MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity
MALAYSIA

First edition
2020-05-05

Guidelines for Secure Internet of Things (IoT)

Reference number:
MyVAC-3-GUI-3-IOT-v1

REGISTERED OFFICE:

CyberSecurity Malaysia,
Level 7 Tower 1,
Menara Cyber Axis,
Jalan Impact,
63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia
Email: myvac@cybersecurity.my

NO ENDORSEMENT

Products and manufacturers discussed or referred to in this document, if any, are presented for informational purposes only and do not in any way constitute product approval or endorsement by CyberSecurity Malaysia.

TRADEMARKS

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalised. CyberSecurity Malaysia cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

DISCLAIMER

This document is for informational purposes only. It represents the current thinking of CyberSecurity Malaysia on the security aspects of the Internet of Things (IoT) environment. It does not establish any rights for any person and is not binding on CyberSecurity Malaysia or the public. The information appearing on this guideline is not intended to provide technical advice to any individual or entity. We urge you to consult with your own IoT advisor before taking any action based on information appearing on this guideline or any other documents to which it may be linked.

Contents Page

1 Introduction

The Internet of Things (IoT) can be defined as connecting everything to the internet be it a computerized device system, mechanical and digital machines, objects, animals or people. Now, IoT is recognized as one of the most important technological fields and has received enormous attention from various key-players.

The IoT will generally cultivate unlimited numbers of devices, people and services to connect and exchange useful information and data. Since the usage is widespread, some security and privacy issues will arise. Reliable, economical, efficient and effective security as well as privacy for IoT is required to ensure the proper confidentiality, integrity, authentication and access control among others.

However, CyberSecurity Malaysia (CSM) findings in 2014 reveal that IoT is not spared from cyber threats [1]. The wide exposures of data on the Internet actually pose security risks. Most IoT devices or systems may be exposed to information security threats and vulnerabilities if the IoT devices or systems are not properly secured [1]. These pose unprecedented data privacy and security challenges to develop secure IoT system [1].

This guideline provides a holistic and yet easily implemented security requirements which is translated into security controls to achieve a secure IoT system. It also provides security controls to assist three (3) group of key-players in IoT system including manufacturers, providers and consumers in understanding security of IoT system. Thus, key-players who intend to implement security control recommended in this guideline are moving towards in building a foundation for a reliable and secure IoT system.

1.1 Scope

In producing this document, researches and document reviews were conducted in CSM IoT Lab to study the security requirements of each component in IoT system. From the researches and projects, CSM gathers valuable data analysis prior to the development of this document.

This document provides guidance for the key-players to incorporate security features in the development of secure IoT system, based on CSM IoT Security Framework. Based on this framework, there are four (4) layers namely; Layer 1: Things, Layer 2: Communication, Layer 3: Application and Layer 4: Data Analytics. The details of this framework is discussed in section 4 of this document. This guideline is focusing on components in Layer 1. However, there are additional components which are applicable to each layer in the framework which are cloud, authentication, access control, data protection and privacy, and operation and maintenance. Therefore, security controls for these additional components are also included in this guideline to ensure that the security aspects of the whole IoT system are addressed accordingly. The selection of appropriate security controls can assist the key-players in minimizing the potential risks in IoT system.

This guideline uses the term IoT devices to indicate that security controls identified in this document are applicable to IoT devices only, while the term IoT system indicates that security controls are applicable to both IoT devices and IoT systems. Throughout this document, all security controls are carefully listed in the most elaborated way to help key-players understand each component effortlessly.

In complementing security controls identified in Layer 2, 3 and 4, there are guidelines that can be read together with this document which include CSM Guideline of Cloud Security Implementation for Cloud Service Subscriber, Guidelines for Secure Software Development Life Cycle (SSDLC) and Guidelines for Secure Industry 4.0.

1.2 Objective

The main objective of this document is to provide guidance in securing IoT system using secure by design approach based on CSM IoT Security Framework.

The specific objectives are:

a) To provide relevant security controls to secure IoT system.
b) To provide a checklist of security controls as a quick guide for the target audience in IoT system.

1.3 Intended audience

The intended audience of this document are the key-players in IoT system including consumers, developers, manufacturers, service providers, and vendors which are categorized into three (3) categories of key-players. Please refer to Section 3 for details.

2 Terms, definitions, abbreviated terms and acronyms

2.1 Terms and definitions

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

2.1.1
Access control
means to ensure that access to assets is authorized and restricted based on business and security requirements

[ISO/IEC 27000: 2014[1]]

2.1.2
Authentication
provision of assurance that a claimed characteristic of an entity is correct

[ISO/IEC 27000: 2014]

2.1.3
Availability
property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 27000: 2014]

2.1.4
Confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

[ISO/IEC 27000: 2014]

[1] ISO/IEC 27000:2014 — Information security management systems — Overview and vocabulary

2.1.5
Critical security parameter
security related information whose disclosure or modification can compromise the security of a cryptographic module

EXAMPLE Secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchors.

[ISO/IEC 19790:2012]

2.1.15
Denial of Service
threat aimed to deny access to valid users such as by making a web server temporarily unavailable or unusable

[OWASP Code Review Guide Version 1.1]

2.1.16
Elevation of privilege
if an application provides distinct user and administrative roles, then it is vital to ensure that the user cannot elevate his/her role to a higher privilege one

[OWASP Code Review Guide Version 2.0]

2.1.6
Internet of Things (IoT)
infrastructure of interconnected entities, people systems and information resources together with services which processes and reacts to information from the physical and virtual world

[ISO/IEC 20924]

2.1.7
Integrity
property of accuracy and completeness

[ISO/IEC 27000: 2014]

2.1.8
IoT device
entity of an IoT system that interacts and communicates with the physical world through sensing or actuating

Note 1 to entry: An IoT device can be a sensor or an actuator.
Note 2 to entry: An IoT device, in this context, is a finished end product which is the assembled end product which is usable for its intended functions without being embedded or integrated into any other product and is not a component.

[ISO/IEC 20924:2018]

2.1.9
IoT system

system providing functionalities of IoT
Note 1 to entry: IoT system is inclusive of IoT devices, IoT gateways, sensors, and actuator.

[ISO/IEC 20924:2018]

2.1.10
IoT trustworthiness

deserving trust or confidence within the entire lifecycle of an IoT implementation to ensure security, privacy, safety, reliability and resiliency

[ISO/IEC 20924:2018]

2.1.11
Objective

result to be achieved

[ISO/IEC 27000: 2014]

2.1.12
Risk

effect of uncertainty on objectives

[ISO/IEC 27000: 2014]

2.1.13
Process

set of interrelated or interacting activities which transforms inputs into outputs

[ISO/IEC 27000: 2014]

2.1.14
Repudiation

assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.

[NIST SP 800-32]

2.2 Abbreviated terms and acronyms

AP	Access Points
CC	Common Certified
CSA	Cloud Security Alliance
CSP	Cloud Service Provider

CSM	CyberSecurity Malaysia
ECG	Electrocardiography
e.g.	Exempli Gratia
ENISA	European Union Agency for Network and Information Security
GB	Gigabytes
Gbps	Gigabytes per second
GLBA	Gramm-Leach-Bliley Act
GSMA	Global System for Mobile Communications Association
HIPAA	Health Insurance Portability and Accountability Act
IC	Integrated Circuit
ICU	Intensive Care Unit
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
KB	Kilobytes
Kbps	Kilobytes per second
MB	Megabytes
Mbps	Megabytes per second
MCMC	Malaysian Communications and Multimedia Commission
MS	Mandatory Standards
NGN	Next Generation Network
PCI DSS	Payment Card Industry Data Security Standard
PIA	Privacy Impact Assessment
POLP	Principle of Least Privilege
QoS	Quality of Service
SIEM	Security Information and Event Management
TB	Terabytes
Tbps	Terabytes per second
UAT	User Acceptance Test
USB	Universal Serial Bus
WiFi	Wireless Fidelity
WPA2	WiFi Protected Access2

3 Key-players in IoT system

Table 1 discusses the description for each category of key player.

Table 1: Description for each category of key player

Category	Description	Example
Manufacturers	Manufacturers, including IoT system developers and programmers that design, develop produce and assemble IoT devices and IoT systems.	Proton, Pensonic, Libelium, etc.
Providers	Service providers, including vendors, distributors, system integrators that operate, configure,	Hospital, Smart City, Organization

	maintain, supply, provide and deploy IoT devices and IoT systems.	implementing and deploying IoT System, Vendors, etc.
Consumers	End users that use or interact with IoT devices and IoT systems.	End users, Patients, Smart City Citizen, etc.

This guideline assumes that the audience has minimal knowledge in the security of IoT system. The security controls identified in this document should be applicable to any IoT system, depending on circumstances and requirements that suit the needs of relevant audience. Table 2 shows the examples of how each security control should be used by each key player in securing their IoT system.

Table 2: Role of key-players in IoT system

IoT System	**Component**	**Security controls applied by key-players**		
		Manufacturers	**Providers**	**Consumers**
Smart City	CCTV System	1. Manufacturers should design the camera with unique identification (ID) label such as barcode, serial number or mac address, and provide ways to verify the authenticity of that label. 2. Manufacturers of CCTV monitoring application should not embed plaintext passwords in source code (hardcoded passwords) to prevent password guessing exploitation.	1. Providers should change default configuration settings upon receiving the CCTV system. 2. Providers should perform User Acceptance Test (UAT), monitored by service provider before CCTV system can be deployed on the premise.	1. Consumer should change default configuration settings upon receiving the CCTV system. 2. Consumer should configure strong and complex password of at least eight (8) characters in length with combination of alphanumeric characters on the CCTV system.

