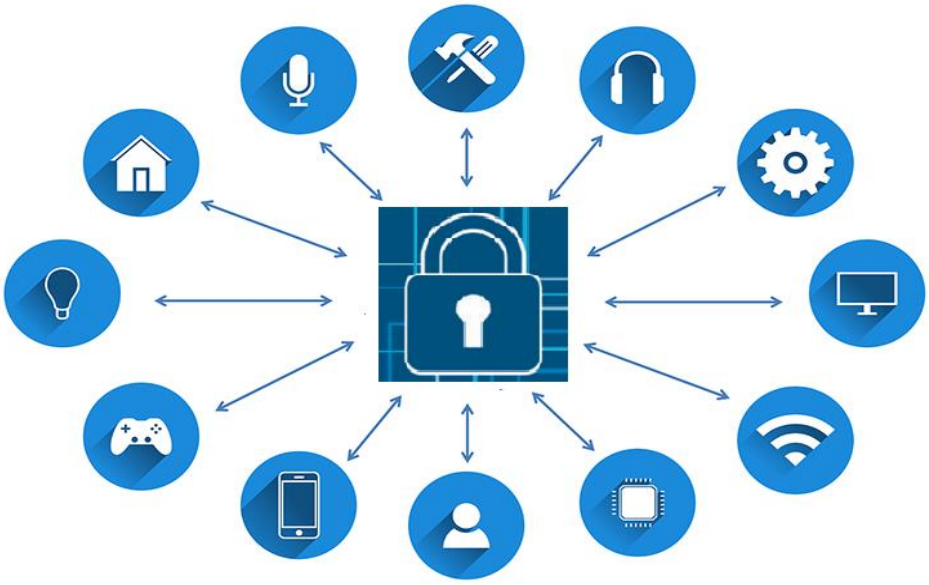
Code of Practice

for

Securing

Consumer Internet of Things (IoT)

TEC 31318:2021



ISO 9001 :2015

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

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)

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:**m2mreports.tec@gov.in**

Disclaimer

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.

There may be 26.4 billion IoT devices in service globally by 2026. Out of this approximately 20% will be on cellular technologies[1].

It has been projected that there would be around 11.4 billion consumer IoT devices and 13.3 billion enterprise IoT devices globally by 2025[2] i.e. consumer IoT devices would account for nearly 45% of all the IoT devices.

As per the National Digital Communication Policy (NDCP) 2018[3] released by Department of Telecommunications (DoT), an eco-system is to be created for 5 billion connected devices by 2022. Therefore, it is expected that around 60% of 5 billion i.e. 3 billion connected devices may exist in India by 2022.

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 Indian Telegraph (Amendment) Rules, 2017.

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] https://www.ericsson.com/4a03c2/assets/local/mobility-report/documents/2021/june-2021-ericsson-mobility-report.pdf
[2] https://enterpriseiotinsights.com/20200305/5g/iot-connections-reach-almost-25-billion-globally-2025-gsma
[3] https://dot.gov.in/sites/default/files/Final%20NDCP-2018_0.pdf

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.

This document on *Code of Practice for consumer IoT security* provides baseline requirements as a basis for the implementation of the above referred recommendations. Substantial input has been taken from the ETSI TS 103 645 and ETSI EN 303 645. It is expected that the ETSI TS 103 701 (Cybersecurity assessment for consumer IoT products) will help in the implementation of the provisions available in these guidelines.

TEC has been working on Security by design principles and National Trust Center (NTC) for IoT in a multi-stakeholders Working Group and the draft document is under development taking into account the standards & best practices being used across the globe. This code of practice is part of the draft document under discussion and a step in the direction of implementing the National Trust Center.

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, organisations, 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 8.2 billion in 2018 to USD 35.2 billion by 2023, at a CAGR of 33.7 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.

IoT Security Foundation (IoTSF) in its annual report on vulnerability disclosure[5] (February 2021) has mentioned an improvement in vulnerability disclosure by the manufacturers from 9.7% in 2018 to 18.9% in 2020. Companies under survey were from North America, Asia and Europe. This is of great concern as vulnerability disclosure is widely considered to be a baseline requirement due to its fundamental importance towards operational IoT

[4] https://www.marketsandmarkets.com/PressReleases/iot-security.asp
[5] https://www.iotsecurityfoundation.org/best-practice-guidelines/

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.

