation needs to cooperate with other organisations regarding the processing of PII.

Protection of privacy in the context of processing PII is a societal need with the enforcement of legislation and/or regulation all over the world. Requirements and guidance for PII protection varies in the context of the organisation, particularly when national legislation and/or regulation exist.

The Information and Network Security (INS) management system defined in the MCMC MTSFB TC G009 specifies the requirements to establish, implement, maintaining and continually improving the information security within the context of an organisation. This Technical Code is designed as a Communications and Multimedia Industry (CMI) sector specific requirement for personal information management that shall be implemented as a combined management system with the MCMC MTSFB TC G009.

This Technical Code can be used by PII controllers (including joint PII controllers) and PII processors (including those using subcontracted PII processors and those processing PII as subcontractors to PII processors).

1. Scope

This Technical Code specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Personal Information Management Systems (PIMS) in the form of an extension to MCMC MTSFB TC G009 for PII management within the context of the organisation.

This Technical Code specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.

This Technical Code is applicable to all types and sizes of organisations, including public and private companies, government entities and not-for-profit organisations, which are PII controllers and/or PII processors processing PII within INS.

2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) applies.

MCMC MTSFB TC G009:2019, *Information and Network Security - Requirements*

ISO/IEC 27701:2019, *Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines*

ISO/IEC 29100, *Information technology - Security techniques - Privacy framework*

Act 588, *Communications and Multimedia Act 1998*

JPDP.100-1/1/10 (1), *Personal Data Protection Standard 2015*

3. Abbreviations

For the purposes of this Technical Code, the following abbreviations apply.

CMI	Communications and Multimedia Industry
ID	Identification
INS	Information and Network Security
MCMC	Malaysian Communications and Multimedia Commission
PDPC	Personal Data Protection Commissioner Malaysia
PIA	Privacy Impact Assessment
PII	Personal Identifiable Information
PIMS	Personal Information Management Systems

4. Terms and definitions

For the purposes of this Technical Code, the following terms and definitions apply.

4.1 Joint Personal Identifiable Information (PII) controller

PII controller that determine the purposes and means of the processing of PII jointly with one or more other PII controllers.

4.2 Personal Identifiable Information (PII)

Any information that:

a) can be used to establish a link between the information and the natural person to whom such information relates; or

b) can be directly or indirectly linked to a natural person.

According to the Act 709, *Personal Data Protection Act 2010*, PII can be referred to as “personal data”.

4.3 Personal Identifiable Information (PII) controller

Privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing PII other than natural persons who use data for personal purposes.

According to the Act 709, *Personal Data Protection Act 2010*, PII controller can be referred to as “data user”.

4.4 Personal Identifiable Information (PII) principal

Natural person to whom the PII relates.

According to the Act 709, *Personal Data Protection Act 2010*, PII principal can be referred to as “data subject”.

4.5 Personal Identifiable Information (PII) processor

Privacy stakeholder that processes PII on behalf of and in accordance with the instructions of a PII controller.

According to the Act 709, *Personal Data Protection Act 2010*, PII processor can be referred to as “data processor”.

4.6 Privacy risk assessment

Overall process of risk identification, risk analysis and risk evaluation with regard to the processing of PII.

This process is also known as a Privacy Impact Assessment (PIA).

4.7 Privacy stakeholder

Natural or legal person, public authority, agency or any other body that can affect, be affected by, or perceive themselves to be affected by a decision or activity related to PII processing.

4.8 Processing of Personal Identifiable Information (PII)

Operation or set of operations performed upon PII.

Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymisation, pseudonymisation, dissemination or otherwise making available, deletion or destruction of PII.

5. Overview

The implementation of this Technical Code shall be combined with the MCMC MTSFB TC G009 and the ISO/IEC 27701 as a whole. This Technical Code extends the requirements of INS to take into account the protection of privacy of PII principals as potentially affected by the processing of PII, in addition to information security.

This Technical Code directly refers to the requirements and guidelines specified in ISO/IEC 27701 listed below to be part of the implementation of this Technical Code:

a) Clause 7 of ISO/IEC 27701 - Implementation guideline for Annex A of ISO/IEC 27701;

b) Clause 8 of ISO/IEC 27701 - Implementation guideline for Annex B of ISO/IEC 27701;

c) Annex A of ISO/IEC 27701 - Normative PIMS-specific reference control and controls for PII controllers; and

d) Annex B of ISO/IEC 27701 - Normative PIMS-specific reference control and controls for PII processors.