4 Internet of Things (IoT) Security Framework

An IoT system typically consists of complex infrastructures and the challenge to cybersecurity is to choose which area to be secured first that worth to be invested in. Any approaches taken in securing IoT environment should cover all aspects of IoT components for all layers. If the security approach is too complex, it will be difficult for organizations to implement it.

CyberSecurity Malaysia's IoT Security Framework serves as a general guidance to key-players to build a secure IoT system [2]. The framework comprises four (4) layers of IoT system as described in Figure 1, which requires security controls for every layer [2]. Layer 1 refers to IoT devices such as sensors, actuators and wearable devices. Meanwhile Layer 2 covers the technology used for data transfer between IoT devices which are protocol, gateway, wired and wireless network. Layer 3 covers systems functionalities to deliver on-demand services such as mobile application and storage. Finally, Layer 4 deals with data analysis and ways to ensure the integrity and accuracy of data that will be used for decision making. Thus, the framework provides holistic approach in order to secure the whole IoT system [2].

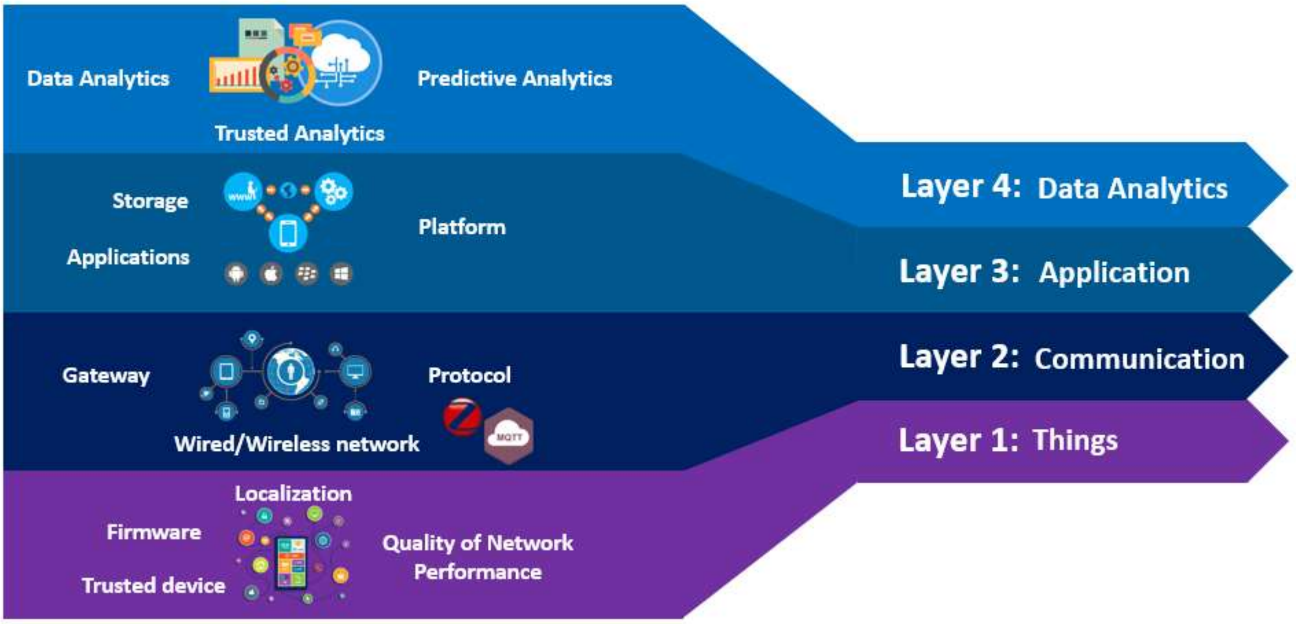

Figure 1: Internet of Things Security Framework

A typical IoT system consists of IoT Products and IoT Devices connected to the Cloud through a Gateway [2] as illustrated in Figure 2. IoT devices refer to all the products used in environments such as Smart Healthcare, Smart City or Smart Home [3]. Data gathered from IoT devices will be sent to the cloud through communication and network via a gateway (usually using a Router for Small Office Home Office (SOHO)) [4]. Nowadays, all system applications, web application, storage, and database can be configured in a cloud [5].

For example, an IoT medical device will collect data using sensors attached to the patients and then send it to the cloud via a WiFi network (wireless network) through a wireless router setup as a gateway. The data collected will be stored in the cloud as medical records. The data stored in the cloud will be used for further monitoring and data analytics purposes. Then, the authorized medical officers will access the cloud to retrieve the required data and information using a web application or mobile application for reference in making medical decisions [6].

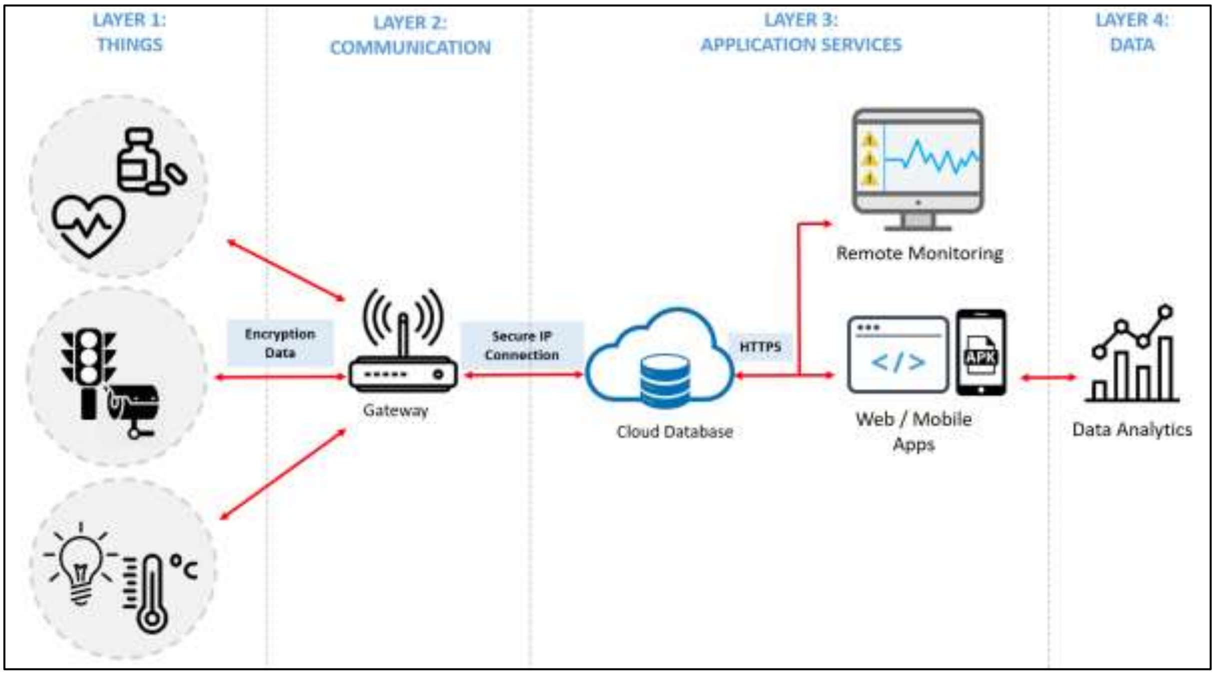

Figure 2: IoT system

The exponential growth in the adoption of IoT in every part of human life will climb steeply and will keep increasing [7]. Hence, CSM views that security aspects of the implementation of IoT must be addressed and for that purpose, CSM has taken a proactive approach and measures to produce this guideline in assisting key-players to secure the IoT system implementation [2]. The IoT Security Framework approaches the security of IoT system both horizontally and vertically. In order to achieve a secure IoT system, each layer that inter-connected must be secured vertically.

5 Existing IoT threats and vulnerabilities

Due to increasing devices connected to each other within IoT system, and data from various sources exchanged between things, the security of the system becomes a major concern. Sources of security threats and vulnerabilities from software, hardware, networks, infrastructures, or interface that are not managed accordingly can lead to compromised system. The followings are some of case studies related to IoT system:

5.1 Power plant hacking

Nearly half of Ivano-Frankisk, Ukraine experienced power outages for several hours, believed to be caused by malware targeting regional power plant systems on December 23, 2015 [19]. Three (3) energy operators were attacked, affecting approximately 225,000 residents in various areas. This attack was the first attack due to malware, causing power outages in a large scale.

A malware known as BlackEnergy 3 is embedded in Microsoft office documents and is manipulated to gain access to the network of electrical companies. One of the capabilities of this malware is that it can cause the infected system to not be restarted.

5.2 Moscow smart transportation weakness

Smart Transportation Moscow functions to manage traffic lights, closed roads, and traffic jam alert. Kaspersky Lab revealed several security issues involving the Moscow Smart Transportation causing the system to be at risk [20]. One of the weaknesses is that the manufacturer's name is clearly printed on the physical parts of the sensor. This weakness helped the Kaspersky Lab team to get technical information about the sensor. Furthermore, traffic sensors stationed around Moscow can be mapped as each sensor is accessible via Bluetooth connection.

