UNITED ARAB EMIRATES
MINISTRY OF CABINET AFFAIRS
PRIME MINISTER'S OFFICE

الإمارات العربية المتحدة
وزارة شؤون مجلس الوزراء
مكتب رئاسة مجلس الوزراء

NATIONAL IoT SECURITY POLICY

May 2023

Version 1.0

DISCLAIMER

This document is the sole property of UAE Cyber Security Council and is approved by the UAE Cabinet.

The UAE Cyber Security Council reserves the right to amend, add, or delete any section of this Policy.

Neither the whole nor part of this document shall be reproduced without the prior written consent of the UAE Cyber Security Council.

VERSION CONTROL

Version	0.1
Date:	21 February 2022
Prepared by:	CSC
Amendment Content:	Initial Draft

Version	0.2
Date:	08 March 2022
Prepared by:	CSC
Amendment Content:	Updates as per session held on 24 February 2022 with ADDA

Version	1.0
Date:	25 August 2022
Prepared by:	CSC
Amendment Content:	Updates as per review comments on the draft v0.2 of the document

	Reviewed by	Approved by
Designation:	xxxxxxxxx	xxxxxxxxx
Name:	xxxxxxxxx	xxxxxxxxx
Signature:	xxxxxxxxx	xxxxxxxxx
Date:	xxxxxxxxx	xxxxxxxxx

Table of Contents

Table of Contents

2. IoT Consumers

Table of Contents

Table of Contents

3. IoT Service Provider

SECTION 1

INTRODUCTION

INTRODUCTION

Internet-connected devices in recent times have become essential to many aspects of day-to-day life, from fitness trackers, pacemakers, and cars; to the control systems that deliver water and power to our homes. They enable seamless connections among people, networks and physical services. They are increasingly being used to collect telemetry data or perform actions without human intervention - on the brink of the fourth industrial revolution.

As we continue to integrate network connections into our nation's critical infrastructure, important processes that once were performed manually and in physical isolation (and thus enjoyed a measure of immunity against malicious cyber activity) are now vulnerable to cyber threats across the vast context of sensors, smart objects, smart city devices, transportation systems, automation devices, robotics, healthcare devices and other industrial components. The risk introduced by the IoT ecosystem to consumer privacy and potential disruptions in critical infrastructure are grave and require a holistic approach while still promoting interconnectivity and intelligent automation.

The Council has established this policy to protect the use, adoption and implementation of IoT, aligned with the UAE's national priority to be a global leader in cyber security; and enhance the security posture of organizations and individuals within the UAE using IoT products and solutions.

1.1 Purpose

This policy aims to strengthen the IoT security posture of the UAE by outlining the principles of securing the IoT ecosystem and addressing challenges in the emerging technology landscape. The policy will further provide guidance to the key stakeholder in the IoT ecosystem in the UAE, define requirements for IoT security and outline the oversight and enforcement of IoT security mandates.

The policy will help to ensure IoT Service Providers achieve a set of security requirements and ensure all IoT Consumers are well protected when procuring and using IoT services. This policy also aims to carefully avoid the potential negative impacts of implementation, i.e. inhibiting investment and stunting the growth of the IoT ecosystem due to overly stringent requirements.

1.2 Scope & Applicability

Achieving a resilient IoT security posture requires that all IoT device domains are considered. This policy applies to all IoT device domains across all sectors in the UAE, including but not limited to:

IoT Ecosystem

The interconnected network of devices collecting, sharing, and processing data over the internet. They can range from common consumer devices like smart watches and smart home devices to heavy machinery and industrial manufacturing equipment. For example, a smart home network that monitors the time of day or senses when the sun sets and automatically closes the blinds and turns on the lights, this simple example makes use of sensors, smart lights, networking, cloud computing and actuators to complete its task.

Industrial IoT Devices

Network of interconnected devices linking industrial equipment and sensors to allow automation throughout an industrial plant. The Industrial Internet of Things or IIoT principally points to an industrial framework where software tools link various machines or devices. The devices of industrial IoT classify from complex industrial robots to diminutive environmental sensors. Commonly, companies utilize industrial IoT projects for internal cost efficiency. The widely used applications of IIoT are smart meters, smart grids, smart factories, and similar.

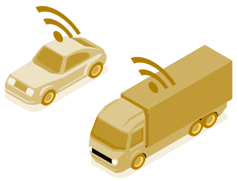
1.2 Scope & Applicability

Smart City IoT Devices

IoT sensors and devices are used for gathering and analyzing data to improve the city's operational efficiency. Conventional cities are turning to smart cities as a result of the Internet of Things. Sensors, data, and connections integrate into a Smart City to develop digital technologies and communication systems that optimize city operations. Smart Cities can leverage IoT devices and intelligent technologies in public safety and security, water and waste management, transportation, air pollution control, building management systems, and similar.

Medical IoT Devices

The ecosystem of internet-connected medical devices, hardware frameworks, and software applications linking health information technology to medical practitioners and patients. IoMT allows wireless and remote devices to securely connect for agile and flexible medical data processing via the internet. For example, wireless blood pressure monitoring, IoT-enabled cardiac rhythm monitoring, and remote patient monitoring can be classified into IoMT devices.



Connected Vehicles

IoT devices and sensors used for intelligent and efficient driving. Connected vehicles are incorporated with the Internet of Things (IoT) technology. A related automobile can link to adjacent devices through wireless networks to transmit data in both directions (bidirectional communication) with other vehicles, mobile devices, and city intersections. A self-driving car or Unattended Automated Vehicle (UAV) can be classified into the connected vehicles environment.

1.2 Scope & Applicability

This policy applies to the following entities involved in IoT devices and services within the UAE, including but not limited to:

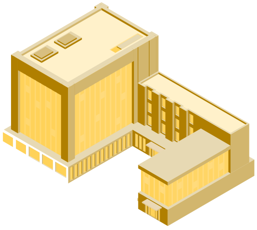
IoT Consumers: IoT Consumers are end-users purchasing and using off-the-shelf IoT devices or systems for application in industry or for personal use. IoT Consumers are further categorized as follows, based on the applicability of this policy:

Critical Information Infrastructure (CII) Entities

The IoT Security Policy is mandated on all critical information infrastructure entities within the UAE using or looking to procure IoT services. Refer to the UAE Critical Information Infrastructure Policy for a detailed list of CII Sectors.

