Guidelines

Internet of Things (IoT) Cyber Security Guide

In consultation with:

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

CSA SINGAPORE

IMDA IoT Cyber Security Guide
Version 2, Oct 2025

Info-communications Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Contents

This Guide is a living document which is subject to review and revision periodically.

Guides are informative documents and voluntary in nature except when it is made mandatory by a regulatory authority. It can also be reference in contracts as mandatory requirements. Users are advised to assess the suitability of this guide for their intended use.

Compliance with this guide does not exempt users from any legal obligations.

NOTICE

THE INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY ("IMDA") MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THE MATERIAL PROVIDED HEREIN AND EXCLUDES ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF NON-INFRINGEMENT, MERCHANTABILITY, SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. SUBJECT TO THE MAXIMUM EXTENT PERMITTED UNDER LAW, IMDA SHALL NOT BE LIABLE FOR ANY ERRORS AND/OR OMISSIONS CONTAINED HEREIN OR FOR ANY LOSSES OR DAMAGES (INCLUDING ANY LOSS OF PROFITS, BUSINESS, GOODWILL OR REPUTATION, AND/OR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES) IN CONNECTION WITH THE USE OF THIS MATERIAL.

IMDA DRAWS ATTENTION TO THE POSSIBILITY THAT THE PRACTICE OR IMPLEMENTATION OF THIS GUIDE MAY INVOLVE THE USE OF INTELLECTUAL PROPERTY RIGHTS AND TAKES NO POSITION CONCERNING THE EXISTENCE, VALIDITY AND/OR APPLICABILITY OF ANY SUCH INTELLECTUAL PROPERTY RIGHTS, WHETHER ASSERTED BY CONTRIBUTORS OF THIS DOCUMENT OR ANY THIRD PARTY.

AS OF THE DATE OF THE ISSUANCE OF THE PUBLIC CONSULTATION OF THIS GUIDE, IMDA HAS NOT RECEIVED WRITTEN NOTICE OF ANY PATENT RIGHTS WHICH MAY BE RELEVANT IN RELATION TO THE IMPLEMENTATION OF THIS GUIDE. HOWEVER, IMPLEMENTERS ARE CAUTIONED THAT THIS MAY NOT REPRESENT THE LATEST INFORMATION AND ARE THEREFORE STRONGLY URGED TO CHECK WITH THE RELEVANT DATABASE IN ITU, ISO, IEC OR THE RELATED STANDARDS DEVELOPMENT ORGANISATION FOR INFORMATION OF PATENT RIGHTS. IMPLEMENTERS ARE ADVISED TO OBTAIN THEIR OWN LEGAL AND/OR TECHNICAL ADVICE IN RELATION TO THE IMPLEMENTATION OF THE GUIDE IF REQUIRED.

IMDA IoT Cyber Security Guide

1 Introduction

The Internet of Things (IoT) brings together the physical environment and a wide range of objects such that they can interact with one another seamlessly through the use of Information and Communication (ICT) systems. It encompasses many supporting technologies such as sensing and control technologies, networking technology, information technology and software technology. Together, all these technologies enable sensors, actuators, middleware, data and communication networks, and applications, to interconnect to form an IoT ecosystem.

The significance of the economic impact of IoT is well-documented and increasingly being felt, with the increasing adoption of IoT solutions among consumers, enterprises and governments. Examples include connected wearables, smart homes, smart buildings, connected vehicles, video surveillance and analytics.

As people and devices become more connected, issues relating to the safeguarding of data and management of cyber security threats become increasingly important. IoT devices can collect significant amounts of information about their users and their environment, including personally identifiable, commercially confidential and/or sensitive data. For example, wearables can track an individual's steps, heart rate and sleep patterns while commercial sensors and actuators may expose enterprise control systems to the risk of data exfiltration, or even worse attacks. Measures will need to be taken to protect this large and growing volume of sensors and sensitive data.

Unfortunately, early IoT devices have several vulnerabilities which may be easily exploited, making them easy targets for cyber security attacks. For instance, compromised devices can be controlled by a botnet and be made to participate in Distributed Denial-of-Service (DDoS) attacks on other organisations.

