सत्यमेव जयते

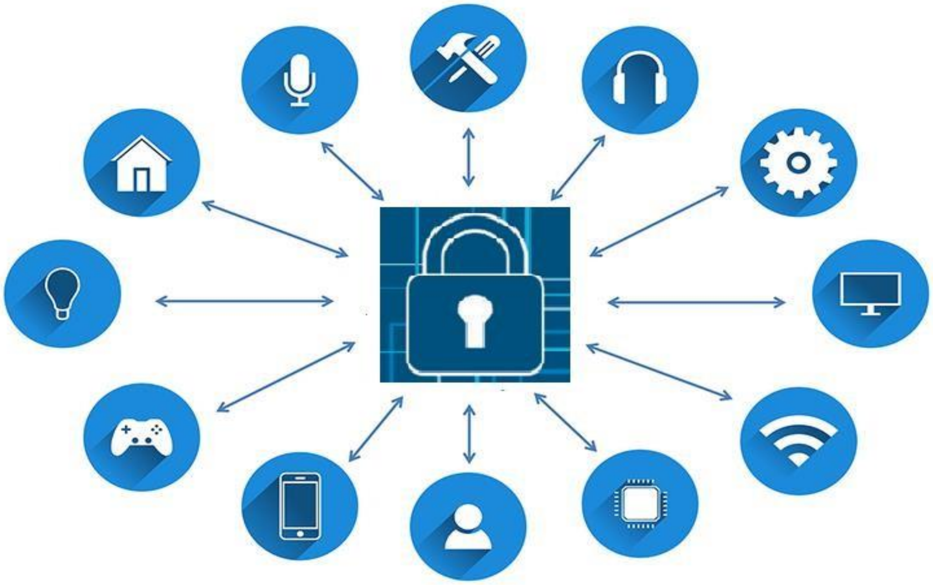
Code of Practice

for

Securing

Consumer Internet of Things (IoT)

TEC 31318:2025



ISO 9001 :2015

TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS
MINISTRY OF COMMUNICATIONS
GOVERNMENT OF INDIA

RELEASE 2.0

TEC 31318:2025

Revision history

Date	Release	Document No.	Description
August 2021	R 1.0	TEC 31318:2021	Code of practice for securing Consumer Internet of Things (IoT)
November 2025	R 2.0	TEC 31318:2025	Code of practice for securing Consumer Internet of Things (IoT)

Important Notice

Individual copies of the present document can be downloaded from **www.tec.gov.in/M2M-IoT- technical-reports**
Users of the present document should be aware that the document may be subject to revision or change of status.
Any comment/suggestions may please be sent to: **adet.iottec-dot@gov.in**

Disclaimer

The information contained is mostly compiled from different sources and no claim is being made for being original. Every care has been taken to provide the correct and up to date information along with references thereof. However, neither TEC nor the authors shall be liable for any loss or damage whatsoever, including incidental or consequential loss or damage, arising out of, or in connection with any use of or reliance on the information in this document. In case of any doubt or query, readers are requested to refer to the detailed relevant documents.

Table of Contents

Executive Summary

IoT is one of the fastest emerging technology across the globe which is being used to create smart infrastructure in various verticals using connected devices. IoT is benefitted by recent advances in several technologies such as sensors, communication technologies (Cellular and non-cellular), AI/ ML, Cloud computing, Edge computing etc.

The number of connected IoT devices is projected to grow by 14% in 2025, reaching approximately 21.1 billion devices. Further, it is projected that global IoT connections will expand to around 39 billion by 2030 and exceed 50 billion by 2035[1].

As per the National Digital Communication Policy (NDCP)[2] 2018 released by Department of Telecommunications (DoT), an eco-system is to be created for 5 billion connected devices.

In view of the anticipated growth of IoT devices, it is important to ensure that the IoT end points comply to the safety and security standards and guidelines in order to protect the users and the networks that connect these IoT devices. The IoT devices must undergo mandatory testing & certification prior to sale, import or use in India, in compliance to the MTCTE guidelines issued by Department of Telecommunications (DoT), Government of India under the Telecommunications (Framework to Notify Standards, Conformity Assessment and Certification) Rules, 2025.

The certified devices may also become vulnerable after deployment due to new vulnerabilities being discovered. To address such issues, a central mechanism like a National Trust Center (NTC) is required to ensure the registration of certified devices, enabling users and networks to distinguish the good from the potentially rogue ones. The repository may also be used to record vulnerabilities discovered in the certified devices to provide a mechanism of continuous improvement in safety and security of the devices and the networks.

TRAI in its recommendations on “Spectrum, Roaming and QoS related requirements in Machine-to-Machine Communications”, released in September 2017, had also mentioned the following requirements which have been accepted by DoT:

1. Device manufacturers should be mandated to implement “Security by design” principle in M2M devices manufacturing so that end to end encryption can be achieved.
2. A National Trust Center (NTC), under the aegis of TEC, should be created for the certification of M2M devices and applications (hardware and software). *This recommendation was accepted in principle by DoT.*

Since different devices may be subject to different levels of security risks, therefore, devices will be required to be classified depending upon the risk associated with the application.