Government Entities

The IoT Security Policy is mandated on all government entities within the UAE using or looking to procure IoT services.



Other Entities

The IoT Security Policy is NOT mandated on other organizations, using or looking to procure IoT services in the UAE and will serve as an advisory guide.

Individuals

The IoT Security Policy is NOT mandated on individuals, using or looking to procure IoT services in the UAE and will serve as an advisory guide.

1.2 Scope & Applicability

IoT Service Providers: The IoT Security Policy is mandated on all IoT service providers, developers, and implementers offering services within the UAE.

IoT Manufacturers: IoT Device manufacturers are advised to adhere to the requirements set out in this policy if they wish to manufacture or sell IoT devices within the UAE.

1.3 Adoption Lifecycle

The National Cyber Security Governance Framework (NCSGF) outlines a common integrated approach for managing and adopting cyber security at the entity, sector, and national levels. The NCSGF introduces a lifecycle for Understanding, Assessing, Implementing, Monitoring and Collaborating on cyber security within UAE. This lifecycle ensures continual improvement of the UAE's cyber security capabilities providing requirements for emerging technologies, such as IoT, are well defined, managed, and adopted.

Understanding the complexity of network-connected technologies, it's increasing dependency on other critical information infrastructure, the economic drivers, and the overall threat landscape within the country.

Assessing risks on IoT devices, processes, and services, identifying risks of potential breach or failure, determining relative impact, and selecting controls to mitigate the risks.

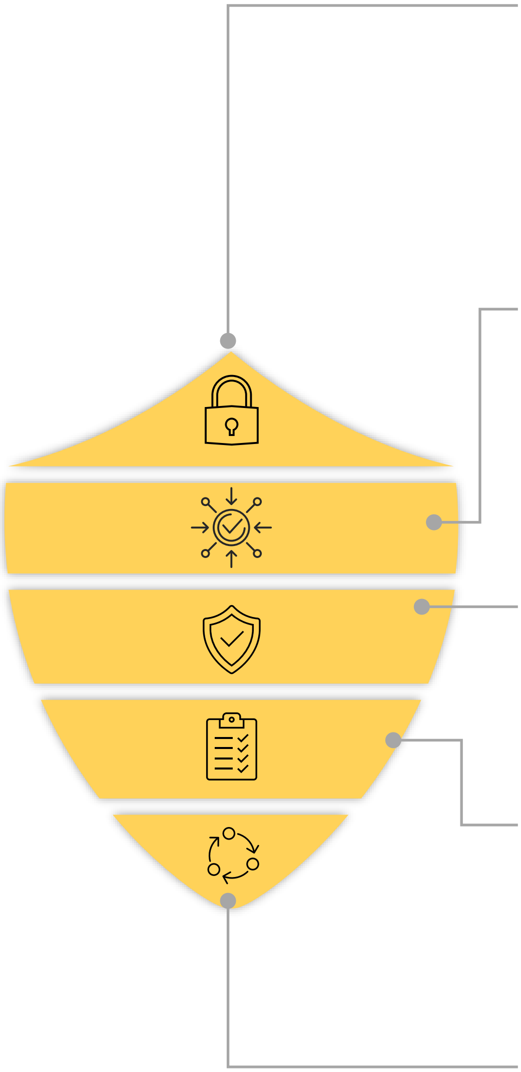
Implementing the identified security controls in the earliest phases of requirement definition, use case design, technology architecture design, software development, and production and operations.

Monitoring and reviewing the performance and effectiveness of the implemented controls.

Collaborating to ensure continual improvement of processes, services, and security controls.

1.4 IoT Security Principles

The five IoT security principles are laid out to provide foundational elements to decision-makers regarding IoT technology adoptions, implementations, and operations in the UAE. They assist IoT consumers and IoT service providers in making procurement and operational decisions, keeping in line with the policies detailed in this document.



Security and Privacy by Design

Certified devices, purpose-built operating system, managed services from recognized service providers, and skilled resources are used to support secure IoT development, deployment and operations.

Security Prioritization based on Impact

Potential consequences of disruption, breach, or malicious activity across the consumer spectrum are considered to determine the security efforts and assign responsibilities to mitigate significant consequences.

Defence in Depth

A holistic approach to security that includes layered defenses against cybersecurity threats are built in IoT architectures and ecosystem.

Best Practices Guidelines

Global best practice frameworks are leveraged to provide security assurance and drive compliance efficiencies.

Collaborative & Transparent Ecosystem

Information on vulnerabilities and intelligence are shared openly among manufacturers, service providers, industrial consumers, and regulators leading to increased awareness.

1.5 Exception Approval

A policy exception may be granted by the Cyber Security Council under special circumstances.

Exceptions are reviewed on a case-by-case basis and their approval is not guaranteed.

SECTION 2

IoT CONSUMER

The following section outlines the policy domains and sub-domains applicable to IoT consumers in the UAE. The policy sub-domains further elaborate on the objectives and policy statements

2.1 IoT Governance

2.1.1 Governance Framework

Version 1.0

Adoption Lifecycle

Understanding | Assessing | Implementing | Monitoring | Collaborating

Policy Objective

To establish leadership and governance to initiate and support the implementation of IoT security requirements.

Policy Statements

2.1.1.1 IoT consumers shall adopt a comprehensive governance model to manage and control IoT components and services used in the related ecosystem.

2.1.1.2 IoT Consumers shall establish a strategy and plan for managing, implementing, and monitoring IoT devices and services, as well as understanding individual roles and responsibilities.

2.1.1.3 IoT consumers shall ensure that IoT service providers, operators and users involved in managing, implementing, and monitoring IoT devices and services are aware of their roles and responsibilities.

2.1 IoT Governance

2.1.2 Risk Management

Version	1.0

Adoption Lifecycle

Understanding	**Assessing**	Implementing	Monitoring	Collaborating

Policy Objective

To proactively identify and ensure timely remediation IoT security and privacy risks.

Policy Statements

2.1.2.1 A robust and continuous risk management program shall be established and implemented to include the IoT ecosystem within the risk assessment regime.