Security has been consistently ranked as the top concern inhibiting user adoption. On the other hand, industry has provided feedback that conforming to existing standards not designed with IoT in mind, is time-consuming, costly and impractical for the dynamic and evolving technologies and applications of IoT.

Protecting organisations and individuals from rising cyber threats is a national priority as well as an area of economic opportunity. It is integral to ensuring that Singapore remains cyber secure in a digital economy, with a set of trusted infrastructure to support our Smart Nation initiatives.

Similar to any system, an IoT system is as secure as its weakest link. It is thus important to ensure that proper security considerations and measures are put in place for both the implementation and operational stages of the deployment of any IoT system. This document aims to provide guidance to users and enterprises when procuring, deploying and operating IoT devices/systems, while enabling solution providers to verify the security posture of their solutions, by providing practical guidelines that include baseline recommendations, foundational concepts and checklists. A risk-based and system-oriented approach is taken to identify and mitigate threats to IoT solutions. Enterprise users and their vendors are guided to work together to secure their IoT systems over their lifecycles.

2 Scope

This document serves as a practical guide for enterprise users (and their vendors) that intend to deploy IoT solutions, providing baseline recommendations[1], foundational concepts and checklists, which focus on the security aspects for the acquisition, development, operations and maintenance of IoT systems.

It focuses primarily on system-level recommendations and builds on the concepts introduced in Singapore Standard, SS711:2025 “IoT security for Smart Nation – Concepts and common requirements” and provides further details on the implementation of IoT security through case studies.

This guide can be used by:

i) IoT developers who want to design, develop and deploy secure IoT products and systems. Examples of developers include solution architects, programmers, manufacturers and system integrators.

ii) IoT providers who need to roll-out, configure, operate, maintain and de-commission IoT systems securely. Examples of providers include network operators, platform providers, data analysts and service delivery managers.

iii) IoT users who want to procure and interact with IoT systems. For system interactions, IoT users can by either human or software agents.

With respect to the lifecycles of IoT systems, IoT developers are mainly involved in the implementation phase, which covers the design, develop, deploy, integrate and test stages, while IoT providers are involved in the operational phase, which covers the operate, support, maintain, upgrade and retire stages. IoT users could be involved in both the implementation and operational phases. It should be noted that multiple cycles of implementation and operation phases could take place with the introduction of new features over the entire life-span of an IoT system.

[1] This guide does not cover areas on privacy. Guidelines on privacy are available on the website of Personal Data Protection Commission (PDPC) at https://www.pdpc.gov.sg/Legislation-and-Guidelines/Guidelines.

3 References

In this document, reference has been made to the following standards. Where versions are not indicated, reference shall be based on current and valid versions of these standards published by the respective Standards Development Organisations.

[1] Cloud Security Alliance IoT Controls Framework

[2] ENISA Baseline security recommendations for IoT

[3] ETSI TS 103 645 cyber security for consumer IoT

[4] GSMA IoT security guidelines for endpoint ecosystems

[5] IEC 62443-3-3 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels

[6] Online Trust Alliance – IoT trust framework

[7] OWASP – https://www.owasp.org/index.php/Application_Threat_Modeling

[8] Singapore Standard, SS695:2023 “IoT interoperability for Smart Nation”

[9] Singapore Standard, SS711:2025 “IoT security for Smart Nation – Concepts and common requirements”

4 Terms and definitions

Access Control	Functions, which include identification, authentication, authorisation and accountability.
Authentication	Act of confirming the identity of an entity.
Authorisation	Act of specifying the access permissions to a resource.
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Denial of service (DoS)	Prevention of authorised access to a system resource or the delaying of system operations and functions, with resultant loss of availability to authorised users.
Identification	Act of stating the identity of an entity.
Internet of Things (IoT)	System of physical and virtual entities that are connected with one another, allowing interaction anytime, anywhere.