[1] https://iot-analytics.com/number-connected-iot-devices/
[2] https://dot.gov.in/sites/default/files/Final%20NDCP-2018_0.pdf

TEC has released a technical report on *Code of Practice for consumer IoT security* in August 2021 which details the baseline requirements for securing consumer IoT based on ETSI EN 303 645 (V2.1.1) (06-2020). This technical report has been revised reflecting the updates in ETSI EN 303 645 (V3.1.3) (2024-09). ETSI has also released ETSI TS 103 701[3] which describes Conformance Assessment criteria for assessing products against baseline requirements in ETSI TS 103 645 and ETSI EN 303 645.

TEC has published key technical reports on “Security by Design Principles for IoT Device Manufacturers” and “the framework of the National Trust Centre (NTC) for M2M/IoT devices and applications”. These reports have been adopted by the International Telecommunication Union (ITU) and are now available on the ITU’s global resource platform, where they are being referenced and utilized worldwide to promote secure and trusted IoT ecosystems.

[3] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/02.01.01_60/ts_103701v020101p.pdf

1. Introduction

IoT / M2M technology is being used to create smart infrastructure in various verticals such as Power Sector, Automotive, Safety & Surveillance, Remote Health Management, Agriculture, Smart Homes and Smart Cities etc. The hacking of the devices/networks being used in daily life would harm companies, organizations, nations and more importantly people, therefore securing the IoT eco-system end-to-end i.e. from devices to the applications is very important. An IoT network that has been compromised may result in the collapse of services, creating panic and chaos. Ensuring end to end security for connected IoT devices is key to success in this market - without security, IoT will cease to exist. Apart from security, the privacy of the data of the individuals is another very important domain, especially in sectors like health care. According to a market research report published by Markets and Markets, the global Internet of Things (IoT) security market size is expected to grow from USD 24.2 billion in 2024 to USD 56.2 billion by 2029 at a CAGR of 18.4 percent during the forecast period[4].

IoT devices, services & software and the communication channels that connect them are at risk of attack by a variety of malicious parties, from novice hackers to professional criminals and even state actors. Possible consequences of such attacks could include:

- Discontinuity and interruption to critical services/infrastructure
- Infringement of privacy
- Loss of life, money, time, property, health, relationships, etc.
- Disruptions of national scale including civil unrest.

For vendors, operators and suppliers, potential consequences may include loss of trust, damage to reputation, compromised intellectual property, financial loss and possible legal liabilities.

Data can be leaked by malicious actors taking advantage of poor design. Even the unintentional leakage of data due to ineffective security controls can also have dire consequences to consumers and vendors. Thus IoT devices and services must have security designed-in from the very outset.

As per IoT Security Foundation (IoTSF) a Vulnerability Disclosure Policy[5] is a publicly available document, typically accessed via the Vendor’s reporting web page. It is the Vendor’s statement as to how they will handle any vulnerability report passed to them. Such a policy enables coordinated handling of security issues and strengthens overall trust in IoT products and services. This is of great concern as vulnerability disclosure is widely considered to be a baseline requirement due to its fundamental importance towards operational IoT security. This report has mentioned that only a few companies are working on vulnerability disclosure despite incoming laws and international standards. Thus, it is imperative that the providers of IoT products implement the vulnerability disclosure policy on priority.

[4] https://www.marketsandmarkets.com/Market-Reports/iot-security-market-67064836.html

[5] https://iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf

ETSI released ETSI EN 303 645 (V2.1.1) in June 2020 which covers 13 basic principles for securing consumer IoT[6]. ETSI has further released ETSI EN 303 645 (V3.1.3) in September 2024, which serves as the updated European Standard for Cyber Security for Consumer Internet of Things: Baseline Requirements[7]. This latest version builds upon the foundation established in previous editions, strengthening security, privacy and usability requirements for consumer IoT devices. ETSI EN 303 645 (V3.1.3) continues to outline 13 key cybersecurity provisions aimed at mitigating the most common and significant security risks in IoT products. The standard aligns closely with evolving global cybersecurity practices and supports conformity assessment through ETSI TS 103 701, which provides corresponding test scenarios for evaluating compliance with ETSI TS 103 645 and ETSI EN 303 645.

UK and Australia have released Code of practice for consumer IoT security in 2018[8] and 2020[9] respectively and are having the similar 13 guidelines as available in ETSI EN 303 645.

The UK Government has mandated three of these guidelines through legislation. Under “Product Security and Telecommunications Infrastructure Act 2022”, UK introduced “Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023[10] ”, which came into effect on April 29, 2024. The objective of this Regulation is to enhance the security of consumer connectable products from cyber threats. The PSTI Regulations 2023 is for consumer connectable products and focusses on following three aspects:

i) Unique Passwords

ii) Information on how to report security issues

iii) Information on minimum security update periods.

