IOT SECURITY STANDARD

VERSION 1.0

حكومة دبي
GOVERNMENT OF DUBAI

DUBAI ELECTRONIC SECURITY CENTER
مركز دبي للأمن الإلكتروني

IOT SECURITY STANDARD

VERSION 1.0

TABLE OF CONTENTS

INTRODUCTION

The IoT Security Standard produced by Dubai Electronic Security Center (DESC) sets out mandatory and recommended controls for the security of Internet of Things (IoT). Compliance with this standard is mandatory for all Dubai government and semi government entities.

There are no internationally recognized standards for IoT security, yet different interest groups have done some work relevant to this area. The work that was considered when developing this standard includes:

- TR 47: 2016 IoT reference architecture for Smart Nation – Singapore Standard Council
- Connected Consumer Products Release 1.0 – Best Practice Guidelines – IoT Security Foundation
- OWASP – IoT Security Guidance
- OWASP – IoT Security Foundation
- OEASP – Strategic principles for the security of IoT
- Oil and Natural Gas – Cyber security Capability Maturity Model (ONG-C2M2)

Additionally, the following documents are indispensable for the use of this standard:

- ISO/IEC 27001:2013 – Information Technology – Information security management system – Requirements
- Information Security Regulation ISR V2.0 – DESC

IoT comprises a large ecosystem of interconnected services and devices, such as sensors, actuators, gateways, smart home objects, car components, industrial and health components. These technologies collect, exchange and process information, which needs protection.

Many security considerations regarding IoT are not necessarily new; they are inherited from the use of networking technologies and other best information security practices. However, the characteristics of some IoT implementations present new security challenges, threats and risks that are manifold and evolving rapidly.

The protection of IoT deployments depends on the protection of all layers involved (please refer to Section 1 of this standard). Addressing these challenges and ensuring security in IoT products and services is a fundamental priority for the maintenance of cyber security in Dubai.

SCOPE

This Standard provides mandatory and rec ommended controls for the security of Internet of Things (IoT) devices in the city of Dubai. The standard is applicable to all organizations using IoT devices, to ensure that the devices they are using fulfills appropriate security requirements. It includes controls for both Information Technology (IT) and Operational Technology (OT). This standard is relevant for all government and semi government organizations in Dubai.

1 STRUCTURE OF THIS STANDARD

This clause describes the structure of this standard, as illustrated in the picture below:

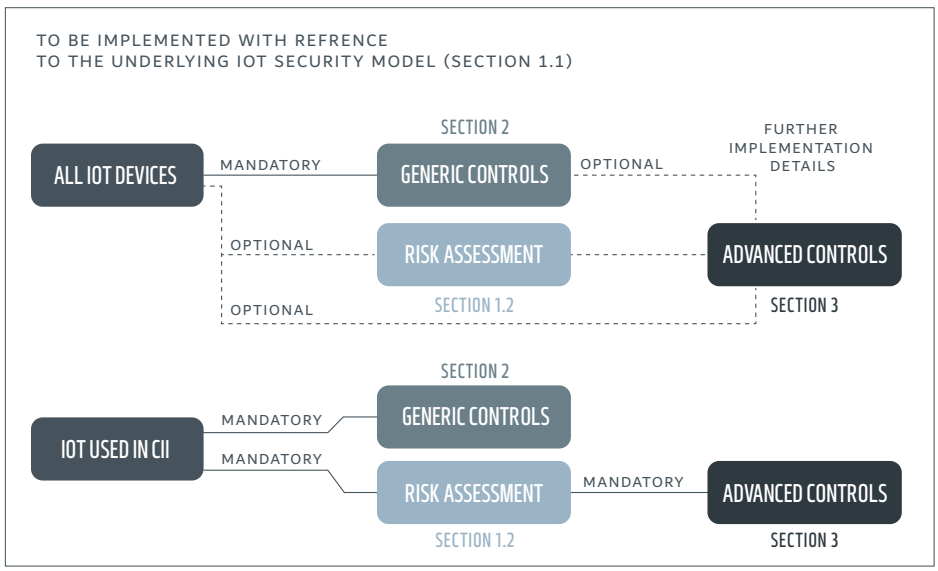


Figure 1 Structure of the IoT security standard

The clauses of this standard are:

- UNDERLYING IOT SECURITY MODEL (Section 1.1)

Currently, there is no international standard for the security of IoT devices, and there are varying approaches taken by different nations and interest groups. It is therefore important to describe the model applied for the security of IoT devices in this standard. Section 1.1 outlines this model, describing a layered approach, as well as the important concept of risk assessment.

- GENERIC MANDATORY IOT SECURITY CONTROLS (Section 2)

Due to the diversity of IoT devices, it is not possible to describe security controls that apply to all devices, there will always be exceptions. In cases where the device layer is not capable or suitable to implement certain controls, the other layers (application and communication) need to be used to put the control in place. Although the generic controls are mandatory, the implementation details for some of them should be based on the risk assessment.

- ADVANCED IOT SECURITY CONTROLS (Section 3)

These advanced controls are to be considered for implementation based on the results of the risk assessment (as outlined in Section 1.2). Similar to the case of the generic controls, the advanced controls can be applied on the device, communication, or application layer.

Additionally, due to the diversity of IoT devices, the applicable security controls are dependent on the criticallity of the device and whether it is implmented in critical information infrastructure (CII) services.