If the hacker is able to obtain information such as the location of the sensor, the hacker may alter the sensor configuration and control traffic lights or other traffic equipment. Not only that, hackers can also alter data such as traffic statistic and determine whether the road should be shut down or direct traffic to other routes resulting in severe traffic congestion across the city.

5.3 Cyber attack on Banner Health company

United States health insurance company, Banner Health, warns their customers and healthcare providers that their personal information is likely to be stolen after an attack has been carried out by cyber attackers [21].

The attack targets patient information, staff information and healthcare plans. Through investigation, it was found that the attackers attempted to hack and access data regarding payment via cards to Banner Health. According to Banner Health, healthcare plan that is likely to be stolen during the attacks is made up of patient personal data, social security number, health officer name and patient claim information.

5.4 Attacks on medical and hardware sectors

The US Food and Drug Administration advised the hospital not to use the infusion system by Symbiq Hospira Inc as security vulnerabilities found on the system could allow cyber attackers to take over the system remotely [22]. These vulnerabilities could allow unauthorized users to control the device and change the dose provided by the pump to cause harm to critical patients. Additionally, a study on pacemakers found more than 8,000 weaknesses in the pacemaker's code. The study showed that only 17% of manufacturers have applied security in their medical devices. However, the report was released after more than 60 health organizations in the UK became victims of cyber-attacks.

5.5 Ransomware attacks against United Kingdom and California Hospitals

A large ransomware attack, known as WannaCry has affected 16 hospitals across the United Kingdom [23]. According to The Guardian, the attack began around 12:30 local time, whereby it freezes the system and confidential documents. When employees try to access a computer, they are threatened to pay around $300 in bitcoin currency.

Not only that, California hospital also was attacked by ransomware and infected other network systems [24]. The hacker has taken control of the hospital computer system and states that access will only be granted when a $ 17,000 redemption fee is paid in bitcoin currency. Based on these problems, all medical equipment manufacturer and service providers should take preliminary action by performing audits to test equipment vulnerabilities and update their response plans to protect organizations against cyber-attacks.

5.6 Distributed Denial-of-Service (DDoS) attacks to closed-circuit cameras

On September 19, 2018, a DDoS attack was launched on a web host company called OVH [25]. The attack involves thousands of cameras as well as digital video recording devices that connected to the Internet. Previously, OVH has experienced a 1 Tbps DDoS attack in 2016. Any IoT devices, including closed circuit television (CCTV) that are not properly configured, coupled with the use of a weak password, allow the attacker to easily detect the devices. This latest attack involved more than 6,800 cameras being part of a botnet, which later launched dozens of DDoS attacks against OVH. Each attack is estimated between 100 and 800 Gbps and took less than 2 days. In fact, 15,000 more devices were said to have been affected by the use of malware in the DDoS attack on the company's hosting company.

5.7 Mirai malware attack

In August 2016, a malware which targets IoT devices known as "Mirai" has spread. Some IoT devices targeted by Mirai were routers, security cameras, printers and digital video recorders (DVRs) as well as Linux servers. The method of the Mirai botnet attack method is to scan IoT devices that use hard-coded, default and easy-to-use passwords and passwords such as "admin", "123456" and "root". When information on targets has been obtained, Mirai botnet will send traffic to that target so it can cause DDoS situations to the devices [26].

5.8 Resource Data Management (RDM) security breach

On Israeli security researchers, Noam Rotem and Ran L from Safety Detective Research Lab discovered a security vulnerability in an IoT system manufactured by Resource Data Management (RDM), a Scotland-based remote monitoring solutions company. The IoT System (smart refrigerator) used by supermarkets and hospitals may allow an unauthorized access to take over the system and remotely control the system [27].

Report by Safety Detective showed that the affected systems use an unsecured HTTP protocol, mostly using port 9000, 8080, 8100, 80. Plus, they all come with a default username and "1234" as the default password, which is rarely changed by system administrators. The security breach also affected a few companies in Malaysia whereby crucial information such as site layout, the device list and temperature control settings are publicly exposed.

6 Security controls for IoT System

CSM has identified nine components to be addressed in order to secure IoT system which are Quality of Network Performance, Trusted Device, Localization, Firmware, Cloud, Authentication, Access Control, Data Protection and Privacy, Operation and Maintenance. Security controls for each component are listed in Table 3 below. A scenario for each sub-control is developed for the purposes of understanding on how to apply the security controls.

Table 3: Security controls for IoT system

SC 1	**Security Control 1: Quality of network performance** Objective: To ensure the quality of network performance in IoT system in terms of efficiency and real time data transmission.
Sub-control	**Description**
1-1	Manufacturers should design IoT devices that support data compression mechanism for minimizing network transmission rate. Scenario: *Manufacturers should implement compression algorithm in order to reduce size of data and to avoid bandwidth wastage.*

1-2	Manufacturers should design IoT devices that support Next Generation Network (NGN) that available, in order to provide efficient response time. _Scenario:_ *Manufacturers should design IoT devices to at least support the 5G network to ensure the quality of the response under 300 milliseconds (ms).*
1-3	Providers and Consumers should configure IoT devices to connect to the best possible network speed that available, in order to provide efficient response time. _Scenario:_ *Providers should configure their IoT devices to the 5G network if available, in order to ensure efficient response time.*
1-4	Manufacturers should design IoT devices to support the most secure protocol that available, so that data transmission process is encrypted. _Scenario:_ *Manufacturers should design the device to at least support WiFi Protected Access 2 (WPA2) protocol.*
1-5	Providers and Consumers should configure IoT devices to connect to the most secure security protocol that available, so that data transmission process is encrypted. _Scenario:_ *Providers should configure the wireless medical device to connect to wireless networks that use security protocol WiFi Protected Access 2 (WPA2) onwards.*
1-6	Providers should implement IoT devices in which the performance of network either cellular, wired or wireless, meet the metrics in the Mandatory Standards (MS) Quality of Service (QoS) set forth by the MCMC [12]. _Scenario:_ *Providers should ensure that network latency and packet loss rate for broadband access service are not more than 85ms and not exceed 1%, respectively [28].*
SC 2	**Security Control 2: Trusted device** Objective: To ensure the trustworthiness of the IoT devices.
Sub-control	**Description**
2-1	Manufacturers and Providers should conduct calibration testing on IoT devices whereby frequency of testing is determined by factors such as: a) how often IoT devices are used b) environmental conditions c) incident or accidental events d) required uncertainty in measurement. _Scenario:_ *Manufacturers and Providers should perform calibration testing to ensure the accuracy of IoT devices such as IoT medical devices.*

2-2	Manufacturers should design IoT devices with the ability to disable external, unused ports (if applicable) [15]. _Scenario:_ *Manufacturers should design an IoT medical devices such as health monitor with the ability of disabling Universal Serial Bus (USB) port to ensure IoT medical devices cannot be physically tampered.*
2-3	Providers should disable external, unused ports on IoT devices (if applicable) [15]. _Scenario:_ *Providers should configure an IoT medical device such as infusion pump with the ability of disabling Universal Serial Bus (USB) port to ensure the device cannot be physically tampered.*
2-4	Providers and Consumers should change IoT devices' default configuration settings upon receiving the devices. _Scenario:_ *Default configuration settings on smart door lock are predefined by the manufacturer in which, usually put usability before security. Thus, the Providers should ensure that the default configuration of the device has been changed during installation.*
2-5	Providers and Consumers should test and harden IoT devices' configuration setting to avoid any tampering by unauthorized users. _Scenario:_ *Providers should configure and revalidate the settings of IoT gateway during User Acceptance Testing (UAT) to ensure "Any to Any Rules" has been removed from the configuration of the device.*
2-6	Manufacturers should design IoT devices with unique identification (ID) label such as barcode, serial number or mac address, and provide ways to verify the authenticity of that label. _Scenario:_ *Manufacturers should design each IoT device with unique serial number (Authenticity Label/Sticker) in order for the Consumers to verify the authenticity of the IoT device.*
2-7	Providers and Consumers should ensure IoT devices have unique identification (ID) label such as barcode, serial number or mac address, and are provided with a link to verify the authenticity of that label. _Scenario:_ *Providers should ensure that IoT devices that they supply include unique serial number (Authenticity Label/Sticker) in order for Consumers to verify the authenticity of the IoT devices.*
2-8	Providers and Consumers should locate or place their IoT devices in a secure physical location to prevent unauthorized physical access to the devices. _Scenario:_ *Providers should configure their IoT system in a secured location and if possible, to protect it with biometric authentication and monitored by CCTV.*