5 Abbreviations and acronyms

APN	Access Point Name
CIA	Confidentiality, Integrity, Availability
DoS	Denial of Service
DDoS	Distributed Denial of Service
DNS	Domain Name System
DTLS	Datagram Transport Layer Security
ENISA	European Network and Information Security
ETSI	European Telecommunications Standards Institute
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IoT	Internet of Things
ISG-CERT	Info-communications Singapore Computer Emergency Response Team
IT	Information Technology
JTAG	Joint Test Action Group
MFA	Multi-Factor Authentication
MQTT	Message Queueing Telemetry Transport
NIST	National Institute of Standards and Technology
OT	Operational Technology
OTA	Over-The-Air
PDPC	Personal Data Protection Commission of Singapore

SingCERT	Singapore Computer Emergency Response Team
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOP	Target Of Protection
TPM	Trusted Platform Module
TR	Technical Reference
TS	Technical Specification
UDP	User Datagram Protocol
UTF	Unicode Transformation Format
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network

6 Baseline recommendations for the implementation phase

6.1 Introduction

Section 6 provides a set of baseline security recommendations for IoT users and IoT developers during the implementation phase.

The recommendations cover four fundamental IoT security design principles (refer to SS711:2025 for more details):

1. Secure by defaults
2. Rigour in defence
3. Accountability
4. Resiliency

Individual products are used to implement a system and the system operates in the context of an organisation's processes, policies and people. The increasing levels of integration, from product to system and finally organisation require additional considerations, as the overall security posture is only as strong as its weakest links. Together, the recommendations are fundamental to safeguarding the IoT system systematically and over its lifecycle.

While the baseline recommendations provided in this document are common across a majority of IoT systems, the IoT users and IoT developers need to determine the appropriateness of the recommendations for the intended systems/solutions, based on the business needs and relevant regulatory requirements.

6.2 Principle 1: Secure by defaults

6.2.1 Employ strong cryptography

Strong cryptographic capabilities are the fundamental building blocks used to ensure the security of data transactions, including authentication and sensing data exchange between IoT devices. Examples of the usage of cryptographic capabilities include digital signatures and encryption.

Recommendation: Industry accepted cryptographic techniques and best practices shall be applied appropriately and adequately on for the IoT system. Examples of best practices include:

- use of approved algorithms
- sufficient key length
- use of approved random number generator(s)
- recommended crypto-period
- recommended entropy sources
- use of updatable cryptography

6.2.2 Protect impactful data

Impactful data of the IoT system can refer to keys, credentials, codes/firmware, personal data, inputs/commands and sensing data, etc. Access to impactful data should require assurance and/or verification that it originates from authentic sources, and be protected from tampering, modification and/or disclosure to unauthorised parties.

Recommendation: Impactful data shall be checked for authenticity and protected from disclosure and modifications by unauthorised parties. All sensitive communications to/from IoT devices shall be encrypted.

6.3 Principle 2: Rigour in defence

6.3.1 Conduct threat modelling

Threat modelling provides a systematic approach, which helps to identify the system assets, the security needs of the system assets and the possible threats to these system assets so that the limited available resources can be focused on what needs to be protected. Threat modelling[2] helps to minimise the exposed attack surfaces and mitigates the remaining vulnerabilities.

Recommendation: Threat modelling should be conducted at the start of the implementation phase, and account for the intended usage of IoT devices within the defined operating environments.

6.3.2 Establish Root-of-Trust

Root-of-Trust provides a tamper protected module that stores and protects the keys of the devices so as to establish a firm foundation for other security mechanisms to build upon, hence achieving higher assurance of security through a chain of trust.

Recommendation: Root-of-Trust should be established and utilised by key system components, such as IoT gateways and IoT platforms, as they may host sensitive data and execute impactful operations. For example, Root-of-Trust can be based on a Trusted Platform Module (TPM) chip embedded in the device, or a virtual secure element integrated within the device's software.

6.3.3 Employ secure transport protocols

Transport protocols are used to transfer data within and between systems. It is thus important to ensure that secure versions of transport protocols are properly configured, protecting data in transit effectively.