6. Requirements related to MCMC MTSFB TC G009

For this clause, INS is referred to as “information security and privacy” instead of “information security”.

6.1 General

In MCMC MTSFB TC G009, information security shall be extended to the protection of privacy as potentially affected by the processing of PII.

6.1.1 Customer

Depending on the role of the organisation (refer to 5.2.1 of MCMC MTSFB TC G009), “customer” can be understood as either:

a) an organisation who has a contract with a PII controller, i.e., the customer of the PII controller;

NOTES:

1. This can be the case of an organisation which is a joint controller.

2. An individual person in a business to consumer relationship with an organisation is referred to as a “PII principal” in this Technical Code.

b) a PII controller who has a contract with a PII processor, i.e., the customer of the PII processor; or

c) a PII processor who has a contract with a subcontractor for PII processing, e.g., the customer of the subcontracted PII sub-processor.

6.2 Organisation context

6.2.1 Understanding context of organisation

The requirements of MCMC MTSFB TC G009 shall be extended to the protection of privacy as potentially affected by the processing of PII.

The organisation shall determine its role as PII controller (including as joint PII controller), and/or PII processor. When the organisation acts in both roles (as a PII controller, as well as a PII processor), separate roles shall be determined, each of which is the subject of a separate set of controls.

The organisation shall determine internal and external issues that are relevant to its purpose and that affects its ability to achieve the intended outcome(s) of this Technical Code. The issues shall include:

a) applicable privacy legislation;

b) applicable regulations;

c) applicable judicial decisions;

d) applicable organisational context, governance, policies and procedures;

e) applicable administrative decisions; and

f) applicable contractual requirements.

NOTE: The role of the organisation can be different for each instance of the processing of PII, since it depends on who determines the purposes and means of the processing.

6.2.2 Understanding the expectation of interested parties

The organisation shall include its interested parties (refer 6.1.2 of MCMC MTSFB TC G009), those parties with interests or responsibilities associated with the processing of PII, including the PII principals.

NOTES:

1. Other interested parties can include customers (refer 6.1.1), supervisory authorities, other PII controllers, PII processors and their subcontractors.

2. Requirements relevant to the processing of PII can be determined by legal and regulatory requirements, by contractual obligations and by self-imposed organisational objectives. The privacy principles set out in ISO/IEC 29100 provide guidance concerning the processing of PII.

3. The 7 Personal Data Protection Principles of Act 709, *Personal Data Protection Act 2010* in Annex A provides legal and regulatory requirements concerning the processing of PII in Malaysia.

4. As an element to demonstrate compliance to the organisation's obligations, some interested parties can expect that the organisation to be in conformity with specific standards, such as the INS management system specified in this Technical Code and/or any relevant set of specifications. These parties can call for independently audited compliance to these standards.

6.2.3 Determining the scope of INS management system

In addition to the requirements specified in 5.1.3 of MCMC MTSFB TC G009, the organisation shall include the processing of PII to determine the scope of PIMS.

6.2.4 INS management system

In addition to the requirements in 5.1.4 of MCMC MTSFB TC G009, the organisation shall establish, implement, maintain and continually improve the PIMS in accordance with the requirements of clauses 5 to 10 of MCMC MTSFB TC G009, extended by the requirements in 6.2.1 to 6.2.3.

6.3 Risk management

6.3.1 General

In addition to the requirements specified in 5.2.1 of MCMC MTSFB TC G009, the organisation shall consider the context of processing PII that is specified in 6.2.1.

6.3.2 Risk management process

In addition to the requirements specified in the 5.2.2 of MCMC MTSFB TC G009, the organisation shall include the scope of this Technical Code in the information security risk assessment process.

The organisation shall apply privacy risk assessment process to identify risks related to the processing of PII, within the scope of this Technical Code. The relationship between information security and PII protection shall be managed appropriately throughout the risk assessment processes.

NOTES:

1. The organisation can either apply for integrated information security and privacy risk assessment process or to separate ones for information security and the risks related to the processing of PII.

2. The organisation may refer to ISO/IEC 29134, *Information technology - Security techniques - Guidelines for privacy impact assessment* to develop the privacy risk assessment process.

6.3.3 Communication and consultation

The requirements specified in 5.2.3 of MCMC MTSFB TC G009 shall apply.