1.1 Underlying IoT Security Model

The basis of the security model applied in this standard is derived from the international standard ISO/IEC 27001 and the local Information Security Regulation (ISR). These standards provide a security framework in which an IoT device can operate securely.

In addition, a layer-based approach, as shown in figure 2, is used to describe the key aspects of information security for an IoT device. The proposed layers are:

- Organizational Information Security Framework (ISO/IEC 27001 and/or ISR) – this layer covers all information security controls contained in ISO/IEC 27001 and/or ISR, such as risk assessment, asset management, access control, and incident management.
- Application Layer – this layer addresses all information security controls that can be provided by an application, such as user identification and authentication, application access control or integrity checks.
- Communication Layer - this layer addresses all information security controls that can be implemented through the network, such as network segregation, access control, logging and monitoring.
- Device Layer – this layer is concerned with the information security controls that can be implemented on the IoT device itself. As IoT devices are very diverse such controls can range from simple features, such as password protection to more complex features, such as encryption.

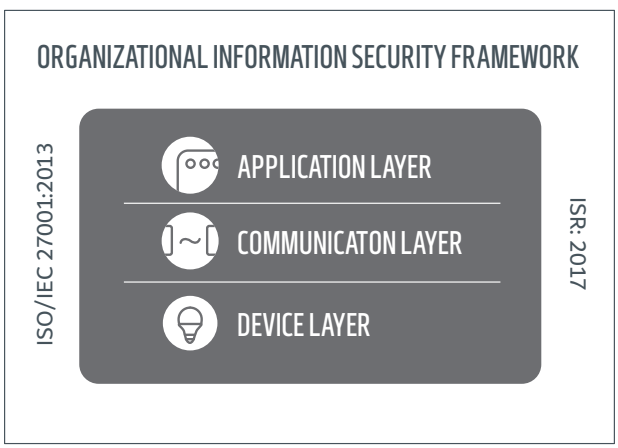


Figure 2 IoT security model

Ensuring that an IoT device operates in a secure environment, provided by the organizational information security framework, minimizes the security issues that might arise from improper implementation or operation of security controls on the device, commu-

nication, or application layer. For example, if there are breaches on the lower levels, the incident management process provided by the organizational security framework will help to manage such situations.

1.2 Risk Assessment

Not all IoT devices have the same requirements for security, how much a device needs to be secured is a direct result of how and where the IoT device is used. For example, a device that is only monitoring server room temperature, and is backed up by two other devices, often has no need for advanced security controls. However, an IoT device used in a critical function like a communication device implemented in an autonomous vehicle, does require the application and configuration of advanced security features. Therefore, the advanced security controls that are applied to an IoT device should be determined through an assessment of the risks (logical or physical) a device might be exposed to. Additionally, the overall impact should the security of a device be compromised is also to be considered in the risk assessment.

Organizations should carry out a risk assessment to determine appropriate security controls for their IoT devices. This risk assessment is mandatory in cases where the IoT devices are supporting a CII function. As most CII organizations already apply ISR or ISO/IEC 27001, it is efficient to combine the risk assessment for the security of IoT devices with the information security risk assessment that is carried out for ISR or ISO/IEC 27001.

DUBAI ELECTRONIC SECURITY CENTER
مركز دبي للأمن الإلكتروني

2 GENERIC MANDATORY SECURITY CONTROLS

This section describes generic mandatory security arrangements that organizations shall follow when procuring and/or developing secure IoT products. The controls listed below form the basic set that each organization using IoT platforms/devices shall comply with. The detailed implementation of these high level mandatory controls should take into account the results of the risk assessment mentioned in Section 1.2 above, as well as the device's relation to CII.

Due to the diversity of IoT devices, the following controls can either be addressed on the IoT device itself, the application layer, or the communication layer. Compliance with international and regional legislation is ensured by the organizational security framework. If a third-party service is used, the organization should ensure that the third party applies the security controls listed below.

To support the ease of implementation of these controls, a link to corresponding controls in ISR has been included in Annex B. The mandatory controls for IoT devices, or systems containing IoT devices, can be applied either by the manufacturers and developers of the IoT devices or by the organizations deploying them, depending on the nature of the device. The generic mandatory controls are:

2.2.1 Ensure that proven security solutions recognized by the security community are applied to the IoT platform.

2.2.2 Ensure that all security-relevant activities (for example access to and/or modification of information) can be logged and monitored.

2.2.3 Ensure that security events and incidents can be detected and recorded for necessary corrective action.

2.2.4 Provide regularly updated disclosure of vulnerabilities.

2.2.5 Ensure that a secure booting process is in place for the IoT platform/device.

2.2.6 Ensure that malicious code cannot be injected into the information system to which the IoT device belongs (for example by code signing[1]).

2.2.7 Disclose information regarding the replacement, removal or addition of any component in the supply chain of an IoT device that is currently approved and provided in the market.

2.2.8 Readdress the security guidelines and risk assessments whenever any update is introduced to the existing IoT platform.

1 Code signing is the method of using a certificate-based digital signature to sign executables and scripts in order to verify the author's identity and ensure that the code has not been changed or corrupted since it was signed by the author.

2.2.9 Ensure that compromised or infected devices are identified and revoked in order to avoid having other functionalities of the system affected.

2.2.10 Inform users/buyers of IoT devices about the expected life period of a given IoT device as well as the risks/issues associated with using it beyond its usability date. Any repair should be conducted in a timely manner.