Recommendation: Proven transport protocols[3] shall be employed with security controls properly activated, wherever possible. Examples of security controls of proven transport protocols include:

- use of TLS for TCP payloads
- use of DTLS for UDP payloads
- use TLS when using MQTT
- disable non-authenticated Bluetooth pairing procedures

6.4 Principle 3: Accountability

6.4.1 Enforce proper access controls

Access to system resources shall be controlled and managed throughout its lifecycles, minimising opportunities for malicious actors. Default passwords and weak passwords are the most commonly exploited vulnerabilities. The use of Multi-Factor Authentication (MFA) provides a higher assurance of the identity of initiators, enhances accountability and mitigates against mistakes.

Recommendation: Proper access controls, both cyber and physical, for devices, networks and data shall be enforced. Fundamental access controls include:

- Replacement of all default passwords
- Enforcement of strong passwords as specified in section 7.2.1
- Enforcement of multi-factor authentication (MFA) for impactful remote operations
- Securing physical access to devices and their service ports

[2] A threat modelling checklist is provided as a reference in section 8 of this document

[3] The latest versions of transport protocols should be employed, whenever possible.

6.4.2 Provide audit trails

Intentional misuse, bypassing restrictions and misconfigurations are still potential risks even with the proper implementation of access control measures. It is thus important to have audit trails.

Recommendation: All attempts to access sensitive data and altering system resources shall be properly monitored and logged.

6.5 Principle 4: Resiliency

6.5.1 Guard against resource exhaustion

IoT systems are vulnerable to resource exhaustion attacks. Attackers and compromised devices can send requests continuously to IoT devices/networks/systems to deplete its resources and impact systems' availability.

Recommendation: The system should employ mechanisms to protect against malicious attacks such as DDoS. Examples include:

- Monitor system/device resources are sufficient to sustain services.
- Detect resource exhaustion for early intervention.
- Specific control over resource-intensive software.
- Enforce power consumption thresholds on IoT devices.
- Limit number of concurrent sessions.
- Operate with excess capacity.

7 Baseline recommendations for operational phase

7.1 Introduction

Section 7 provides a set of baseline security recommendations for IoT users and IoT providers during the operational phase.

The recommendations are organised according to the same four fundamental IoT security design principles used in section 6.

While the baseline recommendations provided in this document are common across a majority of IoT systems, the IoT users and IoT providers need to determine the appropriateness of the recommendations for the intended systems/solutions, based on the business needs and relevant regulatory requirements.

7.2 Principle 1: Secure by defaults

7.2.1 Use strong credentials

Weak credentials, e.g., user identifications and passwords have consistently been placed as top vulnerability, which are subjected to brute-force attacks.

Recommendation: Default credentials shall be avoided, and strong passwords shall be used throughout the system. Password complexity (strength) should adhere to the published international best practices if regulatory requirement is not available. Minimally, passwords should consist of 8 or more characters comprising a combination of letters and numbers. It is also encouraged that symbols and upper-case characters be used to enhance password strength.

Multi-factor authentication should be enabled, whenever possible, for access to impactful data and operations.

7.3 Principle 2: Rigour in defence

7.3.1 Segment IoT and enterprise networks

A single compromised device can be the attack vector into your enterprise systems.

Recommendation: Network segmentation should be employed so that IoT devices belonging to different networks can be properly segmented from one another and also from other corporate enterprise systems and networks. Firewalls and malware mitigation solutions should be implemented to protect each network whenever possible.

7.4 Principle 3: Accountability

7.4.1 Establish proper device management

All connected devices are potentially exposed to malicious actors, and may be exploited, allowing cyberattacks to compromise the whole IoT system. Stolen devices can be tampered with, reverse-engineered and used against the IoT system. Outdated and unpatched firmware/software can contain known vulnerabilities that malicious actors can exploit. Hence, proper management of connected devices is critical to ensure the security of the whole system.

Recommendation: Proper management of devices, including firmware/software updates and patches, shall be established. An inventory of connected devices, software and firmware versions[4] should be kept and up-to-date patches should be applied throughout the "Operational" lifecycle stage. Access controls, including for physical access to IoT devices, should be strictly enforced. IoT users and IoT providers should subscribe to notifications and advisories issued by IMDA's ISG-CERT and Cyber Security Agency (Singapore)'s SINGCERT, as appropriate, to be apprised of newly discovered vulnerabilities and threats to IoT and ICT systems.