2-9	Providers should document and monitor IoT devices' location frequently in order to avoid any installation of rogue devices. _Scenario:_ *A service provider should document all IoT devices in a proper inventory including the location of all IoT devices on the premise and frequently monitor of any installation of rogue devices.*
2-10	Manufacturers should implement Secure by Design approach in developing a secured and trusted IoT device [4]. _Scenario:_ *Manufacturers should design IoT devices according to Secure Software Development Life Cycle (SSDLC) framework that fits in the IoT system. The SSDLC framework include six (6) phases; Security Requirement, Secure Design, Secure Development, Security Testing, Security Deployment and Security Maintenance.*
SC 3	**Security Control 3: Localization** Objective: To ensure the accuracy of an IoT devices' location within IoT system.
Sub-control	**Description**
3-1	Manufacturers should design IoT devices that embeds Global Positioning System (GPS) features to ensure IoT devices' actual coordinate are accurate. _Scenario:_ *In designing a reliable smart transportation, manufacturers should design IoT devices with Global Positioning System (GPS) features such as geo-fence alert. With geo-fencing, users can set a virtual boundary such as encompassing the school and home, and get an alert if the smart transportation gone off the expected route.*
3-2	In the event IoT devices' location are confidential, Providers and Consumers should ensure that IoT devices' location are not publicly exposed [15]. _Scenario:_ *Providers should ensure the location of CCTV system (physically or virtual) are not publicly exposed during installation of the CCTV system, in order to protect Consumer's privacy.*
3-3	Providers and Consumers should ensure that IoT devices are not traceable by unauthorized parties [15]. _Scenario:_ *Providers should configure a smart refrigerator without publicly exposed information as discussed in Section 5.8. In the RDM Case study, as discussed in Section 5.8, the provider fails to change the default configuration, therefore exposing the smart refrigerator to be traceable and accessed remotely by unauthorized parties.*
SC 4	**Security Control 4: Firmware** Objective: To ensure IoT devices implement firmware-level security technologies to guarantee its trustworthiness and protection against tampering attacks.

Sub-control	**Description**
4-1	Manufacturers should design IoT devices with sufficient memory capacity and at least, adhere to the classes of constrained IoT device [10]. *Scenario:* *Manufacturers of Integrated Circuit (IC) should design a serial Flash with high data transfer rate, but low power consumption, which is ideal for IoT system.*
4-2	Manufacturers and Providers should establish a secure firmware update process for IoT devices. *Scenario:* *Manufacturers should provide a secure firmware update process and procedure for the CCTV camera. Meanwhile, Providers should follow the procedure provided by the manufacturer for updating the firmware. Providers should ensure that configuration and data backup was conducted before updating the firmware.*
4-3	Manufacturers should design IoT devices' firmware with security features in order to validate the authenticity of firmware update. *Scenario:* *Manufacturers should implement digital signatures in each update file before releasing it for public usage.*
4-4	Manufacturers should release update for IoT devices to address security issues when they occur, to address bugs discovered in the software or to add support for new models of IoT devices. *Scenario:* *Manufacturers should release an update when there are security issues that occur or minor bug issues in the software. The manufacturer should notify users regarding the update released.*
4-5	Providers and Consumers should install IoT devices with the latest and verified version of firmware. *Scenario:* *Providers should ensure that the firmware installed on the IoT device is the latest and verified version released by the manufacturer.*
SC 5	**Security Control 5: Cloud** Objective: To ensure secure cloud implementation in IoT system.
Sub-control	**Description**
5-1	Manufacturers and Providers should provide options for Consumers to control data synchronization to cloud [11]. *Scenario:* *Manufacturers and Providers for cloud services should provide the ability of controlling data synchronization for Consumers. This will ensure Consumers have the ability to control which data that belong to the consumer to be uploaded and stored in the cloud.*

5-2	Manufacturers and Providers should ensure that the cloud infrastructure can be isolated based on Consumers' request [11]. *Scenario:* *Providers should be able to offer isolation of cloud infrastructure, between virtual machines in the hypervisor, if requested by consumers.*
5-3	Manufacturers and Providers should ensure that cloud services that they use for IoT deployment should be updated in order to fix bugs and security issues and at the same time, to improve performance of cloud services [11]. *Scenario:* *Providers should be responsible for fixing bugs and security loopholes found in cloud services. Providers should mitigate the vulnerabilities and update the services with the latest version of software for security purpose.*
5-4	In the event where Consumers have access to cloud configuration, Consumers should ensure cloud services are updated with the latest version [11]. *Scenario:* *Consumers should regularly check the cloud service they used to ensure it is the latest version released by the Providers.*
5-5	Manufacturers and Providers should encrypt backups using the best, strong encryption mechanism that available [11]. *Scenario:* *Providers should encrypt their backup to ensure consumers' privacy intact.*
5-6	Providers should encrypt sensitive data using the best, strong encryption that available before send the data to cloud [11]. *Scenario:* *Providers should encrypt Consumers' sensitive data using the best possible encryption mechanism before uploading it to the cloud.*
5-7	Manufacturers and Providers should ensure that any backup is tested for restoration [11]. *Scenario:* *Providers that implement cloud-based operation should regularly perform restoration testing to ensure the backup useable.*
5-8	Manufacturers and Providers should ensure that any backup data must be sanitized or deleted according to data retention policy or data retention laws for regulated industries [11]. *Scenario:* *Providers in healthcare industry that use cloud to stored medical records, are subject to data retention period up to 6 years in accordance to laws and regulation.*
5-9	Manufacturers and Providers should provide 24/7 monitoring on cloud services and give prompt response to Consumers in the event of any anomaly activity [11]. *Scenario:*

	Providers should provide 24/7 monitoring services to detect any security breaches and security threats and responsible to notify cloud users and assist them for recovery action as when required.
SC 6	**Secure Control 6: Authentication** Objective: To ensure secure authentication mechanism is implemented on IoT system.
Sub-control	**Description**
6-1	Providers and Consumers should ensure that IoT devices are correctly configured by implementing a strong password mechanism with the following criteria [15]: a) alphanumeric characters; b) at least eight (8) characters; c) at least one (1) uppercase character; d) at least one (1) lowercase character; e) at least one (1) number; and f) special characters *Scenario:* *Providers should configure a password consists of at least eight (8) characters in length with combination of criteria determined above.*
6-2	Manufacturers should implement a multi-factor authentication mechanism in IoT device such as [15]: a) username b) email c) secure passphrase d) one-time token e) SMS token f) biometric verification g) push notification h) security challenge *Scenario:* *Manufacturers should design IoT devices that support a multifactor authentication mechanism in order to provide consumers with a reliable authentication mechanism.*
6-3	Providers and Consumers should configure a multifactor authentication mechanism in IoT system such as [15]: a) username b) email c) secure passphrase d) one-time token e) SMS token f) biometric verification g) push notification h) security challenge *Scenario:*

	Providers should configure multifactor authentication mechanism in order to verify authorized users.
6-4	Manufacturers should design IoT devices that support verification mechanism before establishing connection of devices. *Scenario:* *Manufacturers should design IoT devices such as smart door lock, smart plug, and smart lamp with PIN verification to establish secure connection between these devices.*
6-5	Manufacturers should not embed plaintext passwords in source code (hardcoded passwords) in IoT system to prevent password guessing exploitation. *Scenario:* *Manufacturers of IoT system should not embed plaintext password in source code as discussed in a case study in Section 5.7.*
6-6	Providers and Consumers should ensure that no default credentials are used in IoT system. *Scenario:* *Consumers of smart plug should change the default credential provided by the manufacturer in order to prevent unauthorized users gain access to the smart plug configuration setting.*
6-7	Manufacturers should ensure that passwords of IoT system are not displayed in plaintext and should be hidden with any special character [16]. *Scenario:* *Manufacturers should design the IoT system in a way that if a password was inserted by a user, the password are hidden and represented by asterisk characters on the screen to avoid social engineering threats.*
6-8	Manufacturers should design account lock mechanism in IoT system to prevent brute-force password attack [17]. *Scenario:* *Manufacturers should design account lock mechanism in every home appliance to protect the smart home system from brute force attack by unauthorized parties.*
6-9	Providers should configure account lock mechanism in IoT system whereby the account lock threshold is set to a sufficient value [17]. *Scenario:* *Providers should configure account lock mechanism in the IoT device in a way that it will be locked or provides warning after 5 unsuccessful login attempts. The IoT device can only be unlocked after a predetermined period self-service unlock mechanism, or intervention by an administrator.*
6-10	Manufacturers should design IoT system with password recovery mechanism such as: a) password reset information should be sent to other possible email address or an SMS text number; and b) security questions which can only be answered by Consumers

	Scenario: *Manufacturers should design password recovery mechanism in IoT system. So that in the event of any incident on the system, consumers able to request password recovery via SMS text number or registered email.*
6-11	Providers should configure IoT system with password recovery mechanism such as: a) password reset information should be sent to other possible email address or an SMS text number; and b) security questions which can only be answered by Consumers *Scenario:* *Providers should configure password recovery mechanism in IoT system. So that in the event of any incident on the system, consumers able to request password recovery via SMS text number or registered email.*
6-12	Providers should enforce password expiration policy in IoT system, whereby the maximum password expiration period is vary based on usage and security importance. *Scenario:* *Providers that implement IoT system should configure password expiration policy. For example, passwords for CCTV system should be changed at least twice a year and reuse of previous password is not allowed.*
6-13	Consumers should comply password security best practice and apply it in IoT system. *Scenario:* *Consumers of IoT system should comply to password security best practices. For example, passwords should not be publicly displayed and should always be kept in secure places.*
SC 7	**Security Control 7: Access control** Objective: To ensure access right and authorization is clearly defined and implemented in IoT system.
Sub-control	**Description**
7-1	Providers should create individual account in IoT system, either for human or machine, instead of group-based or role-based account. *Scenario:* *Providers should configure an individual account with relevant access and function, instead of creating group accounts so that no consumers share the same access capability. For example, user A has an administrator access capability whereby user B has a super administrator access capability.*
7-2	Providers should configure user privilege in IoT system to allow access in order to perform required tasks only. *Scenario:*