2.2.11 Clearly indicate on the IoT device itself, and/or its packaging, its dependencies on any other systems/devices.

2.2.12 Provide a secure and reliable method to transfer the ownership of an IoT device from one person to another.

2.2.13 Ensure that the information on the platform/device can completely be wiped or destroyed whenever needed, as part of information protection, and a method of secure destruction.

2.2.14 Ensure that any sensitive personally identifiable information can be anonymized or removed where necessary.

2.2.15 Ensure that the defined security measures are implemented/active, even when an IoT device is facing some technical/operational disruption.

2.2.16 Access to IoT devices should be controlled, based on least privilege access, need-to-know basis principles, and the results of the risk assessment.

2.2.17 Ensure that an access control system is in place for IoT devices, to detect and report invalid login attempts.

2.2.18 Ensure that security measures, such as firewalls and secure authentication methods, are implemented to control access to the IoT device, based on risk assessment results.

2.2.19 Ensure that IoT devices are running on a recent operating system, in line with the organization's policy for operating systems updates.

2.2.20 Ensure that only up-to-date software is used in conjunction with IoT devices; updates of the software should be possible, when necessary. Allow only authorized sources to provide such updates.

2.2.21 Ensure that the information system the IoT device belongs to supports selective connectivity for the administrator to be able to disconnect certain ports when required.

2.2.22 Ensure that sector-specific security and privacy standards are adhered to, such as ISO/IEC 27799 for the health sector.

2.2.23 Ensure that the information system in which IoT devices are used in is equipped with layered defenses against cyber security threats including user level tools.

2.2.24 Ensure that all communication and data storage related to IoT devices are encrypted, where necessary.

2.2.25 Put appropriate network segregation in place (based on risk assessment results).

2.2.26 Ensure that all connections are removed from any IoT device that has been removed from the network.

DUBAI ELECTRONIC SECURITY CENTER
مركز دبي للأمن الإلكتروني

3 ADVANCED IOT SECURITY CONTROLS

The following advanced IoT security controls should be considered and applied based on the results of the risk assessment. These controls can be applied either by the manufacturers and developers of the IoT devices or by the organizations deploying them, depending on the nature of the device. The controls can also be applied on any of the aforementioned layers; device, communication or application layer.

3.1 Secure Web Interface

3.1.1 Ensure that the IoT platform supports a web interface that disallows weak passwords.

3.1.2 Ensure that the IoT platform web interface in the product has an account lockout mechanism.

3.1.3 Ensure that the IoT platform web interface in the product has been tested for XSS, SQLi and CSRF vulnerabilities and OWASP Top 10 security vulnerabilities.

3.1.4 Ensure that the IoT platform has the ability to use HTTPS to protect the transmitted information.

3.1.5 Ensure that the IoT platform supports the feature to disable HTTP services or redirect to HTTPS.

3.1.6 Ensure that the IoT platform administrators change the default username and password.

3.1.7 Ensure that the IoT platform interface uses Secure Coding (for example prevention on the use of old Java code, vulnerable J-Query plugins etc).

3.1.8 Ensure the following, If the IoT platform exposes API to the Internet:

- That it should support SSL.
- That the API mutual authentication is built-in to the protocol feature set where authentication tokens are passed during every request and response between the IoT platform and IoT devices.
- That the API does not expose more services than the authorization level of the tokens and is not subject to any manipulation to retrieve content that is not authorized.

3.1.9 Ensure that the IoT platform supports Software Defined Perimeter Protocol 2.0 as a means to ensure that only authenticated and authorized IoT devices/sensors can connect into the IoT platform.

3.2 Authentication/Authorization

3.2.1 Ensure that the IoT platform uses strong password authentication and that profiles can be created to ensure password policy is conformed to:

- Brute-force attack mitigation
- Disabling the use of default or hardcoded passwords
- Enforcing password best-practices
- Disallowing display of user credentials on login interfaces
- Enforcing thresholds and incremental delays for invalid password attempts

3.2.2 Ensure that user roles are properly segregated in multi-user environments and the Role Based Access Control (RBAC) feature set is available within the IoT platform. Further ensure that RBAC is functional as a multi-tenant platform where entity IoT administrators are only able to view their respective IoT sensors and health statistics.

3.2.3 Ensure that the IoT platform performs object tagging to guarantee roles assigned to the object tags are then only viewed.

3.2.4 Ensure that the IoT platform supports two-factor authentication using OTP (SMS) or backend integrated with Radius Server. Ensure that the IoT platform supports two-factor authentication for all admin level access to the system (Web Interface, SSH etc).

3.2.5 Ensure that the IoT platform supports secure password recovery mechanisms only during secure platform boot.

3.2.6 Ensure that administrators of the IoT platform have the option to force password expiration after a specific period that is conformant to the password policy.

3.2.7 Ensure that administrators of the IoT platform change the default username and password.

3.2.8 Ensure that the platform has the capability to fine tune permissions based on space and time, in case IoT devices are relocated. Ensure that the platform supports location aware permissions utilizing any number of the sensors on an edge device and also supports a permissions model that can change based on rules of time.

3.2.9 Ensure that the IoT devices/sensors and IoT platform support PKI and Certificate Based Authentication Services. Ensure that X.509 certificates are used for application security (Web Services) and that the platform has native features to integrate with DESC PKI solution. Ensure also that the integration fully supports the secure automated certificate provisioning, revocation, and renewal processes.