Additionally, the communication seeks to address the issues relating to the impact on the various privacy stakeholders, the possible consequences, and the measures to manage the issues.

6.3.4 Scope, context and criteria

The requirements stated in 5.2.4 of MCMC MTSFB TC G009 shall apply.

In addition, when establishing the context, the organisation shall include the scope of PIMS specified in 6.2.1 in its risk management in processing PII.

6.3.5 INS risk assessment

The requirements specified in 5.2.5 of MCMC MTSFB TC G009 shall apply.

Furthermore, the risk assessment process shall comprise risk identification, risk analysis and risk evaluation within the scope of this Technical Code.

6.3.5.1 Risk identification

The requirements specified in 5.2.5.1 of MCMC MTSFB TC G009 shall apply.

In addition, the organisation shall identify the risks of processing PII that will affect the intended outcome determined in 6.2.1.

6.3.5.2 Risk analysis

The requirements specified in 5.2.5.2 of MCMC MTSFB TC G009 shall apply.

In addition, the organisation shall analyse the potential consequences for both the organisation and PII principals that would result if the risks identified in 5.2.5.1 of MCMC MTSFB TC G009 were to materialise.

6.3.5.3 Risk evaluation

The requirements specified in 5.2.5.3 of MCMC MTSFB TC G009 shall apply.

6.3.6 Risk treatment

The requirements specified in 5.2.6 of MCMC MTSFB TC G009 shall apply.

Additionally, the controls determined in 5.2.6 of MCMC MTSFB TC G009 shall be compared with the controls in the following annexes to verify the necessary controls have been applied for risk treatment.

a) Annex A in MCMC MTSFB TC G009; and

b) Annex A and/or Annex B in ISO/IEC 27701.

The control objectives and controls shall be considered in the context of both risks to information security, as risks related to the processing of PII, including risks to PII principal.

Not all the control objectives and controls listed in the annexes in ISO/IEC 27701 need to be included in the PIMS implementation due to the roles in processing PII (refer to 6.2.1), legislation and/or regulation (not required by or are subject to exceptions). The organisation shall document the justification for their exclusion.

The requirement of Statement of Applicability specified in 5.2.6 of MCMC MTSFB TC G009 shall be refined to include the justification for excluding any other controls in the following annexes according to the organisation's determination of this role (refer to 6.2.1).

a) Annex A in the MCMC MTSFB TC G009; and

b) Annex A and/or Annex B in ISO/IEC 27701.

6.3.7 Monitoring and review

The requirements specified in 5.2.7 of MCMC MTSFB TC G009 shall apply.

6.3.8 Recording and reporting

The requirements specified in 5.2.8 of MCMC MTSFB TC G009 shall apply.

6.4 Objectives and planning

The requirements specified in 5.3 of MCMC MTSFB TC G009 shall apply.

6.5 Roles and responsibilities

6.5.1 Leadership and commitment

The requirements specified in 6.1 of MCMC MTSFB TC G009 shall apply along with the interpretation specified in 6.1.

6.5.2 Policy

The requirements specified in 6.2 of MCMC MTSFB TC G009 shall apply along with the interpretation specified in 6.1.

6.5.3 Roles, responsibilities within the organisation and authorities

The requirements specified in 6.3 of MCMC MTSFB TC G009 shall apply along with the interpretation specified in 6.1.

6.6 Support

6.6.1 Resources

The requirements specified in 7.1 of MCMC MTSFB TC G009 shall apply along with the interpretation specified in 6.1.

6.6.2 Competence

The requirements specified in 7.2 of MCMC MTSFB TC G009 shall apply along with the interpretation specified in 6.1.

6.6.3 Awareness

The requirements specified in 7.3 of MCMC MTSFB TC G009 shall apply along with the interpretation specified in 6.1.

6.6.4 Communication

The requirements specified in 7.4 of MCMC MTSFB TC G009 shall apply along with the interpretation specified in 6.1.

6.6.5 Documented information

The requirements specified in 7.5 of MCMC MTSFB TC G009 shall apply along with the interpretation specified in 6.1.

6.7 Operations

6.7.1 Operational planning and control

The requirements specified in 8.1 of MCMC MTSFB TC G009 shall apply along with the interpretation specified in 6.1.

6.8 Performance evaluation

6.8.1 Monitoring, measurement, analysis and evaluation

The requirements specified in 9.1 of MCMC MTSFB TC G009 shall apply.