7.5 Principle 4: Resilience

7.5.1 Recover from attacks

IoT systems will be targeted for attacks, especially if the asset is valuable enough. A determined attacker will find a way to compromise the system as more sophisticated attacking tools are developed. There is therefore a need to be prepared to fail safely and recover from it, especially when the compromise of an IoT system can affect the safety of humans or facilities.

Recommendation: Regular backups of system data (include settings) as well as regular disaster recovery exercises for systems shall be conducted.

7.5.2 Conduct periodic assessments

An IoT system can be a dynamic and complex system. As threats are always evolving, periodic penetration testing and/or vulnerability assessment is required to mitigate security risks.

Recommendation: Penetration testing and/or vulnerability assessments of the IoT system should be conducted periodically. Threat modelling should be conducted as part of vulnerability assessments.

[4] IoT users and IoT providers may be dependent on IoT developers to provide patches for new vulnerabilities in a timely manner.

8 Threat modelling checklist

This section provides a suggested checklist for threat modelling. The checklist can be used to guide the threat modelling process and ensure that it is conducted properly and systematically. While STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) is the model used to help analyse and find threats to the system. It should be noted that other methodologies exist and might be more appropriate for specific use cases.

Please refer to the case study in annexes for an illustration of the application of the threat modelling checklist.

ID	Threat modelling checklist	Y (yes) / N (no)	Supporting materials
1	Identify the potential target(s) to be protected i) Define its boundaries and the external systems (including users) that it needs to interact with ii) Decompose the target(s) into its subcomponents iii) Identify data flows within the target(s), and inputs and outputs from external systems iv) Identify sensitive data and where they are handled (at rest, in transit, in use) v) Identify the security needs (based on potential impacts to Confidentiality, Integrity and Availability (CIA triad)) for subcomponents and data flows vi) Identify hardware, software and protocols in use		
2	Define the security problem i) Identify system accessibility – Identify attack surfaces – Determine operating environments – Determine system / device lifecycles and supply chain ii) Identify system susceptibility / vulnerabilities (e.g. using STRIDE as a guide) – Determine known vulnerabilities – Enumerate threats to attack surfaces – Enumerate threats to operating environments – Enumerate threats to stages of system / device lifecycles and supply chain iii) State any assumptions		
3	Conduct risk assessment i) Assess impact of threats and vulnerabilities to CIA triad and match against security needs of assets ii) Determine the system exploitability (resources required, techniques and tools available) to realise threats. iii) Assess the likelihood of the risk iv) Prioritise risks for mitigation, considering factors such as monetary impacts.		
4	Determine the security objectives. For example, OT system emphasises safety, where integrity takes precedent over confidentiality.		
5	Define the security requirements needed to address identified security objectives, without specifying their implementation details.		
6	Design and implement the security capabilities		
7	Validate and verify that the capabilities address the security requirements adequately		

9 Vendor disclosure checklist

This section provides a non-exhaustive list of security questions that enterprise solution vendors can use for self-disclosure. It identifies the possible important security capabilities/services that vendors should focus on and also, allows users to better evaluate and compare the security aspects of the IoT solutions/systems proposed by different vendors. Thus, this checklist facilitates communication, enables fair comparisons of security across IoT solutions and promotes the implementation of better security. Notwithstanding the described uses of the checklist, it should be noted that the checklist is only a template of common security considerations. Users are required to determine the appropriateness and applicability of the checklist items so as to add on, remove, and/or adjust them according to the uses and businesses' needs.

Please refer to the case study in annexes for an illustration of the application of the vendor disclosure checklist.