3.2.10 Ensure that the IoT platform has the ability to create a direct, authenticated, policy-enforced binding between devices and the PKI credentials that are assigned to them to prevent the use of certificates and keys from unauthorized devices.

3.2.11 Ensure that the IoT platform supports IoT device provisioning that is based on dynamic device key generation process whilst providing strong device registration controls to ensure IoT device onboarding process has met the requirements of secure authentication and authorization.

3.2.12 Ensure that the IoT platform supports 'phone home' features from the IoT devices to ensure provisioning of remote devices at scale with authentication and authorization controls part of the device acquisition process/workflow.

3.2.13 Ensure that the IoT platform supports identification of IoT devices using Hardware Level Device Identification Tags/Fingerprint (much like a serial number) that is used as part of the on boarding authentication and authorization process.

3.2.14 Ensure that the Device Identification tag/ Fingerprint is not something that is hard-coded, but a pseudo value generated during initialization time to ensure hard-coded serial numbers cannot be spoofed. The pseudo value can also have an entropy to ensure it is only one-time use and used during provisioning. Once provisioned the device is then using PKI based certificate authentication services.

3.3 Communication Security

3.3.1 Ensure that all IoT devices operate with a minimal number of network TCP/UDP ports active. Ensure that the IoT devices unused ports are disabled.

3.3.2 Ensure that the IoT platform allows data tagging or sanitization to track and contain data from untrusted resources, since the device might be required to process data from unsecured channels.

3.3.3 Ensure that IoT devices/sensors that will support mobile communication services (3G/4G/LTE) are able to support secure Access Point Names (APN[2]) and not only Internet based APNs from the Mobile Service Provider.

2 In cellular networks, an APN acts as a private network configured specifically for a set of authenticated devices. Typically, a private APN (also called "secure APN") is a private network only accessible to authenticated devices associated with a specific business. By utilizing an APN, businesses can restrict what Endpoints are allowed to connect to their service infrastructure over the cellular network. This helps to reduce the amount of users that have direct access to IoT services in the back-end infrastructure.

3.3.4 Ensure that the IoT platform supports a trust anchor, a secure hardware technology that stores and processes cryptographic secrets such as PRE-SHARED Keys (PSK) or asymmetric keys (PKI). Trust anchors, can be used to authenticate not only peers during network communications, but can be augmented to store data useful for Endpoint application security.

3.3.5 Ensure that the IoT platform supports Trusted Computing Base (TCB) that performs mutual authentication with network peers, and manages communications and application security.

3.3.6 Ensure that an IoT platform supporting TCB also provides Separation of Duties such as keys to identify varying components or services within the IoT offerings. For example, one set of cryptographic keys could represent a firmware update service, while a second set of cryptographic keys could represent a push service.

3.3.7 Ensure that the IoT platform guarantees that the IoT device can operate in isolation with the same level of security in case connectivity to the IoT platform is not available.

3.3.8 Ensure that an IoT platform supporting TCB is driven through an API-model that guarantees:

- All signature verification is performed by the TCB
- No private keys are exposed from the TCB
- Key exchange can be performed by the TCB on behalf of the application
- Decryption can be performed by the TCB
- Encryption can be performed on the TCB
- Message signing can be performed on the TCB
- Secure message padding can be performed on the TCB
- Confidentiality and Integrity between the TCB and the application

3.3.9 Ensure that the IoT platform creates a Root of Trust (RoT), which are cryptographic policies and procedures that govern how identities, applications, and communications should be cryptographically secured. The RoT will have the following functions:

- Code signing key
- Server communications key
- Peer-to-peer communications key
- Endpoint identity key
- Master revocation key

3.3.10 Ensure that the IoT platform supports Root of Trust and secure exchange

of keys using common protocols such as:

- Transport Layer Security (TLS); The latest valid specification
- Secure Shell (SSH2)
- Online Certificate Status Protocol (OCSP) IETF RFC 2560
- Generic Bootstrapping Architecture (GBA) – 3GPP TS 33.220

3.3.11 Ensure that the IoT platform supports IoT Device Personalization such as cryptographically unique identities. One mechanism the IoT platform can support this is with the following method to ensure only authorized IoT devices:

- Generate a unique cryptographic key
- Sign the key using the organizational Endpoint Signing Key (or a derivative of)
- Store the key in the TCB's trust anchor
- Generate (or use) a unique internal identifier for that specific Endpoint
- Store the unique identifier in the TCB's trust anchor
- Save the unique identifier, the key, and the signature in the IoT Service back-end authentication system

3.3.12 Ensure Remote Access Administration of Remote IoT Devices is not available over the public interfaces or applications (API). Use of a separate communication channel for Remote Administration is highly recommended.

3.3.13 Apply industry standard and accepted encryption practices and avoid proprietary protocols, in line with the risk assessment results.

3.3.14 Ensure that the IoT platform supports policy-driven based encryption to ensure encryption- as-a-service is applied based on device type, data type, user type etc.

3.3.15 Ensure that the IoT platform and devices support IPSEC VPN (IKEv2) services where possible to provide transport level encryption over unsecured medium and specifically for remote administration of the endpoint devices.

3.3.16 Ensure that the IoT platform supports Perfect Forward Secrecy (PFS) to prevent the disclosure of cryptographic keys exchanged during the setup of communications between the IoT device and IoT platform.