6.8.2 Internal audit

The requirements specified in 9.2 of MCMC MTSFB TC G009 shall apply.

6.8.3 Management review

The requirements specified in 9.3 of MCMC MTSFB TC G009 shall apply.

6.9 Improvement

6.9.1 Nonconformity and corrective action

The requirements specified in 10.1 of MCMC MTSFB TC G009 shall apply.

6.9.2 Continual improvement

The requirements specified in 10.2 of MCMC MTSFB TC G009 shall apply.

7. Specific requirements related to Annex A of MCMC MTSFB TC G009

7.1 General

The control domains and controls in the Annex A of MCMC MTSFB TC G009 shall be extended to the protection of privacy as potentially affected by the processing of PII.

The Annex A in MCMC MTSFB TC G009 mentioning "information security" shall be extended to the protection of privacy as potentially affected by the processing of PII.

7.2 Organisation (Category 1)

7.2.1 INS policy

The controls specified in Annex A.2.1 of MCMC MTSFB TC G009 shall apply.

In addition, the organisation, whether as a PII controller or a PII processor, shall develop and maintain the privacy policies that produce the statement concerning the support and commitment to achieving compliance with the applicable PII protection legislation and/or regulation. The policies shall comply with the contractual terms agreed between the organisation and its partners, its subcontractors and its applicable third parties (customers, suppliers etc.), and the responsibilities shall be clearly allocated within the various parties.

7.2.2 Business continuity management

The controls specified in Annex A.2.2 of MCMC MTSFB TC G009 shall apply.

7.2.3 INS compliance

The controls specified in Annex A.2.3 of MCMC MTSFB TC G009 shall apply.

In additions, the organisation shall identify the potential legal sanctions related to the processing of PII from the following:

a) local supervisory authority; and

NOTES:

1. Personal Data Protection Commissioner Malaysia (PDPC) is the Malaysian local supervisory authority as a legislator where Act 709, *Personal Data Protection Act 2010* is applied.

2. Malaysian Communications and Multimedia Commission (MCMC) is the Malaysian local supervisory authority as regulator where Act 588, *Communications and Multimedia Act 1998* is applied.

b) contract between the organisation and the customer outlining their respective security, privacy and PII protection responsibilities.

The organisation shall comply with the following (but not limited to) technical compliance related to the processing of PII.

a) JPDP.100-1/1/10 (1), *Personal Data Protection Standard 2015*;

b) *The Personal Data Protection Code of Practice - For licensees under the Communications and Multimedia Act 1998*;

c) *General Consumer Code of Practice for the Communications and Multimedia Industry*; and

d) respective licensee's license conditions of the *Communications and Multimedia Act 1998*.

7.2.4 Organisation of information security

The controls specified in Annex A.2.4 of MCMC MTSFB TC G009 shall apply.

In addition:

a) the organisation shall designate a point of contact for use by the customer regarding the processing of PII, and by the PII principals when the organisation is the PII controller in regard to the processing of their PII; and

b) a person or a team shall be appointed to develop, implement, maintain and monitor the organisation-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding processing of PII.

The person should, where appropriate:

a) be independent and report directly to the appropriate management level of the organisation to ensure effective management of privacy risks;

b) be the contact point for supervisory authorities;

c) be involved to manage all issues related to the processing of PII;

d) be the communication channel to ensure top management and employees are told about their obligations with respect to the processing of PII;

e) provide advice in respect of privacy impact assessment conducted by the organisation; and

f) be the expert in data protection legislation, regulation and practise. In some jurisdictions, this person is called a data protection officer.

NOTE: This person can be fulfilled by a staff member or outsourced.

7.2.5 INS incident management

The controls specified in Annex A.2.5 of MCMC MTSFB TC G009 shall apply.

In addition, the organisation shall:

a) establish responsibilities and procedures for the identification and recording of breaches of PII as part of the information security incident management process; and

b) establish responsibilities and procedures related to notification to the required parties of PII breaches and the disclosure to authorities, including the timing of such notification in according to the applicable legislation and/or regulation.

7.3 Infrastructure (Category 2)

7.3.1 Asset management

The controls specified in Annex A.3.1 of MCMC MTSFB TC G009 shall apply.

7.3.2 Data/Information management

The controls specified in Annex A.3.2 of MCMC MTSFB TC G009 shall apply.