	Providers should configure limited functions allowed for a given IoT system by implementing Principle of Least Privilege (POLP) to reduce risk in the event of privilege escalation attack.
7-3	Providers should perform periodic access review whenever there is change in Consumers' status. *Scenario:* *Providers should review consumers access based on frequency defined in the ICT Security Policy or after any change in consumers' status, whether the affected consumer still obtain the account or has terminated their account.*
SC 8	**Security Control 8: Data protection and privacy** Objective: To ensure data and privacy in IoT system is protected against data breach.
Sub-control	**Description**
8-1	Providers should classify data in IoT system according to its impact on Confidentiality, Integrity, Availability (CIA) triad and the data should be managed and protected based on data classification level [6]. *Scenario:* *Provider of IoT medical device should configure security mechanisms to protect medical data in order to ensure its confidentiality and integrity are intact without compromising its availability as when required. Whereby provider of Weather System should configure security mechanisms to protect data integrity without compromising its availability as when required.*
8-2	Manufacturers and Providers should ensure that IoT system provide Consumers the ability to agree or reject data collection and disclosure of personal data in order to control their privacy preferences. *Scenario:* *A health tracker application should obtain permission to store and process personal data such as name, weight, health status of consumers' wearable device, before the application can be installed on the device.*
8-3	Manufacturers should design IoT system to allow Consumers to change their privacy preferences in configuration settings. *Scenario:* *Manufacturers should include a privacy option in the configuration setting so that users able to manage the type of data that the wearable device can collect or share across the IoT system.*
8-4	Providers should ensure IoT system that collect, process and store personal data adhere to relevant laws. *Scenario:* *Providers of IoT system in Malaysia should adhere to ACT 709*[2]*, Personal Data Protection Act.*

[2] LAWS OF MALAYSIA Act 709 Personal Data Protection Act 2010

8-5	Providers should limit IoT system to collect, process and store data that adequate to perform its functions only. *Scenario:* *Providers of Driving Direction Applications, should only provide navigation instruction and driving direction and not obtaining consumer data collection for consumer profiling in order to have financial gain such as advertising.*
8-6	Providers should dispose any personal and sensitive data properly based on data retention policy and should adhere to data retention laws for regulated industries. *Scenario:* *Data retention policy should consider value of data over time. Some examples of data retention periods are purchase orders for three (3) years, safety records for seven (7) years and patents are retained permanently.* *In regulated industry, an organization that deals with credit card or e-commerce may subject to the Payment Card Industry Data Security Standard (PCI DSS) data retention and disposal policy.*
8-7	In the event IoT devices that stored personal and sensitive data need to be disposed, Providers should implement secure data destruction methodologies before physically destroy the IoT devices, according to industry best practices. *Scenario:* *If an ultrasound monitor has reach expiration date and need to be disposed, the responsible department should securely clean up any personal and sensitive data before physically destroy the hard drive.* *For reference, NIST SP 800-88*[3] *provides guidance for media sanitization and US-CERT*[4] *provides guideline on disposing electronic devices safely.*
SC 9	**Security Control 9: Operation and maintenance** Objective: To ensure availability of data and secure provisioning process in IoT system.
Sub-control	**Description**
9-1	Manufacturers should provide documentation for IoT system such as user manual, product datasheet or IoT devices certification (if any) as a reference for Providers and Consumers. *Scenario:* *Manufactures should provide user manual, product datasheet or product certification (if any) so that it can be a reference (recommended in English language for easy reference) for consumers during installation or troubleshooting.*
9-2	Providers and Consumers should ensure that any provision for IoT system includes documentation such as user manual, product datasheet or IoT devices certification (if any) which can be used as reference. *Scenario:*

[3] NIST Special Publication SP 800-88 Rev. 1 Guidelines for Media Sanitization

[4] United States Computer Emergency Readiness Team (US-CERT): Disposing of Devices Safely

	An organization that plans to deploy smart office system should include documentation and product certification (if any) in the requirement during procurement process. *Consumers should ensure that the documentation such as user manual is included in the box when buying any products.*
9-3	Providers and Consumers should ensure that any provision of IoT system covers maintenance service and technical support (warranty) for both hardware and software in which, the scope should also cover the damage and dysfunctionality due to cyber threats. *Scenario:* *Providers and Consumers should ensure warranty service covers maintenance and technical support for both hardware and software during procurement process. The requirement should also state that any damage due to cyber threats is covered in the warranty service.*
9-4	Providers and Consumers should ensure that any provision of IoT system covers the maintenance service and technical support (warranty) in accordance with the lifespan of IoT system. *Scenario:* *Providers and Consumers should ensure the lifespan of the system, for both hardware and software, is stated in technical specification during provisioning process, and the warranty should cover in accordance with the lifespan of the system.*
9-5	Providers should maintain updated inventories for IoT system that cover both hardware and software. *Scenario:* *Providers should create and maintain inventory for the IoT system in a Smart City. The inventory may include information such as version, type of CCTV camera, serial number, IP address or traffic lights' location.*
9-6	Providers and Consumers should ensure that they have the rights to control the credentials (username and password) used to access IoT system. *Scenario:* *Providers such as Hospital IT administrator should change the default credential used to access IoT medical devices once the system has been installed on the premise. The Hospital IT administrator should have the right to manage and control the credential rather than being managed by vendor.*
9-7	Providers should ensure that any installation of IoT devices in IoT system is verified and tested by a competent person [13]. *Scenario:* *Providers should ensure User Acceptance Test (UAT) is executed by vendor during the installation of any product on their premise.*
9-8	Providers should develop and implement preventive, remedial and maintenance plans for their IoT system to ensure operational continuity without unnecessary downtime. *Scenario:*

	Provider should implement preventive, remedial and maintenance plans so that their Consumers are protected from any incident, failure, or downtime.
9-9	Providers should carry out security and vulnerability assessments on a schedule basis and as and when required for their IoT system. *Scenario:* *Providers such as Hospital that deploys IoT medical devices and system should carry out security and vulnerability assessment to identify any potential or existing vulnerability in the system.*
9-10	In the event of IoT system components (eg. OS, IoT device) are about to obsolete, Manufacturers should publish an end-of-life policy that explicitly states the minimum length of time for which the IoT system will receive updates and the reasons for the length of the support period. *Scenario:* *If the support for current software version is about to expire, the Manufacturer should publish the information on official website and provide ways for the consumers and providers to get the latest, stable version for the software.*
9-11	Manufacturers and Providers should implement IoT system with forensic readiness mechanism in order to assist any forensic procedure when required [6]. *Scenario:* *Providers that deploys IoT system should be equipped with forensic readiness mechanism. The provider should correctly configure system logs in order to record relevant events and should be ready as when it is required for forensic purposes.*
9-12	Manufacturers should obtain relevant security certification eg: Common Criteria or at least go for product security testing. *Scenario:* *Manufacturers should obtain Common Criteria security certification based on ISO/IEC 15408 or send their devices for security testing to trusted security testing laboratories.*

Annex A

Existing security standards and guidelines

Table A. 1: Existing security standards and guidelines referred to throughout the development of this guideline

No	Document	Publisher	Source
1	NIST Platform Firmware Resiliency Guidelines	National Institute of Standards and Technology (NIST)	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf
2	IOT Security Guidance	Open Web Application Security Project (OWASP)	https://www.owasp.org/index.php/IoT_Security_Guidance
3	IOT Security Best Practice	Institute of Electrical and Electronics Engineers (IEEE)	https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf
4	Payment Card Industry Data Security Standard	Security Standard Council	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1551857656882
5	NIST 800-88: Guideline for Media Sanitization	National Institute of Standards and Technology (NIST)	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-88.pdf
6	Best Current Practices (BCP) for IoT Devices	Internet Engineering Task Force (IETF)	https://tools.ietf.org/html/draft-moore-iot-security-bcp-00#section-2.6.2
7	IoT Security Guideline Overview Document	Global System for Mobile Communications Association (GSMA)	https://www.gsma.com/iot/wp-content/uploads/2018/08/CLP.-11-v2.0.pdf
8	Internet of Things Guidelines for Sustainability	World Economic Forum	http://www3.weforum.org/docs/IoTGuidelinesforSustainability.pdf
9	Future-proofing the Connected World: 13 Steps to Developing Secure IoT	Cyber Security Alliance (CSA)	https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf
10	Baseline Security Recommendations for IoT	European Union Agency for Cybersecurity (ENISA)	https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
11	Technical Code Internet of Things (IoT) – Security Management	Malaysian Communications and Multimedia Commission (MCMC)	https://www.skmm.gov.my/skmmgovmy/media/General/pdf/MCMC-MTSFB-TC-G013_2018_IoT_SECURITY-MANAGEMENT.pdf

12	Wireless Security Guideline for Wireless Local Area Network (WLAN)	CyberSecurity Malaysia	https://www.cybersecurity.my/en/knowledge_bank/info_guiding/best_practices/main/detail/639/index.html
13	Guidelines for Secure Industrial Control System (ICS)	CyberSecurity Malaysia	https://www.cybersecurity.my/en/knowledge_banks/principles_guidelines/main/detail/2339/index.html
14	Guideline of Cloud Security Implementation for Cloud Service Subscriber	CyberSecurity Malaysia	https://www.cybersecurity.my/en/knowledge_banks/principles_guidelines/main/detail/2339/index.html
15	Guidelines on the Usage of AKSA MySEAL Approved Cryptographic Algorithms	CyberSecurity Malaysia	https://www.cybersecurity.my/en/knowledge_banks/principles_guidelines/main/detail/2339/index.html
16	Guidelines for Secure Software Development Lifecycle (SSDLC)	CyberSecurity Malaysia	https://www.cybersecurity.my/en/knowledge_banks/principles_guidelines/main/detail/2339/index.html

Annex B

IoT Cyber Security Checklist

Security controls listed on the IoT Cyber Security Checklist are derived from this guideline. This checklist can be used by key-players as a guidance during development, installation, or implementation of IoT system.