ETSI has released ETSI TS 103 645 (V 2.1.2)[6] in June 2020 on Cyber *Security for Consumer Internet of Things: Baseline Requirements*. It is having 13 basic principles. ETSI TS 103 645 has been adopted by the European Union (EU) as ETSI EN 303 645. ETSI TC CYBER is taking forward TS 103 701, which will set out test scenarios for assessing products against EN 303 645.

UK and Australia have released Code of practice for consumer IoT security in 2018[7] and 2020[8] respectively, and are having the similar guidelines as available in ETSI TS 103 645.

The Cyber Security Agency of Singapore (CSA) has launched a voluntary cyber security labelling scheme for consumer smart devices to improve IoT security based on ETSI EN 303 645[9]. 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", mandating National Institute of Standards and Technology (NIST) to develop the standard and guidelines on the use and management of IoT.

The guidelines mentioned in this Code of Practice are aligned with the Cyber Security for Consumer Internet of Things: Baseline Requirements mentioned in ETSI EN 303 645.

This document intends to address the following stakeholders:

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

[6] https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf
[7] 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
[8] https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf
[9] https://www.iotaustralia.org.au/2020/10/09/iot-news-asia-pacific/singapore-launches-security-labelling-for-consumer-iot-devices/

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, TVs and speakers
- 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 the consumer IoT devices

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

3. Guidelines for securing consumer IoT

3.1. No universal default passwords

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

Many 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. Associated web services should use Multi-Factor Authentication, and should not expose any unnecessary user information prior to authentication. Any password reset process should appropriately authenticate the user[10].

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 public point of contact as part of a vulnerability disclosure policy for security researchers and others to report security issues. Disclosed vulnerabilities should be acted on in a timely manner.

Implementing a responsible vulnerability disclosure program encourages and rewards the cyber security community for identifying and reporting vulnerabilities, thereby facilitating the responsible and coordinated disclosure and remediation of vulnerabilities.

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

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

3.3. Keep software updated

Software components in IoT devices should be securely updateable. Updates shall be timely 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 updates. For constrained devices that cannot physically be updated, 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 like over the air (OTA) updates.

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-life, 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 providers / System integrators and Mobile Application developers.*

3.4. Securely store sensitive security parameters

IoT devices may need to store security parameters such as 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 processing capabilities of software wherever possible.
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 providers / System integrators and Mobile Application developers.*

3.5. Communicate securely

Security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage of the device. All keys should be managed securely.

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. When configuring a secure connection, if an encryption protocol offers a negotiable selection of algorithms, remove weaker options so that they cannot be selected for use in a downgrade attack.

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

3.6. Minimize exposed attack surfaces

Devices and services should operate on the 'principle of least privilege'. Unused functionality should be disabled; 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, use a secure software development process and perform 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 providers / System integrators.*

3.7. Ensure software integrity

Software (including firmware) on IoT devices should be verified using secure boot mechanisms wherever applicable. If an unauthorized change is detected, the 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 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 and configure the usage of their personal data.

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

3.9. Make systems resilient to outages

Resilience should be built into 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 providers / System integrators.*

3.10. Examine system telemetry data

If telemetry data is collected from 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 providers / 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 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.

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

3.12. Make installation and maintenance of devices easy

Installation and maintenance of 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 providers / 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.

Systems can be subverted by incorrectly formatted data or code transferred across different interface. Automated tools are often employed by attackers 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 providers / 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 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 Personal Data Protection bill, 2018 of India. The present document intends to help manufacturers of consumer IoT devices 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.

(ii) Where personal data is processed based on 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.

(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.

5. 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 4 of the Indian Telegraph Act, 1885 (hereinafter referred to as the said Act), 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)[11] has defined Internet of Things (IoT), as a global infrastructure for the information society, enabling advanced services by

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

interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

Bibliography

1. ETSI TS 103 645 V2.1.2 (2020-06) - https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf

2. ETSI EN 303 645 V2.1.1 (2020-06) https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

3. Ericsson Mobility Report, June 2021 - https://www.ericsson.com/4a03c2/assets/local/mobility-report/documents/2021/june-2021-ericsson-mobility-report.pdf

4. GSMA - https://enterpriseiotinsights.com/20200305/5g/iot-connections-reach-almost-25-billion-globally-2025-gsma

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://www.iotsecurityfoundation.org/best-practice-guidelines/