Vendor disclosure checklist	**Y (yes) / N (no) / NA (not applicable)**	**Supporting materials**
1. Cryptographic support		
CHECK-CS-01: Do your devices and system employ industry-accepted cryptography and best practices? Examples include the use of: a) Accepted algorithms and their correct implementation and application. b) Accepted entropy sources and approved random number generator(s). c) Sufficient key length. d) Sufficient crypto-period. e) Use of updatable cryptography.		
CHECK-CS-02: Do you define and implement proper key management practices (generation, exchange, storage, use, destruction and replacement) accordingly to industry-accepted best practices and recommendations?		
2. Security function protection		
CHECK-FP-01: Do you employ and properly implement a trusted computing base (TCB) according to industry-accepted recommendations and best practices? The TCB should include: a) policies; b) hardware; c) firmware; d) operating systems;		

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
e) virtualisation; f) software; g) basic input/output system; h) system services; i) device drivers; j) protocols; k) RoT; and l) trust anchor.		
CHECK-FP-02: Do you establish RoT for your devices and system, according to industry-accepted best practices and recommendations?		
CHECK-FP-03: Do you employ secure boot mechanisms to protect and verify software according to industry-accepted best practices and recommendations? If an unauthorised change to the software is detected, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.		
CHECK-FP-04: Do you protect security data elements, such as credentials, keys, and tokens, from unauthorised disclosure and modification according to industry-accepted best practices and recommendations?		
3. Identification and authentication		
CHECK-IA-01: Do you establish unique, non-modifiable, and verifiable identities for IoT entities (i.e., users, platforms, gateways, devices)?		
CHECK-IA-02: Do you securely provision and manage the credentials of IoT entities (i.e., users, platforms, gateways, devices)? For example, by being salted, hashed, or encrypted.		
CHECK-IA-03: Do you employ secure authentication mechanisms according to industry-accepted best practices and recommendations?		
CHECK-IA-04: Do you establish mutual authentication before any interactions between clients (users, devices, gateways, applications) and servers?		
4. Network protection		
CHECK-NP-01: Do you employ proven transport protocols and recommended network services with properly activated security controls?		

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
Examples of best practices for transport protocols include using the following: a) TLS for TCP payloads. b) DTLS for UDP payloads. c) TLS for MQTT. d) HTTPS.		
CHECK-NP-02: Do you establish secure connectivity according to industry-accepted best practices and recommendations? Examples include: a) Use of VPN. b) Use of private mobile access point names (APN) from telecommunication operators when using a public mobile carrier network. c) Use of secure DNS to prevent DNS spoofing. d) Use of traffic filtering based on type, port, and destination. e) Use of mutual TLS (mTLS). f) Use whitelisting to establish or deny connections from non-trusted sources. Additionally, IETF Request for Comments (RFC) 8520 Manufacturer Usage Description (MUD) can be a mechanism for devices to provide this information to the network.		
CHECK-NP-03: Do you employ segregation of communication channels for endpoints with varying trust-levels according to industry-accepted best practices and recommendations? Examples include using VLAN, firewalls for DMZ, unidirectional security gateway, network segmentation or micro-segmentation, and physical isolation.		
CHECK-NP-04: Do you implement network monitoring and access control according to organisational information flow control policy? Examples of access control include: a) Use of secure authorisation mechanisms for each connection to join a network. b) Use of secure de-authorisation mechanisms for each connection to disconnect and forget a network.		
5. Data protection		

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
CHECK-DP-01: Do you protect data in transit, in use, and at rest, from unauthorised disclosure and modification according to industry-accepted best practices and recommendations? Examples of data include, but are not limited to, security data, personal data, sensing data, metadata, event logs, software, and their configurations.		
CHECK-DP-02: Do you provide evidence and means to attest the authenticity and integrity of data-in-transit, data-in-use, and data-at-rest according to industry-accepted best practices and recommendations? Examples include using hashing and digital signatures. These data include sensing data, software, and its configurations.		
CHECK-DP-03: Do you implement input validation to safeguard input data, which includes commands and sensing data? Examples of input validation include: a) Validating incoming content types. b) Validating response types. c) Validating the HTTP methods against authorisation credentials. d) Whitelisting allowable HTTP methods. e) Defining the acceptable character set, e.g., Unicode Transformation Format-8 (UTF-8). f) Validating that input characters are acceptable. g) Encoding/escaping input and output. h) Checking for anomalies.		
CHECK-DP-04: Do you enforce access control to detect and prevent unauthorised data access and data exfiltration? Additionally, do you verify and filter independently data output, including commands and processed sensing data?		
6. Access protection		
CHECK-AP-01: Do you employ session management to secure interactions for different clients according to industry-accepted best practices and recommendations? Examples include: a) Verify and protect the integrity of sessions. b) Restrict access by client types.		