3.3.17 In case of machine-to-machine (M2M) communication, it should be ensured that only legitimate communications are made.

3.3.18 The security (confidentiality, integrity and availability) of M2M communication should be ensured.

3.4 Hardware Security

3.4.1 Employ a hardware-based immutable Root of Trust.

3.4.2 Use hardware that incorporates security features to strengthen the protection and integrity of the device – for example, specialized security chips/coprocessors with security at the transistor level and embedded in the processor. Such chips should provide, among other things:

- A trusted storage of device identity and authentication means.
- Protection of keys at rest and in use.
- Preventing unprivileged access to security sensitive code. Protection against local and physical attacks can be covered via functional security.

3.5 Privacy Concerns and Lawful Intercept

3.5.1 Ensure that the IoT platform supports a Privacy Management Interface (PMI – an API for privacy attributes) for IoT devices where data privacy will be of concern[3].

3.5.2 Ensure that the IoT platform supports a Lawful Intercept Interface that can work in one of two ways: the first scenario is that a law enforcement agency will submit a legal request to ask for access to metadata or actual data from communications made by a specific IoT device or subscriber, while in the second instance, the law enforcement agency will ask the IoT service providers for access to a specific subscriber's data and/or metadata.

3.6 Audit and Logging

3.6.1 Ensure that the mandatory control 2.2.2 is enhanced to include:

- Failed privilege elevation attempts
- Failed logins to the device
- Failed device to device authentication attempts

3 The PMI will allow administrators to configure the features of privacy attributes that should be shared from the devices and ability to turn on and off these features. The PMI will also act as a function and feature for Lawful Intercept.

- Failed database access attempts
- Policy changes
- Privilege use
- Account creation
- Account change
- Failed tunnel negotiation
- Internal state
- On/Off
- Changes in the integrity of appropriate file systems

3.6.2 Ensure that the IoT platform supports remote log collection from IoT devices (gateways and edge) for the following;

- Anomaly detection
- Endpoint logging
- Endpoint diagnostics

3.6.3 Ensure that every IoT device type has a profile that is catalogued and baselined to understand the normal and abnormal state (Modelling IoT device behaviour is an important part of IoT security since a compromised endpoint can be indistinguishable from an endpoint behaving normally if only successful interactions with the device are logged and analysed). Ensure that the IoT platform has the basic capabilities of anomaly detection for:

- Erratic reboots or device resets
- Leaving or joining a communications network at erratic intervals
- Significantly different network traffic fingerprint than normal
- Multiple poorly-formed messages sent from the IoT device to the platform

3.7 Cryptography

3.7.1 Ensure that the IoT ecosystem supports cryptographic capabilities to verify trusted components (such as gateway, cloud, or mobile), and include cryptographic lifecycle management. This means supporting the issuing, and re-issuing, of cryptographic material, expiration of cryptographic certificates, a revocation and revocation checking mechanism, and a system from signing key material.

3.7.2 Ensure Cryptographic roots of trust are used for certificates' identity validation. Ensure that these stores are configurable in order to add new certificates and expire or remove revoked certificates to maintain forward compatible security.

3.7.3 Ensure that the platform supports hardware security features such as Hardware Security Modules (HSM's), Trusted Platform Modules (TPM's), and cryptographic coprocessors.

3.7.4 Ensure that cryptographic keys are securely managed.

3.8 Device Management

3.8.1 Ensure that the platform provides mechanisms to detect malicious and anomalous activity or integrate easily into device side malware protection or anomaly detection products.

3.8.2 Ensure that IoT devices are able to detect and resist attacks from the edge including spoofing, replay, and excessive communications.

3.8.3 Ensure that the IoT platform supports IoT device memory protection by preventing unprivileged applications and untrusted (third-party) apps or applications from executing.

3.8.4 Ensure that remote "Firmware over the Air", Remote "Administration", Remote "Patching" and other such IoT device services are secured and only accessible from the IoT platform itself and are not accessible publically or over the Internet.

3.8.5 Ensure that the IoT platform supports the running of applications on the IoT devices using appropriate privilege levels. Applications running on an IoT devices typically do not require super-user privileges. Most often, applications require access to device drivers or a network port. While some of these devices, ports, or other objects may require super-user privileges to initially access them, the super-user privileges are not required to perform subsequent operations.

3.8.6 Ensure that the IoT platform supports disabling debugging and test technology interfaces on the IoT devices.

3.8.7 Design the IoT platform as compartments to encapsulate elements in case of attacks.

3.8.8 Apply a secure mechanism by the IoT platform to decommission IoT devices. Ensure that the IoT platform has a secure method to decommission and revoke communication securely.

3.8.9 Ensure that the IoT platform supports multi-tenancy across all components of the platform

3.9 Software/Firmware

3.9.1 Ensure that update files are encrypted and that the files are also transmitted using encryption

3.9.2 Ensure that update files are signed and then validated by the device before installing

3.9.3 Ensure that the platform has the ability to implement scheduled updates

3.9.4 Ensure that the IoT platform supports IoT Device Image/Firmware Validation using secure cryptographic mechanisms to ensure the IoT device firmware has not been tampered with. This can be integrated as part of the trust anchor.

3.9.5 Ensure that the IoT platform supports all IoT device applications stored outside of a CPU's core ROM to be cryptographically authenticated.