Table B. 1: IoT cyber security checklist

Security Control (SC)				
SC 1	**Quality of network performance**	**Yes**	**No**	**Remark**
1-1	Manufacturers should design IoT devices that support data compression mechanism for minimizing network transmission rate.			
1-2	Manufacturers should design IoT devices that support Next Generation Network (NGN) that available, in order to provide efficient response time.			
1-3	Providers and Consumers should configure IoT devices to connect to the best possible network speed that available, in order to provide efficient response time.			
1-4	Manufacturers should design IoT devices to support the most secure protocol that available, so that data transmission process is encrypted.			
1-5	Providers and Consumers should configure IoT devices to connect to the most secure security protocol that available, so that data transmission process is encrypted.			
1-6	Providers should implement IoT devices in which the performance of network either cellular, wired or wireless, meet the metrics in the Mandatory Standards (MS) Quality of Service (QoS) set forth by the MCMC.			
SC 2	**Trusted device**	**Yes**	**No**	**Remark**
2-1	Manufacturers and Providers should conduct calibration testing on IoT devices whereby frequency of testing is determined by factors such as: (a) how often IoT devices are used (b) environmental conditions (c) incident or accidental events (d) required uncertainty in measurement			

2-2	Manufacturers should design IoT devices with the ability to disable external, unused ports (if applicable).			
2-3	Providers should disable external, unused ports on IoT devices (if applicable).			
2-4	Providers and Consumers should change IoT devices' default configuration settings upon receiving the devices.			
2-5	Providers and Consumers should test and harden IoT devices' configuration setting to avoid any tampering by unauthorized users.			
2-6	Manufacturers should design IoT devices with unique identification (ID) label such as barcode, serial number or mac address, and provide ways to verify the authenticity of that label.			
2-7	Providers and Consumers should ensure IoT devices have unique identification (ID) label such as barcode, serial number or mac address, and are provided with a link to verify the authenticity of that label.			
2-8	Providers and Consumers should locate or place their IoT devices in a secure physical location to prevent unauthorized physical access to the devices.			
2-9	Providers should document and monitor IoT devices' location frequently in order to avoid any installation of rogue devices.			
2-10	Manufacturers should implement Secure by Design approach in developing a secured and trusted IoT device.			
SC 3	**Localization**	**Yes**	**No**	**Remark**
3-1	Manufacturers should design IoT devices that embeds Global Positioning System (GPS) features to ensure IoT devices' actual coordinate are accurate.			
3-2	In the event IoT devices' location are confidential, Providers and Consumers should ensure that IoT devices' location are not publicly exposed.			
3-3	Providers and Consumers should ensure that IoT devices are not traceable by unauthorized parties.			
SC 4	**Firmware**	**Yes**	**No**	**Remark**
4-1	Manufacturers should design IoT devices with sufficient memory capacity and at least, adhere to the classes of constrained IoT device.			

4-2	Manufacturers and Providers should establish a secure firmware update process for IoT devices.			
4-3	Manufacturers should design IoT devices' firmware with security features in order to validate the authenticity of firmware update.			
4-4	Manufacturers should release update for IoT devices to address security issues when they occur, to address bugs discovered in the software or to add support for new models of IoT devices.			
4-5	Providers and Consumers should install IoT devices with the latest and verified version of firmware.			
SC 5	**Cloud**	**Yes**	**No**	**Remark**
5-1	Manufacturers and Providers should provide options for Consumers to control data synchronization to cloud.			
5-2	Manufacturers and Providers should ensure that the cloud infrastructure can be isolated based on Consumers' request.			
5-3	Manufacturers and Providers should ensure that cloud services that they use for IoT deployment should be updated in order to fix bugs and security issues and at the same time, to improve performance of cloud services.			
5-4	In the event where Consumers have access to cloud configuration, Consumers should ensure cloud services are updated with the latest version.			
5-5	Manufacturers and Providers should encrypt backups using the best, strong encryption mechanism that available.			
5-6	Providers should encrypt sensitive data using the best, strong encryption that available before send the data to cloud.			
5-7	Manufacturers and Providers should ensure that any backup is tested for restoration.			
5-8	Manufacturers and Providers should ensure that any backup data must be sanitized or deleted according to data retention policy or data retention laws for regulated industries.			
5-9	Manufacturers and Providers should provide 24/7 monitoring on cloud services and give prompt response to Consumers in the event of any anomaly activity.			

SC 6	Authentication	Yes	No	Remark

6-1	Providers and Consumers should ensure that IoT devices are correctly configured by implementing a strong password mechanism with the following criteria :
	a) alphanumeric characters;
	b) at least eight (8) characters;
	c) at least one (1) uppercase character;
	d) at least one (1) lowercase character;
	e) at least one (1) number; and
	f) special characters			

6-2	Manufacturers should implement a multifactor authentication mechanism in IoT system such as: a) username b) email c) secure passphrase d) one-time token e) SMS token f) biometric verification g) push notification h) security challenge			
6-3	Providers and Consumers should configure a multi-factor authentication mechanism in IoT system such as: a) username b) email c) secure passphrase d) one-time token e) SMS token f) biometric verification g) push notification h) security challenge			
6-4	Manufacturers should design IoT devices that support verification mechanism before establishing connection of devices.			
6-5	Manufacturers should not embed plaintext passwords in source code (hardcoded passwords) in IoT system to prevent password guessing exploitation.			
6-6	Providers and Consumers should ensure that no default credentials are used in IoT system.			
6-7	Manufacturers should ensure that passwords of IoT system are not displayed in plaintext and should be hidden with any special character.			

6-8	Manufacturers should design account lock mechanism in IoT system to prevent brute-force password attack.			
6-9	Providers should configure account lock mechanism in IoT system whereby the account lock threshold is set to a sufficient value.			
6-10	Manufacturers should design IoT system with password recovery mechanism such as: a) password reset information should be sent to other possible email address or an SMS text number; and b) security questions which can only be answered by Consumers			
6-11	Providers should configure IoT system with password recovery mechanism such as: a) password reset information should be sent to other possible email address or an SMS text number; and b) security questions which can only be answered by Consumers			
6-12	Providers should enforce password expiration policy in IoT system, whereby the maximum password expiration period is vary based on usage and security importance.			
6-13	Consumers should comply password security best practice and apply it in IoT system.			
SC 7	**Access control**	**Yes**	**No**	**Remark**
7-1	Providers should create individual account in IoT system, either for human or machine, instead of group-based or role-based account.			
7-2	Providers should configure user privilege in IoT system to allow access in order to perform required tasks only.			
7-3	Providers should perform periodic access review whenever there is change in Consumers' status.			
SC 8	**Data protection and privacy**	**Yes**	**No**	**Remark**
8-1	Providers should classify data in IoT system according to its impact on Confidentiality, Integrity, Availability (CIA) triad and the data should be managed and protected based on data classification level.			

8-2	Manufacturers and Providers should ensure that IoT system provide Consumers the ability to agree or reject data collection and disclosure of personal data in order to control their privacy preferences.			
8-3	Manufacturers should design IoT system to allow Consumers to change their privacy preferences in configuration settings.			
8-4	Providers should ensure IoT system that collect, process and store personal data adhere to relevant laws.			
8-5	Providers should limit IoT system to collect, process and store data that adequate to perform its functions only.			
8-6	Providers should dispose any personal and sensitive data properly based on data retention policy and should adhere to data retention laws for regulated industries.			
8-7	In the event IoT devices that stored personal and sensitive data need to be disposed, Providers should implement secure data destruction methodologies before physically destroy the IoT devices, according to industry best practices.			
SC 9	**Operation and maintenance**	**Yes**	**No**	**Remark**
9-1	Manufacturers should provide documentation for IoT system such as user manual, product datasheet or IoT devices certification (if any) as a reference for Providers and Consumers.			
9-2	Providers and Consumers should ensure that any provision for IoT system includes documentation such as user manual, product datasheet or IoT devices certification (if any) which can be used as reference.			
9-3	Providers and Consumers should ensure that any provision of IoT system covers maintenance service and technical support (warranty) for both hardware and software in which, the scope should also cover the damage and dysfunctionality due to cyber threats.			
9-4	Providers and Consumers should ensure that any provision of IoT system covers the maintenance service and technical support (warranty) in accordance with the lifespan of IoT system.			
9-5	Providers should maintain updated inventories for IoT system that cover both hardware and software.			