2.1.2.2 IoT security and privacy risk assessments shall be conducted to analyze the impact on data/assets hosted within the IoT ecosystem.

2.1 IoT Governance

2.1.3 Awareness and Training

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To enhance the awareness of personnel on IoT threats and vulnerabilities by exposing them to focused trainings.

Policy Statements

2.1.3.1 An awareness and training plan shall be developed to provide specialized IoT security training to all personnel (employees, contractors, third party staff) managing, implementing, and monitoring IoT devices and/or services.

2.1.3.2 IoT security trainings shall be appropriately tailored to employees' roles and responsibilities.

2.1 IoT Governance

2.1.4 Third Party Security

Version 1.0

Adoption Lifecycle

Understanding	**Assessing**	**Implementing**	Monitoring	Collaborating

Policy Objective

To reduce the likelihood of third-party operational failures and data breaches.

Policy Statements

2.1.4.1 Third-party security policies shall be developed and implemented to facilitate the execution of relevant controls and ensure that external stakeholders adhere to the organization's IoT security policies.

2.1.4.2 Non-disclosure agreements, Service level agreements, and documented contractual agreements, including all IoT security, availability, and privacy requirements in line with all applicable standards, laws, and regulations, shall be clearly defined and agreed upon.

2.1.4.3 Access of the third party to critical layers of IoT devices shall be granted based on the least privileged principle for a specified time frame and shall be periodically reviewed and reconciled.

2.1 IoT Governance

2.1.5 Compliance

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To ascertain effective implementation of IoT security controls

Policy Statements

2.1.5.1 IoT solutions shall be compliant with applicable national and international regulation and best practices through maintenance of a compliance management program and periodic assessments.

2.1.5.2 UAE Data sovereignty laws shall be applied to sensitive data at rest, in transit, and in processing.

2.1.5.3 Ensuring compliance with cybersecurity standards issued by the Cyber Security Council .

2.1.5.4 Ensure the application of the approved and enforced standards and policies of the Telecommunications Regulatory Authority and Digital Government (TDRA) to enhance cybersecurity level.

2.1.5.5 The standards and policies approved and applied by the authorities and sectors concerned with the work of those in charge of these technologies must be adhered to.

2.1.5.6 Implementation of cyber security standards issued by the International Organization for Standardization (27001 and 27002)

2.2 Data Security

2.2.1 Data Privacy and Governance

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To protect confidentiality, integrity, and/or availability of data (including PII) collected by, stored on, processed by, or transmitted to or from the IoT device.

Policy Statements

2.2.1.1 Processes and technical measures shall be defined, documented and implemented for data classification based on sensitivity and to capture the physical locations of data.

2.2.1.2 Consumers shall be provided clear and transparent information about how their data is being used, by whom, and for what purposes, for each IoT device and service.

2.2.1.3 Consumer of IoT products and services shall be able to exercise their rights to information, access, erasure, rectification, data portability, restriction of processing, objection to processing, and their right not to be evaluated based on automated processing.

2.2.1.4 Consumers of IoT products and services shall protect the confidentiality, integrity, and/or availability of data including personally identifiable information (PII) collected by, stored on, processed by, or transmitted to or from the IoT device.

2.2.1.5 A contractual agreement shall be created to restrict any unauthorized use or disclosure of confidential information or data

2.2.1.6 Policies and procedures shall be developed to protect the physical/logical location of data and prevent the unauthorized collection of diagnostic data or data used for analysis.

2.2 Data Security

2.2.2 Encryption and Cryptography

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To ensure adequate use of cryptographic capabilities to secure data at rest, data transactions and exchange between IoT devices.

Policy Statements

2.2.2.1 An organizational root of trust shall be defined, which is a set of cryptographic policies and procedures governing how identities, applications, and communications can be cryptographically secured. This model helps to ensure that all messages are secured through the cryptographic hierarchy.

2.2.2.2 A root private key, either symmetric or asymmetric, should be used to digitally sign other keys used in the hierarchy.

2.2.2.3 A risk based approach to encryption shall be implemented to secure all communications against classic and quantum threats.

2.2 Data Security

2.2.3 Secure and Trusted Communications

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To ensure confidentiality (privacy), integrity, availability, and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud.

Policy Statements

2.2.3.1 Secure session management shall be established, due to various communications taking place in IoT systems, and many sessions being established, it is necessary to implement secure sessions in order to ensure security of communications.

2.2.3.2 Develop session management policies and procedures for the different communications sessions and ensure that session expiry and session authentication controls are incorporated into the policies and procedures to eliminate session hijacking.

2.2.3.3 Secure communication protocols shall be employed using encrypted channels, integrity protection, and authenticated connections to share information between IoT systems. Proven encryption techniques shall be used to protect data in any IoT systems and underlying infrastructure.

2.3 Identity and Access Management

2.3.1 Access Control

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To prevent unauthorized access and alteration of organizational resources, applications, and data while using IoT services.

Policy Statements

2.3.1.1 Develop and implement an access management policy based on the principle of least privilege, with unique identification to required resources only, with proper accountability and non-repudiation

2.3.1.2 Develop and implement robust authentication mechanisms for the IoT systems and mandate the deployment of strong passwords, personal identification numbers (PINs), and multi-factor authentication capability in the IoT solutions.

2.3.1.3 All access to IoT systems shall be authenticated using centralized authentication mechanisms. Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software shall not be acceptable.

2.3.1.4 Access to system resources shall be controlled and managed throughout its lifecycles, minimizing opportunities for malicious actors.

2.3.1.5 Implement access control and access review in IoT systems (and other underlying infrastructure) to ensure that the system verifies that users and applications have the right permissions and consider deployment of additional compensating controls in case of personnel changes.

2.3.1.6 Ensure passwords are aligned to the internal password complexity policy/Industry standards and require setting a new password after a defined period.

2.3 Identity and Access Management

2.3.2 Physical Access

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To ensure that the IoT environment is protected against unauthorized physical access

Policy Statements

2.3.2.1 Physical access shall be provisioned to users with valid business needs, with proper authorization and monitoring.

2.3.2.2 All physical and logical access shall only be provisioned to users that have been adequately vetted, including background checks and due diligence.