3.9.6 Ensure that the IoT platform supports "over the air" application updates of the IoT device by ensuring cryptographic verification process is done for the already installed application and the same for the new application that is going to be deployed.

3.9.7 Ensure that automatic firmware updates do not modify user-configured preferences, security, and/or privacy settings without user notification.

3.10 Physical Security and Environment Control

3.10.1 Ensure that the firmware of Operating System cannot be accessed via unintended methods such as through an unnecessary USB port.

3.10.2 Ensure that the IoT platform/device is tamper resistant.

3.10.3 Ensure that the IoT product has the ability to limit administrative capabilities by only connecting locally for admin functions.

3.10.4 Ensure that the IoT platform has the ability to disable external ports such as USB.

3.10.5 Ensure that the IoT platform monitors the environment status and heath check of the remote IoT field devices. Power, temperature and humidity are environment levels that should be detected to determine whether the device should

continue running, or if it should power off. It should be noted, however, that powering off may be a desired effect, and that the adversary may abuse this engineering decision to leverage a denial of service.

3.11 Secure Storage

3.11.1 Ensure that some form of secured local storage for data is offered, that protects it from local malicious applications, compromised operating systems, or malicious owner/operator. Sensitive data can include sensor reading, configuration settings, authentication credentials, or cryptographic keys.

3.12 IoT and Distributed Ledger

3.12.1 Conduct a risk assessment to decide whether an IoT device can be commissioned on a public or private blockchain, or distributed ledger technology.

3.12.2 Ensure that IoT based on distributed ledger technology use distributed Proof of Work (PoW) and Proof of Stake (PoS) methods, where each IoT device can use different security levels depending on its respective security requirements, e.g. Proof-of-Ownership of IoT device, Proof-of-Identity, or Proof-of-Origin.

3.12.3 Ensure, where applicable, that IoT devices (sensors, actuators) infrastructure is implemented using blockchain/distributed ledger based technologies that provides superior security controls.

3.12.4 Ensure the usage of distributed ledger for performing IoT device asset management (such as registration and de-registration).

3.12.5 Ensure that each IoT asset should have a cryptographic ID that is known across the distributed nodes of the blockchain.

3.12.6 Ensure that where IoT devices need to communicate autonomously to each other (machine-to-machine), this should be performed using permissioned based blockchain infrastructure service, where possible.

3.12.7 Ensure that Real-time machine data transfers and transactions over blockchain are facilitated.

3.12.8 Ensure that IoT using blockchain infrastructure supports the immutable records of smart device history and transactions.

3.12.9 Ensure that the IoT blockchain infrastructure uses tamper-proof

properties not susceptible to man-in-the-middle attack; this also provides immutable transaction history.

3.12.10 Ensure, where possible, that the IoT firmware inherits blockchain technology natively (preventing IoT to participate in botnet based attacks).

3.12.11 Ensure that whenever data from IoT devices need to be extracted, self-executing smart contracts should be used to ensure correct extraction.

DUBAI ELECTRONIC SECURITY CENTER
مركز دبي للأمن الإلكتروني

4 ANNEXES

ANNEX A DEFINITIONS

ACCESS CONTROL
Mechanism to enable authorized people to access physical or digital entity resources, while preventing unauthorized people from doing the same.

ASSETS
Economic resources that are tangible or intangible, capable of being owned or controlled to produce value, and held to have positive economic value.

AUTHENTICATION
Act of verifying a claim of identity.

Note It is usually one or more of the following: something you know (password), something you have (identification card) or something you are (finger print).

AUTHORIZATION
Mechanism that verifies that the authenticated subject can carry out the intended action.

AVAILABILITY
Property of being accessible and usable upon demand by an authorized entity

CHANGE MANAGEMENT
Formal process for directing and controlling alterations to the information processing environment.

Note Its objectives are to reduce the risks posed by changes to the information processing, environment and improve the stability and reliability of the processing environment as changes are made. The change management process ensures that a change is: Requested, Approved, Planned, Tested, Scheduled, Communicated, Implemented, Documented and Reviewed after the change.

COMPLIANCE
Act of adhering to, and demonstrating adherence to, a standard or regulation (international, national or internal).

CONFIDENTIALITY
Property that information is not made available or disclosed to unauthorized entities.

CONFIGURATION MANAGEMENT
IT service management process that tracks all the individual configuration items (IT Assets) in an IT system.

Note This IT system might be as simple as a single server or an entire IT department.

CRITICAL INFORMATION INFRASTRUCTURE (CII)
Services, processes or assets supporting the sustainability and continuity of the most important functions and services in Dubai. The incapacity or destruction of which would have a drastic impact on Dubai's society, economy and safety.

CRYPTOGRAPHY
Discipline that embodies principles, means, and mechanisms for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.

EVENT
Any observable occurrence in a system or network.

Note Depending on their potential impact, some events need to be escalated for response.

IDENTITY
Set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish the entity from any other entities.

IDENTITY AND ACCESS MANAGEMENT (IAM)
The creation and management of identities for entities that may be granted logical or physical access to the organization's assets.

Note Access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives, needs to be controlled.

INCIDENT
Violation or imminent threat of violation of cyber security policies, acceptable use policies, or standard security practices.

INFORMATION
Any information, which can exist in many forms, such as printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation.

INTEGRITY
Property of accuracy and completeness.

IOT DEVICE
Any device that connects to a network and has the ability to receive and/or transmit data.