In addition, the implementation of the organisation's information classification shall explicitly consider PII as part of the MCMC MTSFB TC G009 management system. The organisation shall define type and/or categories of PII the organisation is processing, and where such PII is stored and data can flow through the systems.

When defining type and/or categories of PII, the organisation shall define (but not limited to):

a) sensitive personal data; and

b) personal data.

NOTE: Act 709, *Personal Data Protection Act 2010* defines race, religion, health, political opinion, and offence records as sensitive personal data.

The organisation shall ensure that people under its control are made aware of the definition of PII and how to recognise the information that is PII from the labelling of information.

7.3.3 Media management

The controls specified in Annex A.3.3 of MCMC MTSFB TC G009 shall apply.

In addition, the following requirements shall be considered in managing any media related to PII.

a) Any use of removable media and/or devices for the storage of PII within the organisation shall be documented.

b) Removable media intended to handle PII shall have functions for encryption or access control.

c) Secure disposal procedure of removable media where PII is store shall be included in the documented information and implemented to ensure the previous stored PII will not be accessible.

d) Incoming and outgoing physical media containing PII shall be recorded if information transfer through the physical media. The record shall include but not limited to:

   i) type of and number of physical media to transfer;

   ii) authorised sender / recipients; and

   iii) date and time or the transfer.

e) Physical media containing PII shall be encrypted before leaving its premises, to ensure the PII is not accessible to anyone other than the authorised personnel only.

7.3.4 Access control

The controls specified in Annex A.3.4 of MCMC MTSFB TC G009 shall apply.

7.3.5 User access management

The controls specified in Annex A.3.5 of MCMC MTSFB TC G009 shall apply.

In addition, the organisation shall not reissue to users any de-activated or expired users' identifications (IDs) for systems and services that process PII.

User authentication credentials related to systems that process PII shall be reviewed to ensure unused authentication credentials are disabled and/or removed on a regular basis. The frequency of review shall comply with the jurisdiction's requirements if applicable.

The user profiles for the users who have been authorised to access the information system and the PII contained therein shall be kept up-to-date and accurate.

User access IDs shall be configured to enable the systems to identify who accessed PII, and changes such as additions and deletions they made.

Users shall be able to identify what they have processed to the PII.

In the case where the organisation is providing PII processing as a service, it's customer can be responsible for some or all aspects of the user ID and access management. The organisation should:

a) provide documented information about the ID management; and

b) provide the administrative rights to the customer to manage or terminate access.

7.3.6 Systems, services and application access control

The controls specified in Annex A.3.6 of MCMC MTSFB TC G009 shall apply.

7.3.7 Cryptography

The controls specified in Annex A.3.7 of MCMC MTSFB TC G009 shall apply.

In addition, the organisation shall apply the use of cryptography if it is required by the jurisdictions.

In the case where the organisation is providing PII processing as a service, the organisation should:

a) provide information regarding the circumstances in which it uses cryptography to protect the PII it processes; and/or

b) provide information to the customer about any capabilities it provides that can assist the customer in applying their own cryptographic protection, if applicable.

7.3.8 PII and network in operations

The controls specified in Annex A.3.8 of MCMC MTSFB TC G009 shall apply.

In addition, PII that is transmitted over untrusted data transmission networks shall be encrypted.

Untrusted networks can include the public internet and other facilities outside the operational control of the organisation.

NOTE: In some cases, the inherent characteristics of untrusted data transmission network systems can require that some header or traffic data be exposed for effective transmission. e.g., exchange of e-mail.

7.3.9 Malicious software protection

The control specified in Annex A.3.9 of MCMC MTSFB TC G009 shall apply.

7.3.10 Logging and monitoring

The control specified in Annex A.3.10 of MCMC MTSFB TC G009 shall apply.

In addition, event logs shall be configured to record access to PII including (but not limited to):

a) accessed by who;

b) when was the PII being accessed;

c) which PII principal's PII was accessed; and

d) what changes were made (additions, modifications, or deletions) as a result of the event.

In the case where processing of PII involved multiple service providers, the organisation shall ensure the roles are clearly defined in implementing event logging. Documented information shall be developed, and the agreement on any log access between providers shall be addressed.

For the organisations to act as the role of PII processor, the organisation should define the criteria regarding if the log information can be made available, when and how the log information can be made usable by the customer. Such criteria should be made available to the customer. When permission to access log records that is permitted to its customer, the organisation shall implement appropriate controls to ensure that the customer can only access to read records that relate to that customer's activities without permission to amend the logs in any way, access to any log records relate to other customers' activities shall be denied.