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
c) Restrict data transfer and file transfer by clients.		
CHECK-AP-02: Do you implement lock-out mechanism to protect against repeated unauthorised attempts by any user (human, software or device)? Examples of mechanisms include delay in between login attempts, lock-out for repeated unauthorised attempts, and forced reauthorisation.		
CHECK-AP-03: Do you employ multi-factor authentication (for user access) and timely notifications?		
CHECK-AP-04: Do you enforce physical and remote access restriction to safeguard against unauthorised access to assets, equipment, user devices, removable media, and interfaces?		
CHECK-AP-05: Do you employ anti-tampering mechanisms to detect, prevent, make evident and/or respond to physical attacks?		
7. Security audit		
CHECK-AU-01: Do you synchronise your clocks to authoritative time sources to provide timestamps for audit records?		
CHECK-AU-02: Do you record security events to facilitate monitoring, analysis, and timely alerts raised (e.g., who does what and when) regarding activities performed? Examples of security events include the following: a) User logins, logouts, and unsuccessful authentication attempts. b) Connection, disconnection attempts and unsuccessful connection attempts. c) Unsuccessful authorisation attempts. d) Access to sensitive data. e) Import and export of data from removable media. f) Any change in access privileges. g) Creation, modification, and deletion of data by user. h) Remote operations. i) Security update failures. j) Physical access attempts where possible. k) Emergency access where possible. l) Configuration changes.		

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
CHECK-AU-03: Do you protect audit records from unauthorised operations (create, read, update and delete)? Do you allocate sufficient record storage, and raise timely alerts before records are overwritten?		
8. Security management		
CHECK-SM-01: Do you employ strong credential management according to industry-accepted best practices and recommendations? Examples include: a) Enforcing a strong password policy. b) Enforcing no default passwords. c) Specifying password expiration periods. d) Ensuring that password recovery and reset mechanisms are secure. e) Randomising pre-loaded login credentials. f) Use of FIDO2 security tokens.		
CHECK-SM-02: Do you employ access control policies and mechanisms to manage system, networks, and devices according to industry-accepted best practices and recommendations. Examples include: a) Use of attribute-based access control (ABAC) or role-based access control (RBAC). b) Enforce a least privilege policy. c) Restrict and manage privilege access rights.		
CHECK-SM-03: Do you employ protection mechanisms to detect and mitigate the effects of unauthorised and malicious software and hardware? Examples include the following: a) Ensuring file integrity using cryptographic hash. b) Baselining normal behaviour. c) Detecting unauthorised software. d) Monitoring devices and traffic flows. e) Scanning software and backup images. f) Prohibiting insecure bootloaders.		
CHECK-SM-04: Do you employ protection mechanisms to secure the remote management of devices and gateways?		

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
Examples include: a) Supporting secure OTA updates of device applications and configurations. b) Supporting software and/or firmware updates using secure processes and cryptographically secure methods. c) Supporting platform integrity checking such as the measured boot mechanism or verifying the firmware integrity. d) Restricting remote management to secure networks.		
9. Resiliency support		
CHECK-RS-01: Do you employ mechanisms to support integrity self-test, error detection, correction for critical functions, and return to a safe state? For example, leaving the device in a state that minimises potential for harm during an unexpected interruption of an update, taking into account the risks of the IoT device not functioning as expected.		
CHECK-RS-02: Do you implement measures to protect against failures from outages, resource exhaustion, and/or malicious DoS attacks? Examples include the following: a) Monitoring to ensure that cloud resources are sufficient to sustain services. b) Detecting resource exhaustion for early preventive or corrective actions. c) Controlling the execution of resource-intensive software. d) Enforcing power thresholds. e) Limiting the number of concurrent sessions. f) Having the capacity to operate during resource outages (e.g., power, network) or the ability to operate in a degraded mode.		
CHECK-RS-03: Do you employ mechanisms to periodically back up system data, including their settings? Do you conduct disaster recovery exercises to verify the backup and recovery mechanisms?		
CHECK-RS-04: Do you maintain or degrade the IoT system and devices to a safe and expected state on encountering errors/failures? Do you provide timely alerts, with sufficient information, to relevant authorised users to support effective remediation?		
10. Lifecycle support		