Note IoT devices might fall into three categories: sensors, actuators or gateways. Examples of IoT devices are: thermostats, door locks, fridges, and sensors in cars.

IOT PLATFORM
Whole set of components of IoT devices, gateways, and infrastructure that supports the operation of the IoT devices.

LOGGING
Automated recordkeeping (by elements of an IT or OT) of system, network, or user activity.

Note Logging may also refer to keeping a manual record (for example a sign-in sheet) of physical access by personnel to a protected asset or restricted area, although automated logging of physical access activity is commonplace.

MALICIOUS CODE
A code to infiltrate a computer system without the owner's informed consent to make it unavailable, steal information or use it to attack other computers.

Note This includes computer viruses, worms, Trojan horses, spyware, dishonest adware, crime ware, rootkits, and other malicious or unwanted software.

MONITORING
Collecting, recording, and distributing information about the behavior and activities of systems and persons to support the continuous process of identifying and analyzing risks to organizational assets and critical infrastructure that could adversely affect the operation and delivery of services.

MULTIFACTOR AUTHENTICATION
Concept of using two or more factors to achieve authentication.

Note Factors include (i) something you know (e.g. password/PIN), (ii) something you have (e.g. cryptographic identification device, token), (iii) something you are (e.g. biometric), or (iv) somewhere you are (e.g. GPS token).

NETWORK ARCHITECTURE
Framework that describes the structure and behavior of communications among IT and/or OT assets and prescribes rules for interaction and interconnection.

PHYSICAL ACCESS CONTROL
Controls that monitor and control the environment of the work place and computing facilities.

Note They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression

systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and work place into functional areas are also physical controls.

RISK

Quantifiable likelihood of potential harm that may arise from a future event.

RISK ASSESSMENT

Step in the risk management process to determine the qualitative or quantitative value of risk in relation to a recognized threat.

Note Quantitative risk assessment requires calculations of two components of risk; R, the magnitude of the potential loss L, and the probability p; that the loss will occur.

TRUSTED COMPUTING BASE (TCB)

A suite composed of hardware, software, and protocols that ensures the integrity of the endpoint.

VULNERABILITY ASSESSMENT

Systematic examination of an IT or product to determine the adequacy of cyber security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed cyber security measures, and confirm the adequacy of such measures after implementation.

ANNEX B
GAP ANALYSIS OF THE IOT SECURITY CONTROLS AGAINST ISR V2

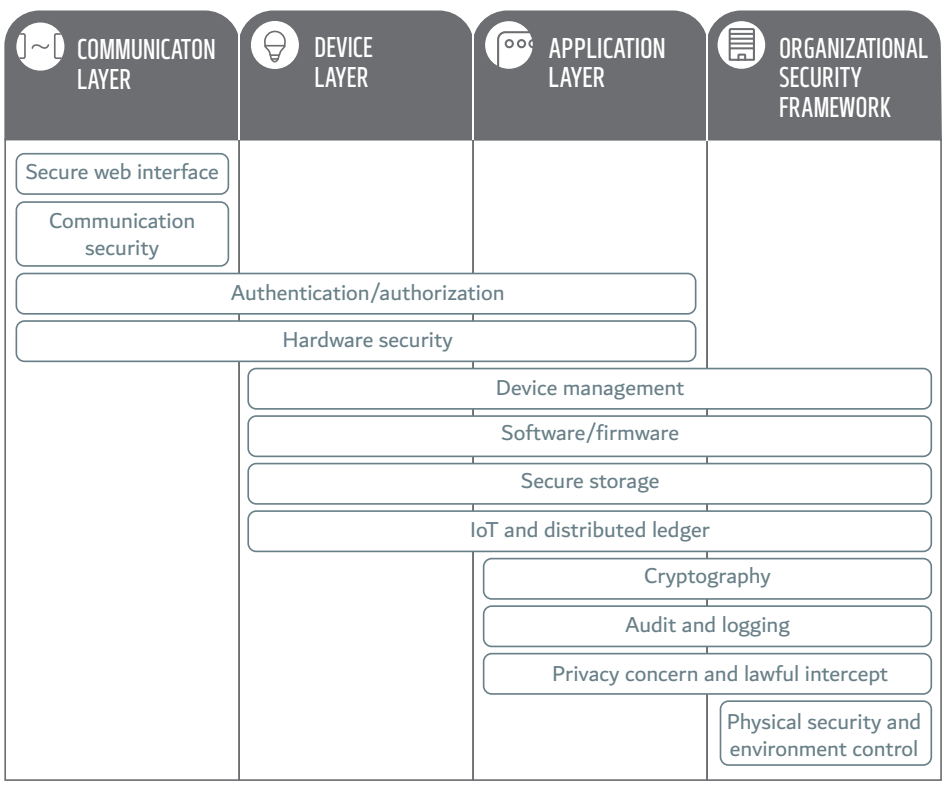
No.	Mandatory IoT Security Controls	Corresponding ISR V2 Clauses
1	Ensure that proven security solutions recognized by the security community are applied to the IoT device.	This links to Main Control 8.2 of ISR V2
2	Ensure that all security-relevant activities (for example access to and/or modification of information) can be logged and monitored.	This links to Main Control 6.9 of ISR V2
3	Ensure that security events and incidents can be detected and recorded for necessary corrective action.	This links to Main Control 4.2 of ISR V2
4	Provide regularly updated disclosure of vulnerabilities.	This indirectly relates to Controls 8.6, 11.4.2 from ISR V2, but is not explicitly addressed in there
5	Ensure that a secure booting process is in place for the IoT device.	This indirectly relates to Controls 5.2.3, 6.4, 8.2 from ISR V2, but is not explicitly addressed in there
6	Ensure, (for example by code signing) that malicious code cannot be injected into the information system to which the IoT device belongs.	This links to Main Control 6.3 of ISR V2