7.3.11 Control of operational software

The controls specified in Annex A.3.11 of MCMC MTSFB TC G009 shall apply.

7.3.12 Technical vulnerability management

The controls specified in Annex A.3.12 of MCMC MTSFB TC G009 shall apply.

7.3.13 Information and network audit

The controls specified in Annex A.3.13 of MCMC MTSFB TC G009 shall apply.

7.3.14 Backup

The controls specified in Annex A.3.14 of MCMC MTSFB TC G009 shall apply.

In addition, the organisation shall include the needs for backup, recovery and restoration of PII in the overall information backup policy. The backup policy shall consider the requirements for the erasure of PII contained in information held for backup required due to contractual and/or legal requirements.

7.3.15 Network communications security management

The controls specified in Annex A.3.15 of MCMC MTSFB TC G009 shall apply.

7.3.16 Information transfer

The controls specified in Annex A.3.16 of MCMC MTSFB TC G009 shall apply.

In addition, the organisation shall develop procedures to ensure the rules related to the processing of PII are enforced throughout and outside of the system, where applicable.

7.3.17 Security requirements of systems

The controls specified in Annex A.3.17 MCMC MTSFB TC G009 shall apply.

7.3.18 Security requirements for development and support processes

The control specified in Annex A.3.18 of MCMC MTSFB TC G009 shall apply.

In addition, the organisation shall include guidance for the organisation's processing of PII needs in the system development procedure. The procedure shall be based on obligations to PII principals and/or any applicable legislation and/or regulation and the types of processing performed by the organisation.

Systems and/or components related to the processing of PII shall be designed following the principles of privacy by design and privacy by default. The system design shall anticipate and facilitate the implementation of relevant controls (PII controllers and PII processors) to support the collection and processing of PII in the systems under conditions for collection and processing (refer to 7.2 of ISO/IEC 27701).

Policies to privacy by design and/or privacy by default shall be established. The organisation should consider the following aspects:

a) guidance on PII protection and the implementation of the privacy principles (refer ISO/IEC 29100) in the software development lifecycle;

b) privacy and PII protection requirements in the design phase, which can be based on the output from a privacy risk assessment and/or a privacy impact assessment (refer 7.2.5 of ISO/IEC 27701);

c) PII protection checkpoints within project milestones;

d) required privacy and PII protection knowledge; and

e) by default, minimize processing of PII.

The *Personal Data Protection Code of Practice - For Licensees Under the Communication and Multimedia Act 1998* shall be considered when developing the privacy by design and/or privacy by default policies.

NOTE: Clause 7 and 8 of ISO/IEC 27701 provide control considerations for processing of PII, which can be useful in developing policies for privacy in systems design.

7.3.19 System acquisition, development and maintenance

The controls specified in Annex A.3.19 of MCMC MTSFB TC G009 shall apply.

Additionally, the same principles in 7.3.18 shall be applied to the outsourced development.

False or synthetic PII should be used as test data. When use of PII for testing purpose cannot be avoided, the testing shall be performed in the production-equivalent testing environment to minimise the risks. Where such environment is not feasible, a risk-assessment shall be undertaken and used to inform the selection of appropriate mitigating controls.

7.4 People (Category 3)

7.4.1 Human resource security

The controls specified in Annex A.4.1 of MCMC MTSFB TC G009 shall apply.

In addition, formal awareness training or education program shall be implemented to the relevant staffs to ensure they are aware of consequences of breaching privacy or security rules and procedures, especially those addressing the handling of PII.

The awareness training should include (but not limited to):

a) legal consequences, loss of business and brand or reputational damage to the organisation;

b) disciplinary consequence to the staff member; and

c) physical, material and emotional consequences to the PII principals.

7.4.2 Supplier relationships

The controls specified in Annex A.4.2 of MCMC MTSFB TC G009 shall apply.

In addition, the supplier agreements in Annex A.4.2 b) of MCMC MTSFB TC G009 shall specify whether the supplier is processing PII. Besides, the supplier shall address the minimum technical and organisational measures that the supplier needs to meet (refer 7.2.6 and 8.2.1 of ISO/IEC 27701)

NOTE: The organisation shall refer to Clause 4 of Part 3 of *The Personal Data Protection Code of Practice - For Licensees Under the Communication and Multimedia Act 1998* to ensure the supplier can support the organisation to achieve the security principle.