Australia government has come with Cyber Security Bill 2024 (Cyber Bill) which will implement legislative proposals stemming from Australian cyber security strategy 2023–2030 by establishing a new Cyber Security Act 2024. The IoT security by design Guidance for the manufacturers has been produced for manufacturers in order to help them implement the thirteen secure-by-design principles from Australia’s AS ETSI EN 303 645 standards on cyber security for consumer IoT devices[11].

The Cyber Security Agency of Singapore (CSA) has launched a voluntary cyber security labelling scheme[12] for consumer smart devices to improve IoT security based on ETSI EN 303 645.

[6] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[7] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

[8] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf

[9] https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

[10] https://www.gov.uk/government/publications/cyber-security-of-consumer-iot-manufacturer-survey/cyber-security-of-consumer-iot-manufacturer-survey

[11] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2425/25bd028

[12] https://www.iotaustralia.org.au/2020/10/09/iot-news-asia-pacific/singapore-launches-security-labelling-for- consumer-iot-devices/

Infocomm Media Development Authority (IMDA) Singapore has released a technical specification, in November 2020, for residential gateways (IMDA-TS-RG-SEC) having some mandatory provisions.

The USA has published a law in December 2020 “IoT Cybersecurity Improvement Act of 2020”. National Institute of Standards and Technology (NIST) has developed cybersecurity framework and privacy standards, guidelines, best practices and resources to meet the needs of U.S. industry, federal agencies and the broader public.

Various standards for NIST addressing the ETSI EN303 645 requirements are as below:

i. NISTIR 8259A and 8259B - Describes core baseline requirements for manufacturer specific and secure password - No universal default passwords from ETSI EN 303 645.

ii. NISTIR 8259B - Highlights the importance of vulnerability disclosure and management as recommended in ETSI EN 303 645 to Implement a vulnerability disclosure policy.

iii. NISTIR 8259B and NIST SP 800-218 – Covers secure software development practices (SSDF) and the ability for devices to receive updates, while ETSI EN 303 645 recommends to keep software updated, while NIST is talking about secure software update environment and security.

iv. NIST SP 800-213 and SP 800-213A - Provides guidance for federal agencies deploying IoT devices, including a catalog of technical requirements that can be mapped to NIST SP 800-53 (security and Privacy Controls for Information Systems and Organizations) security controls, while ETSI EN 303 645 only recommends Secure communication using encrypted communication of data both in transit and at rest.

v. NIST SP 800-213A - Contains a catalog of IoT device cybersecurity capabilities that can be used to document requirements and minimize unnecessary open ports while ETSI 303 645 recommends security by design principle to “Minimize exposed attack surfaces”.

The updated ETSI EN 303 645 (V3.1.3) provides a clearer scope for consumer IoT applicability, offers specific guidance for resource-constrained devices and strengthens transparency by requiring manufacturers to justify any unimplemented security provisions. It enhances vulnerability management expectations, refines data protection and privacy requirements for devices and associated cloud/mobile services and introduces lifecycle-based device-state diagrams to ensure secure operation from factory default to decommissioning. The revision also reinforces security-by-design principles, clarifies control of debug interfaces and adds more measurable guidance to support consistent implementation and audit readiness. Aligning with the current threat landscape and global regulations such as the EU Cyber Resilience Act, the standard promotes stronger supply chain transparency, lifecycle security and holistic compliance throughout the IoT ecosystem. This technical report has been revised reflecting the updates in ETSI EN 303 645 (V3.1.3) (2024-09).

This document intends to address the following stakeholders:

- IoT Device Manufacturers
- IoT Service Providers / System integrators
- Mobile Application Developers
- Retailers

2. Types of consumer IoT devices

This Code of Practice applies to consumer IoT products that are connected to the internet and / or home network and associated services. A non-exhaustive list of examples is as given below:

- Connected wearable healthcare devices
- Smart cameras, Smart speakers and Smart Televisions together with their Remote Controls
- Connected children's toys and baby monitors
- Connected safety-relevant products such as smoke detectors and door locks
- Connected home automation and alarm systems
- Connected appliances (e.g. washing machines, fridges)
- Smart home assistants
- IoT gateway for connecting consumer IoT devices

The security assurance level required by these applications varies across applications and associated services.

3. Guidelines for securing consumer IoT

3.1. No universal default passwords

All consumer IoT device's default passwords shall be unique per device and/or require user to choose a strong password that follows best practices, during device provisioning. The passwords shall not be resettable to any universal default value.

Many consumer IoT devices are being sold with universal default usernames and passwords (such as 'admin, admin') which are expected to be changed by the consumer. This has been the source of many security issues in IoT and the practice needs to be eliminated. Best practice on passwords and other authentication methods should be followed such as the use of the strongest possible password appropriate to the usage context of the device. Where applicable, associated services, such as web portals or mobile applications, should use Multi-Factor Authentication (MFA) such as use of a password plus OTP procedure and should not expose any unnecessary user information prior to authentication. Any password reset process should appropriately authenticate the user[13]. Authentication mechanisms shall also include protections against brute-force and credential-stuffing attacks, such as rate limiting, account lockout or increasing delay between attempts, while balancing against potential denial-of-service risks. Where feasible, machine-to-machine authentication shall not rely on human-memorable passwords, instead, pre-shared keys or certificates generated per device may be used, following cryptographic best practices, appropriate to the properties of the technology, operating environment, risk and usage.