8. News on IoT vulnerability management- 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.

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. Joint Working Group (JWG) Chairman:

Name	Designation	Organisation	E-mail Address
Ms. Deepa Tyagi	Sr. DDG & Head TEC	Telecommunication Engineering Centre (TEC)	srddg.tec@gov.in

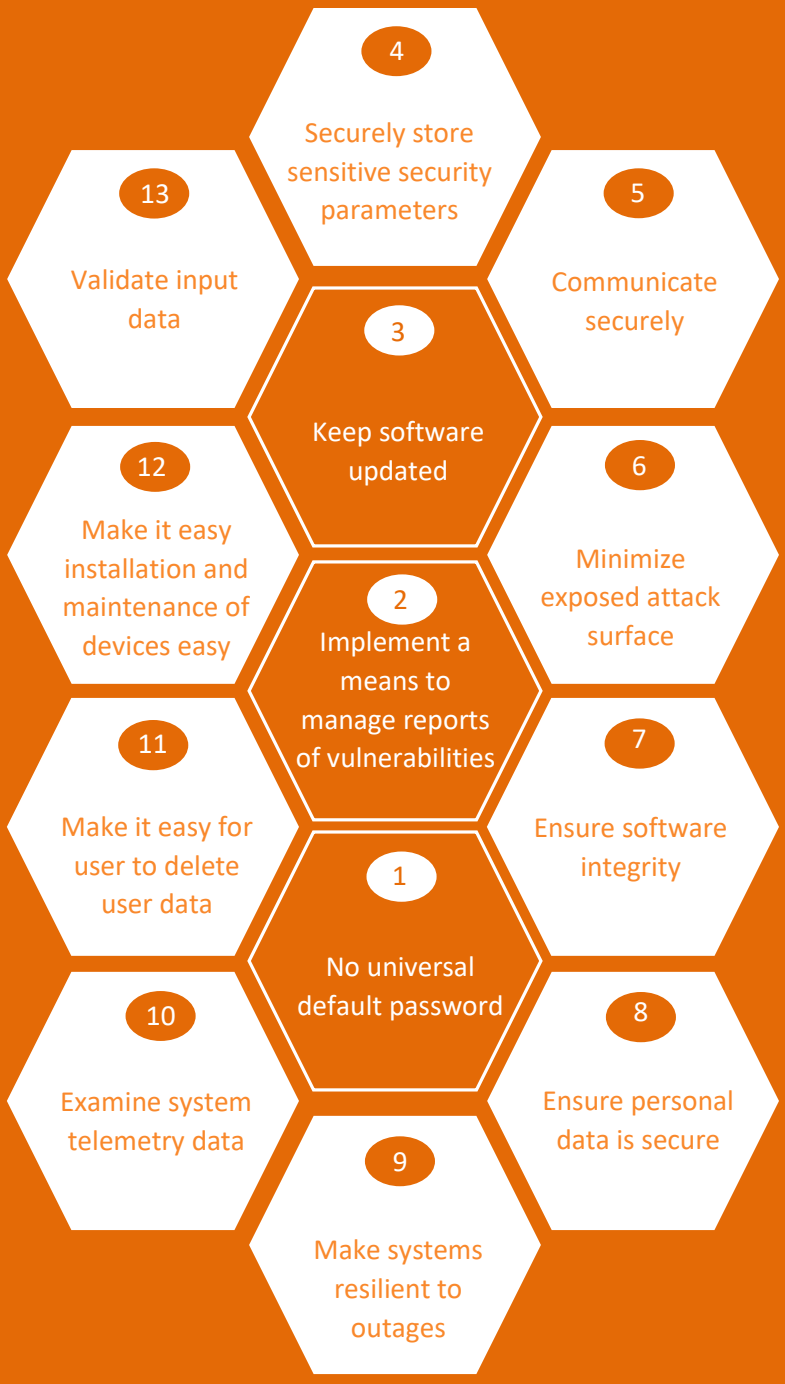
B. Working Group Chairs:

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/ Convenor	Shekhar Singh	TEC	ad.iot-tec@gov.in

C. 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

S. No.	Name	Organization	e-mail address
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.	Hernandez, Maxime	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



ISO 9001 :2015

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