7	Disclose information regarding the replacement, removal or addition of any component in the supply chain of an IoT device that is currently approved and provided in the market.	This indirectly relates to Controls 6.1.3.3, 6.1.6 in ISR V2
8	Readdress the security guidelines and risk assessments whenever any update is introduced to the existing IoT platform.	This is not directly addressed in ISR V2, but links to Domain 3
9	Ensure that compromised or infected devices are identified and revoked in order to avoid having other functionalities of the system affected.	This indirectly relates to Controls 5.2.6.2, 6.3, 6.4.4, 6.9.2, 7.3.2 in ISR V2
10	Inform users/buyers of IoT devices about the expected life period of a given IoT device as well as the risks/issues associated with using it beyond its usability date. Any repair should be conducted in a timely manner.	This indirectly relates to Controls, 2.4.1, 5.2.6, 9.4 of ISR V2
11	Clearly indicate on the IoT device itself, and/or its packaging, its dependencies on any other systems/devices.	This indirectly relates to Controls 2.4.1, 5.2.6 in ISR V2
12	Provide a secure and reliable method to transfer the ownership of an IoT device from one person to another.	This indirectly relates to Controls 2.1, 2.2, 2.4, 2.5 in ISR:2017
13	Ensure that the information on the device can completely be wiped or destroyed whenever it is needed, as part of information protection, and a method of secure destruction.	This links to Control 5.2.6 in ISR V2
14	Ensure that any sensitive personally identifiable information can be anonymized or removed where necessary.	This indirectly relates to Controls, 5.2.6.2, 6.1.5.2, 8.8.2, 11.3 of ISR V2

15	Access to IoT devices should be controlled, based on least privilege access and need-to-know basis principles and the results of the risk assessment.	This links to controls 1.3, 3.3.2, 5.2, 5.3, 5.6 of ISR V2
16	Ensure that the defined security measures are implemented/active, even when an IoT device is facing some technical/operational disruption.	This indirectly relates to Controls 6.1.6, 6.4.6, 6.9.2, 7.2 from ISR V2, but is not explicitly addressed in there
17	Ensure that an access control system is in place for IoT devices, to detect and report invalid login attempts.	This indirectly relates to Controls 4.2.1, 5.2, 5.3, 6.4, 6.9 of ISR V2
18	Ensure that security measures, such as firewalls and secure authentication methods are implemented to control access to the IoT device, based on risk assessment results.	This indirectly relates to Controls 3.3.2, 5.2, 5.3, 5.6 of ISR V2
19	Ensure that IoT devices are running on recent operating systems, in line with the organization's policy for operating systems updates.	This links to Controls, 6.1.6, 8.2 of ISR:2017
20	Ensure that only up to date software is used in conjunction with IoT devices; updates of the software should be possible, when necessary. Allow only authorized sources to provide such updates.	This relates to Controls 8.1.2, 8.2.5, 8.6.1 from ISR V2
21	Ensure that the information system the IoT device belongs to supports selective connectivity for the administrator to be able to disconnect certain ports when required.	This links to Sub-Control 5.2.2 of ISR V2
22	Ensure that sector-specific security and privacy standards are adhered to, such as ISO/IEC 27799 for the health sector.	This links to Controls 6.1.6.2, 11.2.1 and 11.4 of ISR V2

23	Ensure that the information system in which IoT devices are used is equipped with layered defenses against cyber security threats including user level tools.	This is indirectly related to Controls 5.2.2., 5.2.3, 11.4.2 in ISR V2
24	Ensure that all communication and data storage related to IoT devices is encrypted, where necessary.	This links to Main Control 8.8 of ISR V2
25	Put appropriate network segregation in place (based on risk assessment results).	This links to Sub control 5.2.2 of ISR V2
26	Ensure that all connections are removed from any IoT device that has been removed from the network.	This is indirectly related to Controls 5.2.2.3, 5.2.2.7, 5.6.2, 6.4.4, 6.4.7 in ISR:2017

ANNEX C
SUGGESTIONS ON THE IMPLEMENTATION OF THE ADVANCED IOT SECURITY CONTROLS



ANNEX D
ORGANIZATIONS AND WORKS CONSULTED IN BRIEF

Extensive research was conducted on existing information security standards, regulations and frameworks in relation to IoT security during the course of drafting this standard. Pertinent information security documents were identified and consulted from the following organizations among others:

- Singapore Standard Council
- IoT Security Foundation
- OWASP
- OEASP
- ONG-C2M2

Further various versions of several standards, regulations and frameworks related to IoT security were considered, including but not limited to:

- TR 47: 2016 IoT reference architecture for Smart Nation – Singapore Standard Council
- Connected Consumer Products Release 1.0 – Best Practice Guidelines – IoT Security Foundation
- OWASP – IoT Security Guidance
- OWASP – IoT Security Foundation
- OEASP - Strategic principles for the security of IoT
- Oil and Natural Gas – Cyber security Capability Maturity Model (ONG-C2M2)