9-6	Providers and Consumers should ensure that they have the rights to control the credentials (username and password) used to access IoT system.			
9-7	Providers should ensure that any installation of IoT system is verified and tested by a competent person.			
9-8	Providers should develop and implement preventive, remedial and maintenance plans for their IoT system to ensure operational continuity without unnecessary downtime.			
9-9	Providers should carry out security and vulnerability assessments on a schedule basis and as and when required for their IoT system.			
9-10	In the event of IoT system components (eg. OS, IoT device) are about to obsolete, Manufacturers should publish an end-of-life policy that explicitly states the minimum length of time for which the IoT system will receive updates and the reasons for the length of the support period.			
9-11	Manufacturers and Providers should implement IoT system with forensic readiness mechanism in order to assist any forensic procedure when required.			
9-12	Manufacturers should obtain relevant security certification eg: Common Criteria or at least go for product security testing.			

Annex C

Summary of Guideline for Secure Internet of Things

The security controls and affected key-players listed in Table C.1 are directly derived from this guideline and has been simplified for ease of use.

Table C. 1: Security controls and affected key-players for IoT system

Security Control (SC)		Key-players		
SC 1	**Quality of network performance**	**Manufacturers**	**Providers**	**Consumers**
1-1	Manufacturers should design IoT devices that support data compression mechanism for minimizing network transmission rate.	/		
1-2	Manufacturers should design IoT devices that support Next Generation Network (NGN) that available, in order to provide efficient response time.	/		
1-3	Providers and Consumers should configure IoT devices to connect to the best possible network speed that available, in order to provide efficient response time.		/	/
1-4	Manufacturers should design IoT devices to support the most secure protocol that available, so that data transmission process is encrypted.	/		
1-5	Providers and Consumers should configure IoT devices to connect to the most secure security protocol that available, so that data transmission process is encrypted.		/	/
1-6	Providers should implement IoT devices in which the performance of network either cellular, wired or wireless, meet the metrics in the Mandatory Standards (MS) Quality of Service (QoS) set forth by the MCMC.		/	
SC 2	**Trusted device**	**Manufacturers**	**Providers**	**Consumers**
2-1	Manufacturers and Providers should conduct calibration testing on IoT devices whereby frequency of testing is determined by factors such as: a) how often IoT devices are used	/	/	

	b) environmental conditions c) incident or accidental events d) required uncertainty in measurement			
2-2	Manufacturers should design IoT devices with the ability to disable external, unused ports (if applicable).	/		
2-3	Providers should disable external, unused ports on IoT devices (if applicable).		/	
2-4	Providers and Consumers should change IoT devices' default configuration settings upon receiving the devices.		/	/
2-5	Providers and Consumers should test and harden IoT devices' configuration setting to avoid any tampering by unauthorized users.		/	/
2-6	Manufacturers should design IoT devices with unique identification (ID) label such as barcode, serial number or mac address, and provide ways to verify the authenticity of that label.	/		
2-7	Providers and Consumers should ensure IoT devices have unique identification (ID) label such as barcode, serial number or mac address, and are provided with a link to verify the authenticity of that label.		/	/
2-8	Providers and Consumers should locate or place their IoT devices in a secure physical location to prevent unauthorized physical access to the devices.		/	/
2-9	Providers should document and monitor IoT devices' location frequently in order to avoid any installation of rogue devices.		/	
2-10	Manufacturers should implement Secure by Design approach in developing a secured and trusted IoT device.	/		
SC 3	**Localization**	**Manufacturers**	**Providers**	**Consumers**
3-1	Manufacturers should design IoT devices that embeds Global Positioning System (GPS) features to ensure IoT devices' actual coordinate are accurate	/		

3-2	In the event IoT devices' location are confidential, Providers and Consumers should ensure that IoT devices' location are not publicly exposed.		/	/
3-3	Providers and Consumers should ensure that IoT devices are not traceable by unauthorized parties.		/	/
SC 4	**Firmware**	**Manufacturers**	**Providers**	**Consumers**
4-1	Manufacturers should design IoT devices with sufficient memory capacity and at least, adhere to the classes of constrained IoT device.	/		
4-2	Manufacturers and Providers should establish a secure firmware update process for IoT devices.	/	/	
4-3	Manufacturers should design IoT devices' firmware with security features in order to validate the authenticity of firmware update.	/		
4-4	Manufacturers should release update for IoT devices to address security issues when they occur, to address bugs discovered in the software or to add support for new models of IoT devices.	/		
4-5	Providers and Consumers should install IoT devices with the latest and verified version of firmware.		/	/
SC 5	**Cloud**	**Manufacturers**	**Providers**	**Consumers**
5-1	Manufacturers and Providers should provide options for Consumers to control data synchronization to cloud.	/	/	
5-2	Manufacturers and Providers should ensure that the cloud infrastructure can be isolated based on Consumers' request.	/	/	
5-3	Manufacturers and Providers should ensure that cloud services that they use for IoT deployment should be updated in order to fix bugs and security issues and at the same time, to improve performance of cloud services.	/	/	
5-4	In the event where Consumers have access to cloud configuration,			/

	Consumers should ensure cloud services are updated with the latest version.			
5-5	Manufacturers and Providers should encrypt backups using the best, strong encryption mechanism that available.	/	/	
5-6	Providers should encrypt sensitive data using the best, strong encryption that available before send the data to cloud.		/	
5-7	Manufacturers and Providers should ensure that any backup is tested for restoration.	/	/	
5-8	Manufacturers and Providers should ensure that any backup data must be sanitized or deleted according to data retention policy or data retention laws for regulated industries.	/	/	
5-9	Manufacturers and Providers should provide 24/7 monitoring on cloud services and give prompt response to Consumers in the event of any anomaly activity.	/	/	
SC 6	**Authentication**	**Manufacturers**	**Providers**	**Consumers**

6-1	Providers and Consumers should ensure that IoT devices are correctly configured by implementing a strong password mechanism with the following criteria :
	a) alphanumeric characters;
	b) at least eight (8) characters;
	c) at least one (1) uppercase character;
	d) at least one (1) lowercase character;
	e) at least one (1) number; and special characters
			/	/

6-2	Manufacturers should implement a multifactor authentication mechanism in IoT system such as: a) username b) email c) secure passphrase d) one-time token e) SMS token f) biometric verification g) push notification h) security challenge	/		

6-3	Providers and Consumers should configure a multi-factor authentication mechanism in IoT system such as: a) username b) email c) secure passphrase d) one-time token e) SMS token f) biometric verification g) push notification h) security challenge		/	/
6-4	Manufacturers should design IoT devices that support verification mechanism before establishing connection of devices.	/		
6-5	Manufacturers should not embed plaintext passwords in source code (hardcoded passwords) in IoT system to prevent password guessing exploitation.	/		
6-6	Providers and Consumers should ensure that no default credentials are used in IoT system.		/	/
6-7	Manufacturers should ensure that passwords of IoT system are not displayed in plaintext and should be hidden with any special character.	/		
6-8	Manufacturers should design account lock mechanism in IoT system to prevent brute-force password attack.	/		
6-9	Providers should configure account lock mechanism in IoT system whereby the account lock threshold is set to a sufficient value.		/	
6-10	Manufacturers should design IoT system with password recovery mechanism such as: a) password reset information should be sent to other possible email address or an SMS text number; and b) security questions which can only be answered by Consumers	/		
6-11	Providers should configure IoT system with password recovery mechanism such as: a) password reset information should be sent to other possible email address or an SMS text number; and		/	

	b) security questions which can only be answered by Consumers			
6-12	Providers should enforce password expiration policy in IoT system, whereby the maximum password expiration period is vary based on usage and security importance.		/	
6-13	Consumers should comply password security best practice and apply it in IoT system.			/
SC 7	**Access control**	**Manufacturers**	**Providers**	**Consumers**
7-1	Providers should create individual account in IoT system, either for human or machine, instead of group-based or role-based account.		/	
7-2	Providers should configure user privilege in IoT system to allow access in order to perform required tasks only.		/	
7-3	Providers should perform periodic access review whenever there is change in Consumers' status.		/	
SC 8	**Data protection and privacy**	**Manufacturers**	**Providers**	**Consumers**
8-1	Providers should classify data in IoT system according to its impact on Confidentiality, Integrity, Availability (CIA) triad and the data should be managed and protected based on data classification level.		/	
8-2	Manufacturers and Providers should ensure that IoT system provide Consumers the ability to agree or reject data collection and disclosure of personal data in order to control their privacy preferences.	/	/	
8-3	Manufacturers should design IoT system to allow Consumers to change their privacy preferences in configuration settings.	/		
8-4	Providers should ensure IoT system that collect, process and store personal data adhere to relevant laws.		/	