2.3.2.3 Physical access shall be restricted and controlled using tamper-proof fences, casing, and mechanical or electronic locks.

2.4 Incident Management

2.4.1 Incident Management

Version 1.0

Adoption Lifecycle

Understanding | Assessing | **Implementing** | Monitoring | Collaborating

Policy Objective

To minimize the impact of security risks and with the IoT environment

Policy Statements

2.4.1.1 Develop and implement a robust incident response strategy & plan to contain and recover from incidents with the minimum operational and business impact.

2.4.1.2 Incidents shall be classified based on the business or operational impact on the organization.

2.4.1.3 Establish the applicable incident management playbooks with detailed possible threats and impact and pre-defined containment and recovery activities.

2.4 Incident Management

2.4.2 Incident Response

Version 1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	**Collaborating**

Policy Objective

To effectively contain and minimize impacts of security incidents.

Policy Statements

2.4.2.1 The effectiveness of the security incident response plan and team shall be evaluated periodically.

2.4.2.2 Post incident analysis and lessons learned shall be used to continuously enhance the incident response strategy and plan.

2.4.2.3 IoT solutions and services shall be configured to be in resilient mode during any unforeseen events.

2.4 Incident Management

2.4.3 Incident Reporting

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To ensure security incidents are reported in acceptable timescales and format.

Policy Statements

2.4.3.1 Any identified security flaws or irregularities shall be reported to the relevant incident management team within the organization.

2.4.3.2 Security incidents shall be disclosed and reported to the relevant local/national authorities within defined time intervals, and the report/communication shall be supported by all necessary documentation.

2.4 Incident Management

2.4.4 IoT Forensics

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To determine and investigate the exact intent and extent of security breaches related to IoT devices.

Policy Statements

2.4.4.1 Identify skilled resources to support with IoT Forensics analysis.

2.4.4.2 Use effective methods or automated process to trace data on IoT devices, in network, and in the cloud.

2.4 Incident Management

2.4.5 Vulnerability Management

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To support identifying, classifying, prioritizing, remediating, and mitigating vulnerabilities within the IoT environment

Policy Statements

2.4.5.1 Comprehensive vulnerability management process for proactive identification and timely remediation of vulnerabilities shall be defined and effectively implemented.

2.4.5.2 Vulnerabilities in the IoT device, solution, and application environments shall be periodically assessed for proactive identification and reported to relevant parties.

2.4.5.3 IoT systems and applications shall be regularly patched & updated to minimize the threat landscape.

2.4.5.4 Independent third-party penetration testing shall be performed periodically or after significant system changes in a controlled environment.

2.4.5.5 Threat intelligence capabilities should be implemented to monitor and assess security threats to IoT systems

2.5 IoT Resilience

2.5.1 Secure Backup

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	**Collaborating**

Policy Objective

To ensure the availability of information and minimize the impact of incidents.

Policy Statements

2.5.1.1 IoT consumers shall perform periodic user and configuration data backups and undertake backup restoration testing.

2.5.1.2 IoT consumers are required to save and document backup data using advanced technological systems with the use of approved encryption methods in this regard.

2.5.1.3 Determining and providing access, transfer and restoration of backup copies by authorized personnel within the institution in accordance with the approved and authorized roles and responsibilities.

2.5.1.4 IoT consumers must follow security controls for storing, transferring and restoring backup copies to ensure the confidentiality and integrity of data.

2.5.1.5 IoT consumers must periodically test the integrity of their backup copies to ensure that an alternative backup is available in the event of any incident or natural disaster.

2.5 IoT Resilience

2.5.2 Disaster Recovery

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To ensure high availability of resources and information as part of continuity efforts and minimize the impact of outages and incidents.

Policy Statements

2.5.2.1 IoT consumers shall assess IoT solutions, services, and information availability requirements to ensure continuity of services.

2.5.2.2 IoT consumers shall establish a disaster recovery plan to ensure continuity of IoT operations.

2.5.2.3 IoT consumers should monitor and update their recovery and business continuity plans periodically to ensure the best implementation and compliance with international and national standards.

2.6 Device Management

2.6.1 Asset Management

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To maintain an inventory and manage IoT assets across their lifecycle, including the hardware and software.

Policy Statements

2.6.1.1 IoT consumers shall establish and maintain asset management procedures for critical IoT systems.

2.6.1.2 IoT device inventory shall be maintained and updated regularly for connected devices, software, and firmware versions.

2.6.1.3 IoT consumers shall establish procedures to ensure timely maintenance of IoT devices, replacement and/or secure disposal of out-of-support/end-of-life IoT devices.

2.6 Device Management

2.6.2 Application Security

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To implement the necessary security controls in applications that interface with IoT devices and related components.

Policy Statements

2.6.2.1 IoT solution components such as applications, middleware, APIs, and devices shall be configured for secure authentication and information exchange over encrypted channels.

2.6.2.2 Applications shall be implemented with end-to-end security controls and availability aspects across the IoT solution and shall enforce access control rules on trusted service layer.

2.6.2.3 A secure and dedicated gateway shall be utilized for data normalization and processing within IoT networks.

2.6 Device Management

2.6.3 Device Security

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To safeguard the IoT environment during the operational lifecycle of the device.

Policy Statements

2.6.3.1 IoT devices & sensors shall be securely installed and configured to protect the hardware from unauthorized access or tampering.

2.6.3.2 IoT device shall be managed and administrated remotely over encrypted and authenticated channels, with security logs enabled.

2.6.3.3 A device management strategy, ensuring periodic updates and regular maintenance to safeguard IoT devices, shall be documented and implemented.

2.6.3.4 Security patches and updates from authentic sources shall be periodically implemented in a secure and fail-safe mode, including compatibility with security configurations set in earlier firmware versions.

2.6.3.5 All patches and updates shall be are tested and assessed for risk and impact before being applied across all IoT devices or systems.

2.6.3.6 Compensatory measures shall be applied for the devices that have reached their end-of-life cycle.

2.7 Network Security

2.7.1 Network Management

Version	1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	Collaborating

Policy Objective

To ensure protection of IoT network components and related ecosystems.