Primarily applies to: *IoT Device Manufacturers*

3.2. Implement a means to manage reports of vulnerabilities

IoT device manufacturers, IoT service providers/System integrators and Mobile application developers should provide a dedicated publicly accessible point of contact as part of a Vulnerability Disclosure Policy (VDP) for security researchers and others to report security issues. The policy should specify acknowledgement timelines (e.g. "7 days", "quickly", etc.), status update procedures and resolution timelines to ensure transparency and accountability. Disclosed vulnerabilities should be acted on in a timely manner, with prioritization based on the criticality of the issue, the affected components and potential impact on users and the wider IoT ecosystem.

Implementing a responsible Coordinated Vulnerability Disclosure (CVD) program encourages and rewards the cyber security community for identifying and reporting vulnerabilities,

[13] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

thereby facilitating the responsible and coordinated disclosure and remediation of vulnerabilities.

Primarily applies to: *IoT Device Manufacturers, IoT service provider/System integrators and Mobile Application developers.*

3.3. Keep software updated

All Software components in consumer IoT devices that are not immutable for security reasons should be securely updateable. Updates shall be made in a timely manner and should not adversely impact the functioning of the device. An end-of-life policy shall be published for end-point devices which explicitly states the assured duration for which a device will receive software and security updates. For constrained devices that cannot physically be updated due to technical or resource limitations, the product should be isolatable and replaceable.

Developing and deploying security updates in a timely manner is one of the most important actions a manufacturer can take to protect its customers and the wider IoT ecosystem. It is good practice that all software is kept updated and well maintained.

The retailer and/or manufacturers should inform the consumer that an update is required and the need for each update should be made clear to consumers. An update should be easy to implement, preferably using non-intrusive approaches and automated mechanisms such as over the air (OTA) updates. It is advisable not to bundle security updates with more complex software updates, such as feature updates.

Consumers shall have the option to enable, disable or postpone automatic updates and to receive update notifications where supported.

Regular software updates should be provided after the sale of a device and pushed to devices for the lifecycle of the device. This period of software update support shall be made clear to a consumer when purchasing the product.

If a user interface is available, it should clearly display when a device has reached its end-of-support inform the user of the risk of security updates no longer being available and provide suggestions for mitigating this risk.

Primarily applies to: *IoT Device Manufacturers, IoT service provider/ System integrators and Mobile Application developers.*

3.4. Securely store sensitive security parameters

Consumer IoT devices may need to store security parameters such as cryptographic keys & credentials, certificates, device identity etc. which are critical for the secure operation of the device. Such information should be unique per device and shall be implemented in such a way that it resists tampering by means such as physical, electrical or software.

Credentials (e.g. user names, passwords) should not be hard-coded in the source code as they can be discovered via reverse engineering.

Secure storage mechanisms can be used to secure sensitive security parameters. Obfuscation methods used to obscure or encrypt security information without employing hardware-based protection can be trivially broken. Appropriate mechanisms include those provided by a Trusted Execution Environment (TEE), encrypted storage associated with the hardware, Secure Elements (SE) or Dedicated Security Components (DSC) and software-based cryptographic libraries where hardware support is unavailable.

Such a means ensure that hardware level protection is available for critical building blocks of the device with the ability to encrypt and protect/allocate critical sections of the memory for secure processing, ability to detect, validate and process software updates securely in the field.

Primarily applies to: *IoT Device Manufacturers, IoT service provider/ System integrators and Mobile Application developers.*

3.5. Communicate securely

Security-sensitive data, including any remote management and control, should be encrypted in transit using best practice cryptography, appropriate to the properties of the technology, operating environment, risk and usage of the device. All cryptographic keys and critical security parameters shall be generated, stored and managed securely throughout their lifecycle.

Depending on the requirement, a Trusted Execution Environment (TEE) may be enough. If needed this can be coupled with a Secure Element (SE) that stores the credentials, certificates or other sensitive security parameters. When configuring a secure connection, if an encryption protocol offers a negotiable selection of algorithms, remove/disable weaker/deprecated options so that they cannot be selected for use in a downgrade attack. Only strong, reviewed and up-to-date cryptographic algorithms and primitives should be used to ensure long-term security and crypto agility.

Primarily applies to: *IoT Device Manufacturers, IoT service provider/ System integrators and Mobile Application developers.*

3.6. Minimize exposed attack surfaces

Devices and services should operate on the 'principle of least privilege'. All unused functionality should be disabled to minimize the device's attack surface; hardware should not unnecessarily expose access (e.g. unrequired ports both network and logical should be closed).