7.5 Environment (Category 4)

7.5.1 Physical and environmental security

The controls stated in Annex A.5.1 of MCMC MTSFB TC G009 shall apply.

In addition, storage space to be re-assigned shall be verified to ensure that PII which had previously residing on a storage space is not accessible. Storage media used to store PII shall be security overwritten prior to disposal or re-use.

The organisation shall restrict the creation of hardcopy material containing PII to the minimum needed that is sufficient for the identified processing purpose.

8. Control objectives and controls for PII controllers

Annex A of ISO/IEC 27701 is the normative used by organisations acting as PII controllers, with or without the use of PII processor.

The additional or modified control objectives and controls in the Annex A of ISO/IEC 22701, Table A.1 are directly derived from and aligned with those defined in the ISO/IEC27701 and are to be used in the context of 5.3.6.

This Technical Code refers to the PIMS specific reference control objectives and controls for PII controllers to the Annex A of ISO/IEC 27701. Not all the control objectives and controls listed need to be included in the PIMS implementation.

A justification for excluding any control objectives where controls are not deemed necessary by risk assessment, and where they are not required by applicable legislation and/or regulation shall be documented.

Clause 7 of ISO/IEC 27701 provides the implementation guidelines relate to the controls listed in Annex A of ISO/IEC 27701. Organisation acting as PII controller should refer to this guideline when implementing the controls objectives in the Annex A of ISO/IEC 27701.

9. Control objectives and controls for PII Processors

Annex B of ISO/IEC 27701 is the normative used by organisations acting as PII processors, with or without the use of PII subcontractors.

The additional or modified control objectives and controls in the Annex A of ISO/IEC 22701, Table B.1 is directly derived from and aligned with those defined in the ISO/IEC27701 and are to be used in the context of 6.3.4.

This Technical Code refers to the PIMS specific reference control objectives and controls for PII processors to the Annex B of ISO/IEC 27701. Not all the control objectives and controls listed need to be included in this Technical Code implementation. A justification for excluding any control objectives where he controls are not deemed necessary by risk assessment, and where they are not required by applicable legislation and/or regulation shall be documented.

Clause 8 of ISO/IEC 27701 provides the implementation guidelines relate to the controls listed in Annex B of ISO/IEC 27701. Organisation acting as PII processors should refer to this guideline when implementing the controls objectives in the Annex B of ISO/IEC 27701.

Annex A
(normative)

7 Principles of data protection

7 Personal Data Protection Principles which shall be adhered to under section 5 (1) of the Act 709, *Personal Data Protection Act 2010* by maintaining the integrity of personal data:

a) General Principle

Personal data shall not be processed without CONSENT from the subjects.

b) Notice and Choice Principle

Data Subject shall be informed through written notice of the purpose personal data is being collected and processed and to whom they disclose it.

c) Disclosure Principle

PII shall not be disclosed for any other purposes other than the intended purpose.

d) Security Principle

Data User processing personal data shall take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

e) Retention Principle

PII shall not be kept longer than necessary for the fulfilment of the intended purpose.

f) Data Integrity Principle

PII controller shall be responsible to ensure personal data is accurate, complete, not misleading and kept up-to-date.

g) Access Principle

PII controller shall allow individual or customers (data subjects) to access their PII and the ability to correct the PII.

Bibliography

[1] ISO/IEC 27005, *Information technology - Security techniques - Information security risk management*

[2] ISO/IEC 29134, Information technology - *Security techniques - Guidelines for privacy impact assessment*

[3] ISO/IEC 29151, *Information technology - Security techniques - Code of practice for personally identifiable information protection*

[4] BS 10012, *Personal Information Management System*

[5] EU GDPR, *Article 3 - Territorial scope*

Acknowledgements

Members of the Trust and Privacy Sub Working Group

Mr Ong Yew Seng (Chairman)	Provintell Technologies Sdn Bhd
Ms Norkhadhra Nawawi (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Ridzwan Mahdi	Maxis Broadband Sdn Bhd
Mr Mohamad Isa Razhali	MEASAT Broadcast Network Systems Sdn Bhd
Ms Rafeah Omar/ Ms Ragini Thevi Subramanam/ Mr Thaib Mustafa	Telekom Malaysia Berhad

By invitation:

Ms Sabariah Ahmad	CyberSecurity Malaysia
Ms Leniza Nihar	Jabatan Perlindungan Data Peribadi