Policy Statements

2.7.1.1 IoT networks shall be secured using secure ports and protocols with authentication and encryption enabled.

2.7.1.2 Security controls and interoperability shall be considered across different routing networks.

2.7.1.3 IoT networks shall be segregated from the corporate network and micro-segmented for controlled access.

2.7.1.4 Information exchange and infrastructure management of IoT devices and applications shall be restricted and controlled.

2.7.1.5 Unused and default network services, protocols, and ports shall be disabled.

2.7.1.6 IoT solution administration and management shall be conducted via a separate segregated network.

2.7.1.7 The consumer IoT device shall use best practice cryptography to enable secure communications.

2.8 Security Logging and Monitoring

2.8.1 Audit Logging

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To track and record activities and events in the IoT environment.

Policy Statements

2.8.1.1 IoT devices, systems, and application logs shall be enabled and monitored in real-time, where technically feasible.

2.8.1.2 IoT devices, systems, and application logs shall be monitored for unauthorized access, connections, or configuration changes.

2.8.1.3 Security controls for IoT devices, systems, and applications shall be audited and reviewed periodically.

2.8 Security Logging and Monitoring

2.8.2 Monitoring

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To identify, detect, and remediate inappropriate access, use of systems and information.

Policy Statements

2.8.2.1 IoT devices, systems, and application logs shall be correlated, analyzed, and reviewed to identify any security threat or malicious activity.

2.8.2.2 Regular monitoring of device behaviour, to detect malware and to discover integrity errors shall be undertaken.

2.8.2.3 IoT devices, systems, and application logs shall be securely retained in line with the entity retention policy, requirements of applicable laws, and regulations.

SECTION 3

IoT SERVICE PROVIDER

The following section outlines the policy domains and sub-domains applicable to IoT consumers in the UAE. The policy sub-domains further elaborate on the objectives and policy statements

3.1 IoT Governance

3.1.1 Governance Framework

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To establish leadership and governance to initiate and support implementation of IoT security requirements.

Policy Statements

3.1.1.1 An IoT security strategy and program shall be developed, defining a governance structure and IoT security operating model, and are compliant with existing standards, laws and regulations.

3.1.1.2 Ensure IoT service providers, operators, and users involved in managing, implementing, and monitoring IoT devices and services are aware of their roles and responsibilities.

3.1.1.3 The confidentiality of the personal data of users of technology and owners of associated machines and devices must be ensured that it is encrypted and ensured its integrity and protection (CIA).

3.1.1.4 A record must be created containing the technologies, devices and machines used for IoT technologies to ensure continuous updating of the data.

3.1 IoT Governance

3.1.2 Risk Management

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To proactively identify and ensure the timely remediation of IoT security and privacy risks.

Policy Statements

3.1.2.1 A robust and continuous risk management program shall be established and implemented to include the IoT ecosystem within the risk assessment regime.

3.1.2.2 IoT security and privacy risk assessments shall be conducted to analyze the impact on data/assets hosted within the IoT ecosystem.

3.1 IoT Governance

3.1.3 Awareness and Training

Version 1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	Collaborating

Policy Objective

To enhance the awareness of personnel on IoT threats and vulnerabilities by exposing them to focused trainings.

Policy Statements

3.1.3.1 An awareness and training plan shall be developed to provide specialized IoT security training to all personnel (employees, contractors, and outsourced staff) managing, implementing, and monitoring IoT devices and/or services.

3.1.3.2 IoT security trainings shall be appropriately tailored to employees' roles and responsibilities.

3.1 IoT Governance

3.1.4 Third Party Security

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To reduce the likelihood of third-party operational failures and data breaches.

Policy Statements

3.1.4.1 Third-party security policies shall be developed and implemented to facilitate the execution of relevant controls and ensure that external stakeholders adhere to the organization's IoT security policies.

3.1.4.2 Non-disclosure agreements, Service level agreements, and documented contractual agreements, including all IoT security, availability, and privacy requirements in line with all applicable standards, laws, and regulations shall be clearly defined and agreed upon when procuring IoT services.

3.1.4.3 Establish and implement a supply chain management plan to protect the integrity of the supply chain. The plan should include security frameworks, risk management, and contractual requirements.

3.1 IoT Governance

3.1.5 Compliance

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To ascertain effective implementation of IoT security controls.

Policy Statements

3.1.5.1 IoT solutions shall be compliant with applicable Local, national and international regulation and best practices through maintenance of a compliance management program and periodic assessments.

3.1.5.2 UAE Data sovereignty laws shall be applied to sensitive data at rest, in transit, and in processing.

3.1.5.3 Ensuring compliance with cybersecurity standards issued by the Cyber Security Council.

3.1.5.4 Ensure the application of the approved and enforced standards and policies of the Telecommunications Regulatory Authority and Digital Government (TDRA) to enhance cybersecurity.

3.1.5.5 The standards and policies approved and applied by the authorities and sectors concerned with the work of those in charge of these technologies must be adhered to.

3.1.5.6 Implementation of cyber security standards issued by the International Organization for Standardization (27001 and 27002)

3.2 Data Security

3.2.1 Data Privacy and Governance

Version	1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	Collaborating

Policy Objective

To protect confidentiality, integrity, and/or availability of data (including PII) collected by, stored on, processed by, or transmitted to or from the IoT device.

Policy Statements

3.2.1.1 Access to and tampering with data at rest or in transit that might expose sensitive information or allow manipulation or disruption of IoT device operations, shall be prevented.

3.2.1.2 Data protection obligations based on applicable regulations shall be adhered to when developing and delivering IoT devices and services.

3.2.1.3 IoT device activity shall be monitored and analyzed for signs of incidents involving data security.

3.2.1.4 Consumers shall be provided with all rights as per applicable data privacy law to preserve their privacy by securely configuring the device and service functionality.

3.2.1.5 When dealing with sensitive user data, IoT service providers are obligated to preserve the confidentiality, integrity, and/or availability of data, including personally identifiable information (PII), collected by, stored on, processed by, or sent to or from the IoT device.

3.2.1.6 Acknowledge and agree upon policies and procedures as per contractual agreement to restrict any unauthorized use or disclosure of user confidential data and information. As per agreement safeguard the physical/logical location of user data and prevent the unauthorized collection of diagnostic data or data used for analysis.