8-5	Providers should limit IoT system to collect, process and store data that adequate to perform its functions only.		/	
8-6	Providers should dispose any personal and sensitive data properly based on data retention policy and should adhere to data retention laws for regulated industries.		/	
8-7	In the event IoT devices that stored personal and sensitive data need to be disposed, Providers should implement secure data destruction methodologies before physically destroy the IoT devices, according to industry best practices.		/	
SC 9	**Operation and maintenance**	**Manufacturers**	**Providers**	**Consumers**
9-1	Manufacturers should provide documentation for IoT system such as user manual, product datasheet or IoT devices certification (if any) as a reference for Providers and Consumers.	/		
9-2	Providers and Consumers should ensure that any provision for IoT system includes documentation such as user manual, product datasheet or IoT devices certification (if any) which can be used as reference.		/	/
9-3	Providers and Consumers should ensure that any provision of IoT system covers maintenance service and technical support (warranty) for both hardware and software in which, the scope should also cover the damage and dysfunctionality due to cyber threats.		/	/
9-4	Providers and Consumers should ensure that any provision of IoT system covers the maintenance service and technical support (warranty) in accordance with the lifespan of IoT system.		/	/
9-5	Providers should maintain updated inventories for IoT system that cover both hardware and software.		/	
9-6	Providers and Consumers should ensure that they have the rights to control the credentials (username and password) used to access IoT system.		/	/

9-7	Providers should ensure that any installation of IoT system is verified and tested by a competent person.		/	
9-8	Providers should develop and implement preventive, remedial and maintenance plans for their IoT system to ensure operational continuity without unnecessary downtime.		/	
9-9	Providers should carry out security and vulnerability assessments on a schedule basis and as and when required for their IoT system.		/	
9-10	In the event of IoT system components (eg. OS, IoT device) are about to obsolete, Manufacturers should publish an end-of-life policy that explicitly states the minimum length of time for which the IoT system will receive updates and the reasons for the length of the support period.	/		
9-11	Manufacturers and Providers should implement IoT system with forensic readiness mechanism in order to assist any forensic procedure when required.	/	/	
9-12	Manufacturers should obtain relevant security certification eg: Common Criteria or at least go for product security testing.	/		

Bibliography

[1] Rahman A.F.A., Ahmad R. and Ramli S.N.: Forensics Readiness for Wireless Body Area Network System. The 16th International Conference of Advanced Communication Technology (ICACT 2014), ISSN: 17389445, pp 177-180, 2014

[2] Rahman A.F.A, Daud M, and Mohamad M.Z.: Securing Sensor to Cloud System using Internet of Things (IoT) Security Framework. Proceedings of the International Conference on Internet of things and Cloud Computing, Article No. 79, 2016

[3] Rahman A.F.A, AH. Azni, NHM. Alwi and K. Seman.: Measuring Sensor to Cloud Energy Consumption. Proc. 2nd International Conference on IoT and Cloud Computing ICC17, Article 186, 2017

[4] Rahman A.F.A, Azni A.H., Kamarulzaman N.S., Daud M., Mohamad M.Z., Yahood M.I.: Development of Denial of Service (DoS) Mitigation for Internet of Things (IoT) Sensor Node. Global Journal of Engineering and Technology Review, Vol 4 (2), pp 26-34, 2019

[5] Syamsul S.S.K, Rahman A.F.A, Salleh M.N.T., Mohamad F.A., Daud M., and Marshima M.R.: Comparison on Scorecard and Dashboard in Smart Water Monitoring Application. Proceedings of the 23rd Conference of Open Innovations Association FRUCT, 2018

[6] Rahman A.F.A., Ahmad R. and Mohamad M.Z.: Developing Forensic Readiness Secure Network Architecture for Wireless Body Area Network (WBAN). International Journal of Security and Its Applications. Vol. 8., pp 403-420, 2014

[7] M. Daud, R. Rasiah, M. George, D. Asirvatham, A. F. A. Rahman and A. A. Halim.: Denial of service: (DoS) Impact on Sensors. 4th International Conference on Information Management (ICIM), Oxford, 2018, pp. 270-274

[8] Rahman A.F.A and Mohamad M.Z.: Developing the Security Zone for Wireless Body Area Network (WBAN) Implementation Using Practical Security Assessment (PSA). Journal of Advance in Computer Network, Vol. 3, No. 2, pp 119-123, 2015

[9] Rao, S.; Chendanda, D.; Deshpande, C.; Lakkundi, V. Implementing LWM2M in constrained IoT devices. In Proceedings of the 2015 IEEE Conference on Wireless Sensors (ICWiSe), Melaka, Malaysia, 24–26 August 2015; pp. 52–57

[10] Sreekanth Anyapu, G. Aparna, R. Manognya, D. Ravi Kumar" Message Security Through Digital Signature Generation and Message Digest Algorithm" International Journal of Emerging Technology and Advanced Engineering Volume 3, Issue 3, March 2013

[11] Certified Cloud Security Professional 3rd Edition, (ISC)2 Inc

[12] MTSFB 001:2005 – Guidelines on Next Generation Network (NGN)

[13] Part IV – Maintenance of Installations, Suruhanjaya Tenaga Malaysia

[14] NIST Special Publication 800-88, Guidelines for Media Sanitization

[15] OWASP Internet of Things Project, IoT Security Guideline

[16] Storing Passwords in a Secure Way a SQL Server Database, available at https://www.mssqltips.com/sqlservertip/4037/storing-passwords-in-a-secure-way-in-a-sql-server-database/

[17] Microsoft Documentation on Account Lockout Threshold, available at https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold

[18] John, Spacey. 5 Examples of Non-repudiation. Simplicable, available at https://simplicable.com/new/non-repudiation

[19] Katie, Collins. Ukraine Blackout is a Cyberattack Milestone, available at https://www.cnet.com/news/cyberattacks-causes-widespread-power-blackout-in-ukraine

[20] Russia Looks to ITS to Curb Congestion and Reduce Accidents, available at https://www.itsinternational.com/categories/utc/features/russia-looks-to-its-to-curb-congestion-and-reduce-accidents

[21] Chris, Baraniuk. US Health Insurer Warns 3.7M After Cyber Attack, available at https://www.bbc.com/news/technology-36976701

[22] 'Thousands' of Known Bugs Found in Pacemaker Code, available at https://www.bbc.com/news/technology-40042584

[23] Russell, Brandom. UK Hospitals Hit with Massive Ransomware Attack, available at https://www.theverge.com/2017/5/12/15630354/nhs-hospitalsransomware-hack-wannacry-bitcoin

[24] Carter, Evans. California Hospital Computer System Taken "Hostage", available at https://www.cbsnews.com/news/california-hospital-computer-system-taken-hostage-by-hackers

[25] The DDoS That Didn't Break the Camel's VAC*, available at https://www.ovh.com/world/news/articles/a2367.the-ddos-that-didnt-break-the-camels-vac

[26] Mirai, available at https://www.cyber.nj.gov/threat-profiles/botnet-variants/mirai-botnet

[27] Paul, Kane. Major Security Breach Found in Hospital and Supermarket Refrigeration Systems, available at www.safetydetectives.com/blog/rdm-report

[28] Quality of Service, available at <https://www.skmm.gov.my/sectors/broadband/quality-of-service>

Acknowledgements

CyberSecurity Malaysia would like to express our appreciation and gratitude to all members who have participated tirelessly in the development of this guideline. Members of Technical Committee on Guideline for Secure Internet of Things (IoT) are as follows:

Ts. Dr. Zahri Yunos/	CyberSecurity Malaysia
Ts. Dr. Solahuddin Shamsuddin/	
Ts. Dr. Maslina Daud/	
Mr Abdul Fuad Abdul Rahman/	
Ms Fateen Nazwa Yusof/	
Mr Mohamad Nasrul Taufiq Salleh/	
Mr Muhamad Izzat Yahood/	
Mrs Nurul Syazwani Kamarulzaman/	
Mrs Shazwani Salleh/	
Mr Syamsul Syafiq Syamsul Kamal	
Mrs Noraishah Awaludin	Bank Negara Malaysia
Mr Saiful Bahry M.Hissham	Dell Global Business Center Sdn Bhd
Dr Gopinath Rao	Favoriot
Mr Ahmad Hafiz Mohd	German-Malaysian Institute (GMI)
Mr Abdul Fattah Mohd Yatim	Independent Expert IEM
Mrs Suhara Abdul Rahman	Jabatan Peguam Negara (AGC)
Mrs Siti Mariam Mohd Din	Jabatan Standard Malaysia
Mrs Lyana Shohaimay	Kementerian Komunikasi dan Multimedia Malaysia (KKMM)
Mrs Vimala Murugan	Kementerian Perdagangan Antarabangsa dan Industri (MITI)
Mrs Nas Fatehah Mahadi	Malaysia Digital Economy Corporation Sdn Bhd (MDEC)
Mr Paul Ng	Malaysia IOT Association (MyIoTA)
Mr Shahrulniza Musa	Malaysian Software Testing Board (MSTB)
Mrs Nur Hidayah Abdullah	MAMPU
Mrs Shariffah Rashidah Syed Othman	National Cyber Security Agency (NACSA)
Mr Kamaruzaman Abdol Rahim	Perbadanan Putrajaya (PPJ)
Prof. Dr. Raha Abdul Rahman	Pusat Perubatan Universiti Kebangsaan Malaysia (PPUKM)
Mrs Azleyna Ariffin	Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM)
Dr. Dzaharuddin Mansor	The National Tech Association Of Malaysia (PIKOM)
Mr Thaib Mustapa	TM Applied Business Sdn Bhd
Mrs Hafizah Mansur	Universiti Islam Antarabangsa Malaysia (UIA)