Any web management interface should only be accessible to the local network unless the device needs to be managed remotely via the Internet and only after proper authentication); functionality should not be available if they are not used; and code should be minimized to the functionality necessary for devices and services to operate. Software should run with appropriate privileges, taking account of both security and functionality. To further reduce the number of vulnerabilities, follow a secure software development lifecycle (SSDLC), perform regular code reviews, conduct vulnerability assessments and penetration testing periodically.

The principle of least privilege is a foundation stone of good security engineering, applicable to IoT as much as in any other field of application.

Primarily applies to: *IoT Device Manufacturers, IoT service provider/ System integrators.*

3.7. Ensure software integrity

Software (including firmware) on Consumer IoT devices should be verified using secure boot mechanisms wherever applicable. If an unauthorized change is detected to the software, the consumer IoT device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.

During the boot sequence, wherever possible, check that only the expected hardware and peripherals are present and matches the current configuration parameters. Boot should fail gracefully, if it fails, it should never reveal an elevated permissions interface.

Software authenticity is important to avoid the usage of software provided by an unauthorized source. In addition, it is necessary to ensure that the software is loaded only on an authorized device to avoid authorized software to run on an unauthorized device.

Primarily applies to: *IoT Device manufacturers.*

3.8. Ensure that personal data is secure

In case the device collects or transmits personal data, such data should be securely stored. Also, the confidentiality of personal data transiting between a consumer IoT device and a service, especially associated services, should be protected, with best practice cryptography. When transmitting sensitive personal data e.g., streams from a security camera, special care should be taken by employing strongest cryptography available appropriate for the technology and usage.

Several principles in this document are related to protecting personal data, such as installing and securely configuring. The devices and associated services should have mechanisms (either through on device interface or through mobile applications) to allow users to view, manage and configure the usage of their personal data.

Primarily applies to: *IoT Device Manufacturers, IoT service provider/ System integrators, Mobile Application developer and Retailers.*

3.9. Make systems resilient to outages

Resilience should be built into Consumer IoT devices and services where required by their usage or by other relying systems. The possibility of outages of data networks and power should also be taken into account. As far as reasonably possible, IoT devices should remain operating and locally functional in the case of a loss of network, without compromising security or safety. They should recover cleanly in the case of restoration of a loss of power or connectivity.

Design IoT devices to continue basic functioning of it's intended purpose as much as possible if an associated IoT service becomes unavailable and disclose upfront to the consumer which features will cease working in this case. IoT service providers should also update data when network connection is restored. Devices should be able to return to a network in a sensible state and in an orderly fashion, rather than all attempt to reconnect at the same time.

Mechanisms should exist to verify that the device was not altered / tampered during the period of connectivity disruption.

Primarily applies to: *IoT Device Manufacturers, IoT service provider/ System integrators.*

3.10. Examine system telemetry data

If telemetry data is collected from Consumer IoT devices and services, such as usage and measurement data, it should be monitored for security anomalies.

Constant monitoring of the device is necessary to handle operational and security issue in time. Ensure all logged data comply with prevailing data protection regulations. All logs and telemetry data should be stored securely before it's sent to monitoring service. While communicating with the telemetry service, service should be authenticated and data should be encrypted. Access to telemetry data should be on need-to-know basis.

All remote access should be logged, including the date, time and source of access at a minimum. If the device runs out of storage, the oldest log may be over-written. For resource constrained devices the associated services or gateways may also be used to maintain these logs on behalf of IoT device.

Primarily applies to: *IoT Device Manufacturers, IoT service provider/ System integrators.*

3.11. Make it easy for users to delete user data

Devices and services should have mechanisms such that personal data can easily be removed when there is a transfer of ownership, when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear, step-by-step instructions on how to delete their personal data, including how to *reset the device to "factory default" and delete data stored on the device and in associated services including backend/cloud accounts and mobile applications.*

A 'factory reset' function must fully remove all user data/credentials stored on a device. Users should be provided with clear confirmation that personal data has been deleted and where possible erased from devices and associated services.

Primarily applies to: *IoT Device Manufacturers, IoT service provider/ System integrators, Mobile Application developers.*

3.12. Make installation and maintenance of devices easy

Installation and maintenance of Consumer IoT devices should employ minimal steps and should follow security best practice on usability. Consumers should also be provided with guidance on how to securely set up their device and also *to check whether the device is securely set up.*

Primarily applies to: *IoT Device Manufacturers, IoT service provider/ System integrators, Mobile Application developers.*

3.13. Validate input data

The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.

Data input at application layer to the device via user interfaces shall be validated to prevent unexpected data from causing system manipulations and failures. For example, manipulation of the integrated database via SQL injection over a user interface is mitigated via discarding invalid data input. Similarly, data input via network interfaces, including unauthenticated APIs and authentication-related APIs, shall also be validated to prevent system manipulations and failures.

Systems can be subverted by incorrectly formatted data or code transferred across different types of interfaces. Automated tools such as fuzzers are often employed by attackers or testers in order to exploit potential gaps and weaknesses that emerge as a result of not validating data. Examples include, but are not limited to, data that is:

i. Not of the expected type, for example - executable code rather than user inputted text.

ii. Out of range, for example - a temperature value which is beyond the limits of a sensor.