3.2 Data Security

3.2.2 Encryption and Cryptography

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To ensure adequate use of cryptographic capabilities to secure data at rest, data transactions and exchange between IoT devices.

Policy Statements

3.2.2.1 Confidentiality, authenticity, and/or integrity of data and information (including control messages), in transit and in rest shall be ensured through proper selection of strong encryption algorithms and strong keys and disable insecure protocols.

3.2.2.2 Service provider shall ensure that devices are built to be compatible with lightweight encryption and security techniques.

3.2.2.3 Industry accepted cryptographic techniques and best practices shall be applied appropriately and adequately for IoT devices and systems.

3.2.2.4 Secure web interfaces shall be implemented for IoT systems with encryption, authentication, and authorization.

3.2.2.5 The latest and best standard and approved encryption algorithms should be used.

3.2 Data Security

3.2.3 Secure and Trusted Communications

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To ensure communications cannot be compromised by using encrypted channels, integrity protection & authenticated connection to share information between IoT systems.

Policy Statements

3.2.3.1 IoT devices should be restrictive rather than permissive in communicating and only specific ports and/or network connections shall be enabled for selective connectivity.

3.2.3.2 Secure web interfaces shall be implemented for IoT systems with authentication and authorization check.

3.2.3.3 Enforce session management policies and procedures for various communications sessions and have session expiry and session authentication controls in place to secure communication against session hijacking as per the consumer requirements.

3.2.3.4 Enforce communication protocols including encrypted channels, integrity protection, and authenticated connections to secure communication between IoT devices and systems as per consumers requirements.

3.3 Identity and Access Management

3.3.1 Access Control

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To prevent unauthorized access and alteration of organizational resources, applications, and data while using IoT services.

Policy Statements

3.3.1.1 Develop and implement an access management policy based on the principle of least privilege, with unique identification to required resources only, with proper accountability and non-repudiation.

3.3.1.2 All access to IoT systems shall be authenticated using centralized authentication mechanisms. Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software shall not be acceptable.

3.3.1.3 Access to system resources shall be controlled and managed throughout its lifecycles, minimizing opportunities for malicious actors.

3.3.1.4 IoT service providers and administrators shall enable a mechanism for IoT users to change the default username and password before connecting the device to the network.

3.3 Identity and Access Management

3.3.2 Physical access

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To ensure that the IoT environment is protected against unauthorized physical access.

Policy Statements

3.3.2.1 Physical access shall be provisioned to users with valid business needs, with proper authorization and monitoring.

3.3.2.2 All physical and logical access shall only be provisioned to users that have been adequately vetted, including background checks and due diligence.

3.3.2.3 Physical access shall be restricted and controlled using tamper-proof fences, casing, and mechanical or electronic locks.

3.4 Incident Management

3.4.1 Incident Management

Version	1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	Collaborating

Policy Objective

To minimize the impact of security issues with the IoT environment.

Policy Statements

3.4.1.1 Service providers shall implement a robust incident response strategy & plan to contain and recover from incidents with the minimum operational and business impact in alignment with the National Incident Response Framework and Plan.

3.4.1.2 Incident classification guidelines shall be based on the business or operational impact of the consumers environment.

3.4.1.3 Support consumers in establishing and implementing the applicable incident management playbooks with detailed possible threats and impact and pre-defined containment and recovery activities

3.4 Incident Management

3.4.2 Incident Response

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To effectively contain and minimize impacts of security incidents.

Policy Statements

3.4.2.1 The effectiveness of the security incident response plan and team shall be evaluated periodically.

3.4.2.2 Post-incident analysis and lessons learned shall be used to continuously enhance the incident response strategy and plan.

3.4.2.3 IoT solutions and services shall be configured to be in resilient mode during any unforeseen events.

3.4 Incident Management

3.4.3 Incident Reporting

Version 1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	Collaborating

Policy Objective

To ensure security incidents are reported in acceptable timescales and format.

Policy Statements

3.4.3.1 Any identified security flaws or irregularities shall be reported to the relevant incident management team within the organization

3.4.3.2 IoT service providers shall promptly report the incident to the consumer/affected party within a defined timeframe. The IoT service providers should also inform the consumer about any incident at the associated third party (supply chain incidents).

3.4 Incident Management

3.4.4 Vulnerability Management

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To support identifying, classifying, prioritizing, remediating, and mitigating vulnerabilities within the IoT environment.

Policy Statements

3.4.4.1 Comprehensive vulnerability management processes for proactive identification and timely remediation of vulnerabilities shall be defined and effectively implemented.

3.4.4.2 Vulnerabilities in the IoT device, solution, and application environments shall be periodically assessed for proactive identification and reported to relevant parties.

3.4.4.3 IoT systems and applications shall be regularly patched & updated to minimize the threat landscape.

3.4.4.4 Independent third-party penetration testing shall be performed periodically or after significant system changes in a controlled environment.

3.4.4.5 Threat intelligence capabilities should be implemented to monitor and assess security threats to IoT systems.

3.5 IoT Resilience

3.5.1 Resilience of IoT Services

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	**Collaborating**

Policy Objective

To cater for high availability of IoT components as part of continuity efforts and minimize the impact of outages and incidents.

Policy Statements

3.5.1.1 IoT service providers shall ensure that regular backups of system data (including settings) can be achieved.

3.5.1.2 IoT devices and services shall have built-in capabilities to remain operational and locally functional for essential features, in case of a loss of communications.

3.5.1.3 IoT solutions and services shall fail in a safe and secure manner to ensure information integrity and availability while recovering to a normal state.

3.5.1.4 IoT systems shall be provided with mechanisms for self-diagnosis and self-repair/ healing to recover from failure, malfunction, or a compromised state. If an automated/self-repair process is not achievable , the use of a manual restoration technique to allow the IoT system to return to a secure configuration shall be.

3.6 Device Management

3.6.1 Asset Management

Version	1.0

Adoption Lifecycle

Understanding | Assessing | **Implementing** | Monitoring | Collaborating

Policy Objective

To manage IoT assets across their lifecycle, including hardware and software.

Policy Statements

3.6.1.1 Asset management practices and configuration controls for key information systems shall be made available to consumers.

3.6.1.2 Installation and maintenance of IoT devices shall employ minimal steps and allow consumers to confirm secure set-up.