Vendor disclosure checklist	**Y (yes) / N (no) / NA (not applicable)**	**Supporting materials**
CHECK-LP-01: Do you conduct threat modelling to identify, analyse, assess, and document threats to the IoT system?		
CHECK-LP-02: Do you design and develop your IoT solution according to industry-accepted secure systems engineering approaches, best practices, and recommendations?		
CHECK-LP-03: Do you construct and maintain your IoT solution using components with no known unmitigated vulnerabilities?		
CHECK-LP-04: Do you identify and manage supply chain risks with defined processes and procedures, including risks from the use of opensource software?		
CHECK-LP-05: Do you harden your IoT solution before putting it into operation? Examples of system hardening include the following: a) Removing all backdoors; b) Removing all debug codes from the released version; c) Enabling secure configuration and settings; d) Removing unnecessary software and services; e) Removing or tamper-covered JTAG; f) Removing unnecessary serial ports and other ports before deployment; g) Appropriate hardening of VM host, including disabling memory sharing between VMs; h) Removing default and hardcoded passwords; and i) Removing unused networks and interfaces.		
CHECK-LP-06: Do you provide, communicate, and update security information in a timely manner? Examples of security information include the following: a) Terms of service. b) Support policies. c) Security guidelines, instructions, and educational materials. d) Security notifications and updates. e) Instructions for device/media sanitisation. f) Phase out plan and end-of-life notifications.		

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
CHECK-LP-07: Do you maintain an information inventory of system components and assets throughout the IoT system operation? Examples include the following: a) Supplier information. b) Hardware models and versions, including physical locations. c) Software and firmware versions, including applied patches and updates. d) Configurations and settings, including IP addresses, ports, protocols, and services. e) Maintenance status.		
CHECK-LP-08: Do you conduct penetration testing and vulnerability scanning as part of the security assessment, before commissioning, periodically, and before each major release? Do you enable and test all optional, non-default features of the IoT devices for security?		
CHECK-LP-09: Do you establish vulnerability management and disclosure according to industry-accepted best practices and recommendations? Examples include the following: a) Ensuring the supply chain's capability to provide upgrades and patches. b) Providing vulnerability disclosure and processes to track and respond promptly. c) Providing firmware and software patches/updates for discovered vulnerabilities in a timely manner. d) Employing proper change management processes to manage security patches or updates. e) Notifying and/or allowing users to approve/reject updates, patches, and changes to user settings, where appropriate. f) Disclosing minimum support period.		
CHECK-LP-10: Do you manage identities, certificates, and secrets securely throughout their lifecycles, including creation, provisioning, renewal, and revocation?		
CHECK-LP-11: Do you employ mechanisms for the proper disposal of devices and systems, and for resetting or sanitising sensitive data by authorised users when feasible, according to industrial best practices?		

Vendor disclosure checklist	**Y (yes) / N (no) / NA (not applicable)**	**Supporting materials**
Examples include the option to factory reset, erase and zeroise both security data and user data.		

10 Bibliography

[1] https://cve.mitre.org/

[2] https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[3] Industrial Internet of Things: volume G4 – Security framework

[4] ISO/IEC 27000 Information security management systems – Information security risk management

[5] ISO/IEC 27002 Information security management systems – Code of practice for information security controls

[6] NIST Special Publication (SP) 800-63B Digital identity guidelines – Authentication and lifecycle management

[7] Strategic principles for securing the Internet of Things (IoT) – U.S. Department of Homeland Security

[8] Singapore Standard SS 695:2023 IoT interoperability for Smart Nation

[9] Singapore Standard SS 711:2025 IoT security for Smart Nation – Concepts and common requirements

[10] TS-0003 OneM2M technical specification – Security solutions