Primarily applies to: *IoT Device Manufacturers, IoT service provider/ System integrators, Mobile Application developers*.

4. Data protection provisions for consumer IoT

Many consumer IoT devices process personal data. It is expected that manufacturers provide features within consumer IoT devices that support the protection of such personal data. In addition, there exist country specific laws and regulations that relate to the protection of personal data in consumer IoT devices. For example, devices and services processing personal data in India shall do so in accordance with applicable data protection law, such as the Digital Personal Data Protection Rules, 2025 under Digital Personal Data Protection(DPDP) Act, 2023 of India.

The present document intends to help manufacturers of consumer IoT devices to provide features for the protection of personal data from a strictly technical perspective.

(i) The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers.

- EXAMPLE 1: This information could be provided by the manufacturer in their privacy policy.
- EXAMPLE 2: A smart health tracker app stores medical information (sleep profiles, pulse readings, blood pressure) and activity information (step counts, running speed and location), from paired smart fitness devices belonging to the user. This information is provided in a centralized service in order for users to track their training activities and change in fitness over time. This data is held by the manufacturer as the provider of the service, it is not made available to any third parties except as regulated by law. The data is retained until either the user deletes it, or the user's account is deactivated (after 90 days of inactivity or by user action).

To support the information to the user, the manufacturer has a process in place to inform the user with a notification if personal data was compromised as described by the vulnerability management process.

(ii) Where personal data is processed based on the basis of consumers' consent, this consent shall be obtained in a valid way. Obtaining consent "in a valid way" normally involves giving consumers a free, obvious and explicit opt-in choice of whether their personal data can be used for a specified purpose.

(iii) Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time. Consumers expect to be able to preserve their privacy by configuring IoT device and service functionality appropriately.

(iv) If telemetry data is collected from consumer IoT devices and services, the processing of personal data should be kept to the minimum necessary for the intended functionality.

Some telemetry cannot be easily collected without the risk of personal data collection (e.g. crash dumps). Where telemetry data could contain personal data, the use of techniques such as data anonymization can reduce the risk of personal data compromise if the processing does not require the personal data.

(v) If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom and for what purposes.

(vi) Data stored and processed on a consumer IoT device, or made available to an associated service by the consumer IoT device, for purposes identified in provision 4(i) shall be limited to that which is necessary for the purpose for which it is being collected or processed and deleted once no longer necessary for any of the purposes identified.

- EXAMPLE: A smart Television stores user viewing history and user program ratings in order to suggest programs of interest to the user and save them for later viewing. The viewing history is stored on the device for up to 1 year, after which it is deemed no longer relevant for this purpose and deleted. User ratings are retained indefinitely on the device but can be deleted by the user. The programs automatically saved are replaced after 28 days by default, with the user able to configure their own retention policy, including indefinite retention. The viewing history is also made available to the operator by the device for the purpose of improving suggestions only if the user has consented to this collection.

(vii) When the purpose of data collection from consumer IoT devices or processing on the consumer IoT device, is solely to compute an aggregate result, the data collected should be the minimum required to compute the aggregate, the aggregation should happen as early as possible and the retention of both collected data and the resulting aggregate should be minimized.

- EXAMPLE: Federated learning and analytics enable multiple devices to collaboratively train machine learning models or compute data queries, under the coordination of a central server. Each device's raw data is stored locally and not exchanged or transferred; instead, focused updates intended for immediate aggregation are uploaded to achieve the learning objective.

(viii) Data anonymization technologies should be used to protect privacy during data collection, processing and storage.

- EXAMPLE: IoT devices may locally add protective noise to data before sending it to the centralized aggregators or processing coordinators.

Definitions

IoT Device manufacturers: Entities that create an assembled final consumer IoT product, which is likely to contain the products and components of many other suppliers.

Mobile Application Developers: Entities that develop and provide applications that run on devices. These are often offered as a way of interacting with devices as part of an IoT solution.

IoT Service Providers / System integrators: Companies that provide services such as networks, cloud storage and data transfer which are packaged as part of IoT solutions. Internet-connected devices may be offered as part of the service.

Consumers: Consumers may take many forms. Governments, businesses and individuals may all be consumers of IoT devices. This Code of Practice particularly focuses on consumer grade, internet-connected devices and associated applications (e.g. wearable devices, and home appliances such as “smart” televisions and refrigerators).

Retailers: The sellers of internet-connected products and associated services to consumers.

IoT Gateway: A unit in the Internet of things which interconnects the devices with the communication networks. It performs the necessary translation between the protocols used in the communication networks and those used by devices.