3.6.1.3 End-of-life strategy shall be developed and followed for IoT products, along with disclosures on duration and end-of-life security and patch support.

3.6.1.4 Proven security solutions, including communications protocols and cryptographic controls, shall be prioritized for IoT products, rather than customized solutions.

3.6 Device Management

3.6.2 Application Security

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To implement the necessary security controls in applications that interface with IoT devices and related components.

Policy Statements

3.6.2.1 Applications shall be developed using a secured software development framework considering all security requirements, including mandatory configurable security, privacy, and location-based controls.

3.6.2.2 Applications shall have secure processing logic, secure input, and output interface along with auditable events and activities.

3.6.2.3 A secure and dedicated gateway shall be utilized for data normalization and processing within IoT networks.

3.6 Device Management

3.6.3 Device Security

Version 1.0

Adoption Lifecycle

Understanding	Assessing	**Implementing**	Monitoring	Collaborating

Policy Objective

To safeguard the IoT environment during the operational lifecycle of the device.

Policy Statements

3.6.3.1 IoT devices shall be designed for security and privacy by default, including encrypted storage and unauthorized access notifications.

3.6.3.2 IoT devices & sensors shall be securely installed and configured to protect the hardware from unauthorized access or tampering.

3.6.3.3 IoT devices shall boot and operate securely while protecting their hardware and software integrity. They shall securely utilize system resources, manage communications, and execute code.

3.6.3.4 Software components in internet-connected devices shall be securely updateable. The need for each update and its application should be made available to consumers. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.

3.7 Network Security

3.7.1 Network Management

Version	1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To ensure the protection of IoT network components.

Policy Statements

3.7.1.1 IoT networks shall be secured using secure ports and protocols with authentication and encryption enabled.

3.7.1.2 Security controls and interoperability shall be considered across different routing networks.

3.7.1.3 IoT networks shall be segregated from the corporate network and micro-segmented for controlled access.

3.7.1.4 Information exchange and infrastructure management of IoT devices and applications shall be restricted and controlled.

3.7.1.5 Unused and default network services, protocols, and ports shall be disabled.

3.7.1.6 IoT solution administration and management shall be conducted via a separate segregated network.

3.8 Security Logging and Monitoring

3.8.1 Audit Logging

Version 1.0

Adoption Lifecycle

Understanding	Assessing	Implementing	Monitoring	Collaborating

Policy Objective

To track and record activities and events in the IoT environment.

Policy Statements

3.8.1.1 IoT services shall have telemetry data enabled for anomaly detection, end-point logging, and endpoint diagnostics.

3.8.1.2 IoT endpoint should log its own behaviour and intermittently upload this log to back-end services.

SECTION 4

IMPLEMENTATION

IMPLEMENTATION

This policy should be read in conduction with the IoT security controls framework attached in the appendix 6.5 which provides control statements supporting the policy requirements.

The Cyber Security Council will work with sector regulators and Emirate lead entities to ensure compliance to the requirements of this policy.

Consumers and service providers are expected to conduct compliance self-assessments against these policy requirements and report back to relevant authorities annually and/or as required.

To bring about the change required to successfully promote IoT security, education, awareness, and communications are needed. The CSC will engage participants to promote IoT security as a national and organizational priority. As processes, procedures, and solutions are built to support the collection, analysis, dissemination, and use of information across organizational boundaries, the CSC will educate and raise awareness to provide a foundational understanding and trust among participants. Furthermore, the CSC will work with participating stakeholders to acknowledge stakeholder organizations that contribute information that leads to innovative cyber solutions and connections among disparate sources of information that enhances the resilience of the UAE’s cyberspace.

SECTION 5

PERFORMANCE MONITORING

PERFORMANCE MONITORING

The National IoT Security Policy outlines measures for monitoring and evaluating progress towards the following objectives:

- Promote transparency and effective management of the IoT devices
- Provide guidance for improvement and taking necessary intervention steps when appropriate.
- Measure the successful implementation of IoT Security requirements by service provider and consumers

SECTION 6

APPENDICES

6.1 Reference Documents

UAE Policies and Standards

The following UAE policies and standards were referenced when defining security requirements set out in this policy.

Authority/Body	Document
CSC	UAE IA Regulation
TDRA	IoT Regulatory Policy
TDRA	IoT Regulatory Procedures
DESC	ICS Standard
DESC	IoT Security Standard
DOH	IoMT Security Standard for Healthcare

6.1 Reference Documents

International Standards

The following table outlines the international sources referenced in this document.

Authority/Body	Document
NIST	800-213 - IoT Device Cybersecurity Guidance for the Federal Government
NIST	8228 - Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
NIST	8259 - Foundational Cybersecurity Activities for IoT Device Manufacturers
NIST	8259A - IoT Device Cybersecurity Capability Core Baseline
ISO/IEC	27402 - IoT security and privacy — Device baseline requirements 21823-1 - Interoperability for IoT systems
European Commission	ANNEXES 1 to 6 – Proposal for a regulation of the European Parliament and of the Council
ISA/IEC	62443 - Standard specifies security capabilities for control system components
IEEE	P2413 - Standards Activities in the Internet of Things (IoT)
IEEE	1451-99 - Standard for Harmonization of Internet of Things (IoT) Devices and Systems
ENISA	WP2017 - Baseline Security Recommendations for IoT
ENISA	WP2018 - Good Practices for Security of Internet of Things
ENISA	WP2019 - Good Practices for Security of IoT

6.2 Abbreviations

Usage	Description
API	Application Programming Interface
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
ICS	Industrial Control System
IoT	Internet of Things
IP	Internet Protocol
IR	Incident Report
IT	Information Technology
ITL	Information Technology Laboratory
LTE	Long-Term Evolution
MAC	Media Access Control
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
ROM	Read-Only Memory
SBOM	Software Bill of Materials
SDK	Software Development Kit
SP	Special Publication
SSDF	Secure Software Development Framework
USB	Universal Serial Bus
UWB	Ultra-Wideband
Wi-Fi	Wireless Fidelity
SDLC	Software Development Life Cycle

6.3 Roles and Responsibilities

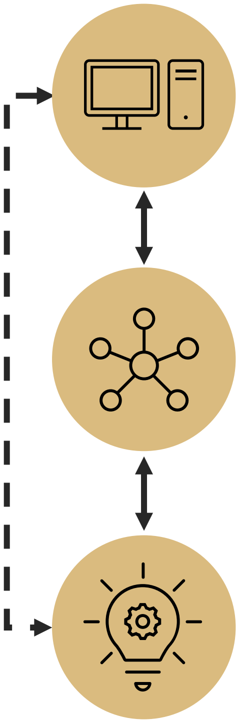
The below table defines the key stakeholders and their respective roles and responsibilities with regards to this policy.

Stakeholder	Roles and Responsibilities
UAE Cyber Security Council (CSC)	- As the custodian of this document, CSC shall: - Issue the National IoT Security Policy and review the document periodically to ensure its relevance. - Coordinate with relevant stakeholders to disseminate the policy to critical sectors and entities. - Oversee the implementation of the provisions of the regulation to ensure compliance with the policy.
Government Entities and National Critical Infrastructure Sectors	- Comply with the requirements outlined in the National IoT Security Policy. - Implement the Policy’s provisions on applicable services. - Exercise due diligence and conduct the appropriate risk assessments outlined in this policy.
IoT Service Providers	- IoT Service Providers are required to comply and meet the security requirements outlined in the policy.
Individuals	- Individuals are not mandated to comply and meet the security requirements outlined in the policy. However, they are advised to use this policy as a guideline if they wish to procure IoT services within the UAE.
IoT Device Manufacturers	- IoT Device Manufacturers are advised to adhere to the requirements set out in this policy if they wish to manufacture or sell IoT devices within the UAE.
IoT Consumers	- To improve their security posture, consumers may choose to adhere to the policy's security requirements.

6.4 Compendium

6.4.1 Internet of Things (IoT) Description

The definition of IoT used in this policy is derived from the IEEE paper "Toward a Definition of Internet of Things (IoT)". According to IEEE, the Internet of Things consists of two primary components, (1) the internet itself and (2) semi-autonomous devices (the "Things") that leverage inexpensive computing power, networking, sensing and actuation capabilities in unique implementations to sense and control the physical world. Being IP based, these devices have the ability to connect to the internet or be deployed in stand-alone IP networks that are not connected to the internet. Additionally, IoT also includes the tools, software and systems (Platforms) that allows for the understanding of actions and analysis of data from these devices.



Devices

Devices within a network are instrumented so they can be addressed individually.

Platform

Devices are interconnected by way of a shared platform, such as a cloud service.

Intelligence

Devices may perform functions adaptively, on their own or with other devices and applications, based on programming and inputs from the physical world.

6.4 Compendium

6.4.2 IoT User perspective

In order to take a collaborative approach to the risks concerning IoT devices and related systems, the UAE Cyber Security Council aims to take a user’s perspective on IoT security risks to enhance the guidance and requirements set out in this policy. The risks outlined in the below section are categorized into the three main groups of users responsible for using IoT devices:

- Consumers
- Enterprises
- Government

Consumers

Consumer use of IoT devices is typically in their home, vehicles, and accessories. These uses can be characterized by the following:

- Share hardware with limited computing power such as internet-connected devices or security systems that may be used by individuals or groups
- Machine-generated insights into user-generated data using cloud-based applications on small screen devices such as tracking physical activities and then using a mobile application to monitor progress
- Connected devices used to share or monitor user data such as IP cameras. These devices can often transmit sensitive information.

6.4 Compendium

6.4.2 IoT User perspective

Enterprises

Enterprises make use of IoT to improve business processes (maintenance, supply chain, inventory) and enhance customer journeys (delivery, retail). They also use other innovative solutions to resolve numerous business challenges. This may also be referred to as Industry 4.0 or the technology-powered Fourth Industrial Revolution.

Enterprises are largely concerned with privacy risks resulting from threats and vulnerabilities in IoT environments, another challenge that they face is managing IoT and cyber risks at an enterprise level.

- Enterprise operations are highly dependent on data availability and integrity; hence, data corruption may have severe consequences. For example, medical devices may be hacked to expose sensitive patient information and ransomware attacks may be used to cause a denial of access and reputational damage.
- Cyber threats can be enhanced in IoT environments and may also introduce vulnerabilities when not adequately managed. As an example, IoT devices may be used to create a botnet of zombified devices used in Distributed Denial of Service (DDoS) attacks.

6.4 Compendium

6.4.2 IoT User perspective

Government

Uses of IoT in government may be more diverse than in enterprises, often used to improve services offered to citizens and improve environmental protection efforts (e.g. monitoring environmental factors and providing e-government services to its citizens)

IoT security risks in government are similar to those in enterprises with additional concerns around the following:

- Complying to minimum baseline security requirements according to regulatory standards and best practices
- Increased threats against critical infrastructure and attacks from nation state actors
- Longevity of IoT device security when products reach end-of-life or end-of-support cycles

الإمارات العربية المتحدة

6.4 Compendium

6.4.3 IoT Innovation

Even though IoT has seen massive adoption in the past few years, device capabilities and innovative solutions are continuously growing. IoT is still very much in its infancy and with new enabling technologies such as 5G and edge processing (processing power on IoT devices) the applications and future innovation of IoT will see major improvements and development in the coming years. With this technology-driven fourth industrial revolution also comes security risks that should be considered in the early stages of these innovations. Though this policy cannot cover every future aspect of IoT security, the goal is to consider some of the emerging changes in the IoT landscape and make an effort to prepare for what is to come.

Some of the trends seen in IoT technology and its surrounding technology are as follows:

- **Connectivity** – Allowing for uninterrupted real-time and near real-time network communications
- **Platforms** – Addressing scalability and security issues while using a standardized approach
- **Federated Architectures** – Enabling distributed devices to be integrated into edge and cloud networks
- **Distributed Ledger Technology (DLT**) – Using blockchain technology for secure transactions on edge devices
- **Artificial Intelligence (AI)** – Integration of AI-enabled devices and systems at different layers of the IoT ecosystem to allow for autonomous decision-making.
- **Tactile Connectivity** – Moving the compute power away from the cloud or cloud edge and onto the devices themselves.