MTCTE (Mandatory testing and Certification of Telecom Equipment): Department of Telecommunications, Ministry of Communications has notified “Indian Telegraph (Amendment) Rules” in Gazette of India vide G.S.R. 1131(E) PART XI" on 5th September 2017 which prescribes for Mandatory Testing and Certification of Telecommunication Equipment. Any telegraph which is used or capable of being used with any telegraph established, maintained or worked under the license granted by the Central Government in accordance with the provisions of section 8(2) of Telecommunications (Framework to Notify Standards, Conformity Assessment and Certification) Rules, 2025, shall have to undergo prior mandatory testing and certification in respect of parameters as determined by the telegraph authority from time to time.

IoT: ITU-T in its Recommendation ITU-T Y.2060 (06/2012) [14]has defined Internet of Things (IoT), as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

[14] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

Bibliography

1. ETSI EN 303 645 V3.1.3 (2024-09) CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

2. ETSI TS 103 645 V2.1.2 (2020-06) CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf

3. ETSI EN 303 645 V2.1.1 (2020-06) CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

4. ETSI TS 103 701 V2.1.1 (2025-05) Cyber Security (CYBER); Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements: https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/02.01.01_60/ts_103701v020101p.pdf

5. National Digital Communication Policy (NDCP) 2018: https://dot.gov.in/sites/default/files/Final%20NDCP-2018_0.pdf

6. Markets and Markets report on IoT security market: https://www.marketsandmarkets.com/PressReleases/iot-security.asp

7. IoT Security Foundation (IoTSF) annual report on vulnerability disclosure, February 2021: https://iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf

8. IoT Vulnerability Management: Adhering to the New Laws: https://www.electronicdesign.com/technologies/iot/article/21132742/iot-vulnerability-management- adhering-to-the-new-laws

9. UK DCMS Code of practice on Consumer IoT security: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf.

10. Code of Practice - Securing Internet of Things for Consumers, Government of Australia: https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

11. Cyber security labelling scheme for consumer smart devices Cyber Security Agency of Singapore (CSA) -https://www.iotaustralia.org.au/2020/10/09/iot-news-asia-pacific/singapore-launches-security-labelling-for-consumer-iot-devices/

12. Overview of Internet of Things ITU-T Y.2060 (06/2012): https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060.

13. Cyber security of consumer IoT - manufacturer survey: https://www.gov.uk/government/publications/cyber-security-of-consumer-iot-manufacturer-survey/cyber-security-of-consumer-iot-manufacturer-survey

14. Cyber Security Bill 2024 [and] Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2425/25bd028

15. State of IoT 2025:https://iot-analytics.com/number-connected-iot-devices/

List of contributors

Working Group - "Security by design Principles in M2M device manufacturing and National Trust Center for certification of M2M devices and applications".

A. Approving Authority:

Name	Designation	Organization	E-mail Address	Version
Mr. Syed Tausif Abbas	Sr. DDG & Head TEC	Telecommunication Engineering Centre (TEC)	srddg.tec@gov.in	Release 2 (Nov 2025)
Ms. Deepa Tyagi	Sr. DDG & Head TEC	Telecommunication Engineering Centre (TEC)	srddg.tec@gov.in	Release 1 (Aug 2021)

B. Drafting committee for Release 2:

Designation	Name	Organization	e-mail address
Chairman	Mr. R. S. Singh	TEC	ddgiot.tec@gov.in
Vice Chairman	Mr. Dinesh Chand Sharma	SESEI (ETSI)	dinesh.chand.sharma@sesei.eu
Rapporteur	Ms. Namrata Singh	TEC	namrata.singh51@gov.in
Co-Rapporteur	Mr. Pranav Singh	IDEMIA	pranav.singh2@idemia.com
Convener	Mr. Raghav Purwar	TEC	rpurwar.96@gov.in

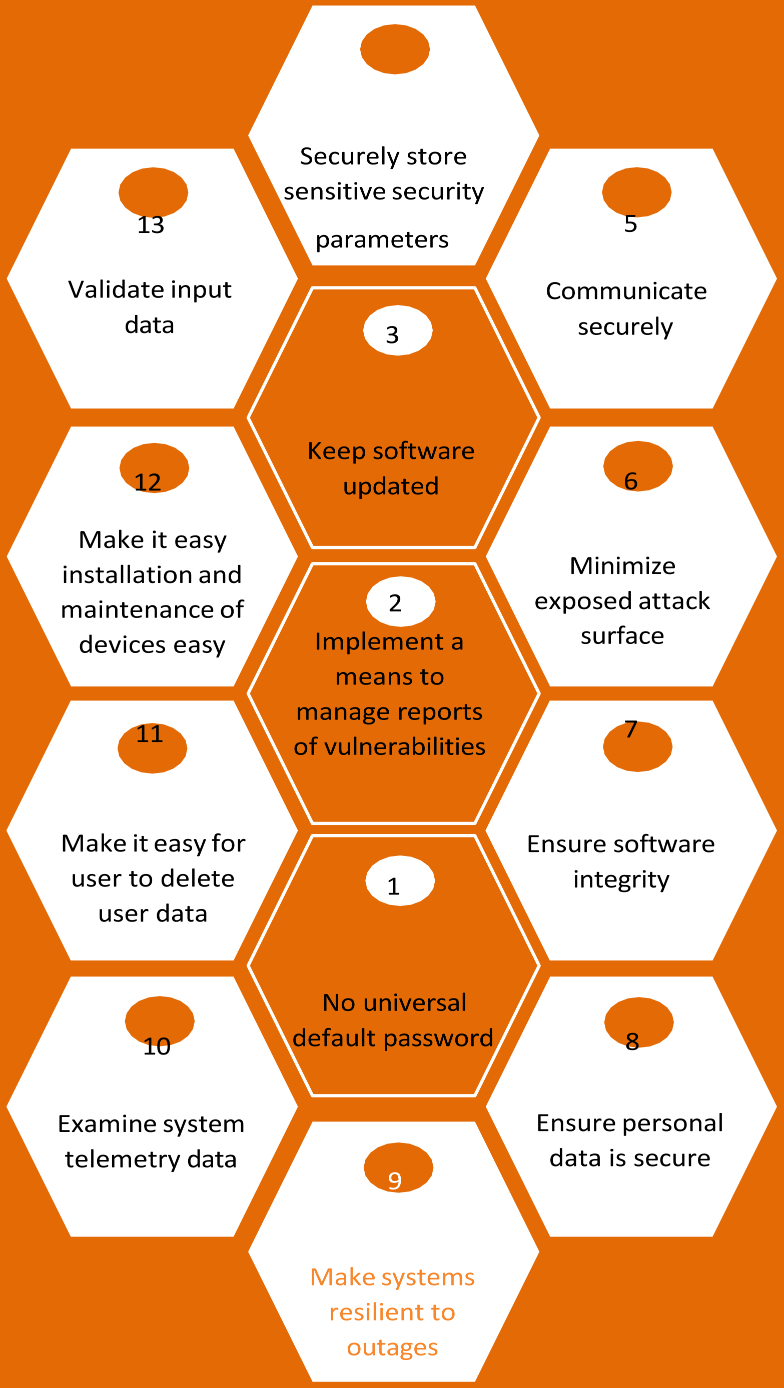
C. Working Group Chairs for Release 1:

Designation	Name	Organization	e-mail address
Chairman	Sushil Kumar	TEC	ddgsd.tec@gov.in
Vice Chairman	Aurindam Bhattacharya	C-DOT	aurindam@cdot.in
Rapporteur	Prashant Pandey	STMicroelectronics	prashant-mpa.pandey@st.com
Co- Rapporteur	Shekhar Singh	TEC	ad.iot-tec@gov.in

D. Contributors:

S. No.	Name	Organization	e-mail address
1.	Sushil Kumar	TEC	ddgsd.tec@gov.in
2.	Aurindam Bhattacharya	C-DOT	aurindam@cdot.in
3.	Prashant Pandey	STMicroelectronics	prashant-mpa.pandey@st.com
4.	Ms. Ashima	TEC	dirsd1.tec@gov.in

5.	Shekhar Singh	TEC	ad.iot-tec@gov.in
6.	Sharad Arora	Sensorise Digital Services Pvt. Ltd.	sharad.arora@sensorise.net
7.	Amit Rao	Trusted Objects	a.rao@trusted-objects.com
8.	Arvind Tiwary	IoT Forum	arvind_t@sangennovate.com
9.	Dinesh Sharma	SESEI (ETSI)	dinesh.chand.sharma@sesei.eu
10.	Ms. Sonia Compans	ETSI	sonia.compans@etsi.org
11.	Aseem Jakhar	Payatu	aseem@payatu.com
12.	Narang kishore	Narnix Technolabs Pvt. Ltd.	kishor@narnix.com
13.	Vijay Madan	TSDSI	vijay.madan@tsdsi.in
14.	Kanishka Gaur	India Future Foundation	kanishk@indiafuturefoundation.com
15.	Rohit Singh	UL India Pvt. Ltd.	rohit.Singh@ul.com
16.	Arthur van der Wees	Arthurs Legal, Strategies & Systems	vanderwees@arthurslegal.com
17.	Maxime Hernandez	TUV SUD	maxime.hernandez@tuvsud.com
18.	Prashant Ghadi	Novateur Electrical & Digital Systems Pvt. Ltd. (Legrand)	prashant.ghadi@legrand.co.in
19.	Rajeev Kumar	Intern, TEC	rajeevkrsinghania@gmail.com
20.	Ms. Namrata Singh	TEC	namrata.singh51@gov.in



Securely store sensitive security parameters

13 Validate input data

5 Communicate securely

3 Keep software updated

12 Make it easy installation and maintenance of devices easy

6 Minimize exposed attack surface

2 Implement a means to manage reports of vulnerabilities

11 Make it easy for user to delete user data

7 Ensure software integrity

1 No universal default password

10 Examine system telemetry data

8 Ensure personal data is secure

9 Make systems resilient to outages

ISO 9001 :2015

TELECOMMUNICATION ENGINEERING CENTER DEPARTMENT OF TELECOMMUNICATIONS MINISTRY OF COMMUNICATIONS GOVERNMENT OF INDIA