TASMU Security Policy

Document Information

Title: TASMU Security Policy

Policy Reference: TASMU-SEC-POL

Policy Number: 001/2020

Editors: Farrukh Ahmad

Date: 2020-06-18

Published Version: V1.0

Status of This Policy: FINAL DRAFT FOR PUBLICATION

Classification: RESTRICTED ACCESS. Do not distribute.

Policy Abstract

This is the TASMU Security Policy, which provides a criticality assessment mechanism and corresponding minimal, baseline and enhanced security controls to be implemented by the TASMU Service Operator. It also provides IoT controls for applicable TASMU Systems, and finally concludes with controls for Personal Data used in the TASMU Ecosystem, which are applicable to all TASMU Service Operators.

Copyright Notice

Copyright ©2020 by Ministry of Transport & Communications, Government of Qatar. All rights reserved. This document or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the Ministry.

Requirements Language

The key words “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “NOT RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as follows:

- **SHALL**: This word, means that the definition is an absolute requirement of the policy.
- **SHALL NOT**: This phrase, means that the definition is an absolute prohibition of the policy.
- **SHOULD**: This word, or the adjective “RECOMMENDED”, mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT**: This phrase, or the phrase “NOT RECOMMENDED” mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- **MAY**: This word, or the adjective “OPTIONAL”, mean that an item is truly optional.

Normative References

[Common Criteria]

ISO/IEC 15408, Information technology, Security techniques, Evaluation criteria for IT security, 2009, ISO/IEC

[Cybercrime Law]

Qatar Cybercrime Law, Law No.14 of 2014 on Combating Cybercrime, 2014, MOI

[Datagram Transport Layer Security]

Request for Comments: 6347, Datagram Transport Layer Security, January 2012, IETF

[DTPR]

Designing for Digital Transparency in the Public Realm

[FIPS 140-2]

Security Requirements for Cryptographic Modules [includes Change Notices as of 12/3/2002], May 2001, NIST

[IPSEC]

Request for Comments: 5406, Guidelines for Specifying the Use of IPsec Version 2, Feb 2009, IETF

[IPv6]

Request for Comments: 8200, Internet Protocol, Version 6 (IPv6) Specification, July 2017, IETF

[NIAS]

National Information Assurance Standard, Version 3.0, MOTC, **DRAFT**

[OAuth Security]

OAuth 2.0 Security Best Current Practice, draft-ietf-oauth-security-topics-14, Feb 2020, IETF

[OWASP API Security]

API Security Top 10 2019, OWASP

[OWASP Mobile Top 10]

Top 10 Mobile Risks, OWASP

[OWASP Top 10]

Top 10 Web Application Security Risks, OWASP

[PIPP]

Qatar's Personal Information and Privacy Protection (PIPP) Law, Law No 13 of 2016 on protecting personal data

[Qatar National Cryptographic Standard]

Qatar National Cryptographic Standard, Version 1.0, Oct 2019, MOTC

[QUIC Protocol]

draft-ietf-quic-transport-28, QUIC: A UDP-Based Multiplexed and Secure Transport, May 2020, IETF

[RFC4253]

Request for Comments: 4253, The Secure Shell (SSH) Transport Layer Protocol, January 2006, IETF

[RFC8446]

Request for Comments: 8446, The Transport Layer Security (TLS) Protocol, Version 1.3, August 2018, IETF

[SFTP]

Draft-ietf-secsh-filexfer-13.txt, SSH File Transfer Protocol, July 2006, IETF

[TASMU Electronic Commerce and Transaction Policy]

TASMU Electronic Commerce and Transaction Policy, 2020, MOTC

[TASMU Interoperability Policy]

TASMU Interoperability Policy, 2020, MOTC

Informative References

[Azure]

Azure security best practices and patterns, March 2019, Microsoft

[BSIMM]

Building Security In Maturity Model (BSIMM), Version 10, BSIMM

[Cloud Controls Matrix (CCM)]

Cloud Controls Matrix Version 3.0.1, March 2019, Cloud Security Alliance

[TS 103645]

ETSI TS 103 645, Cyber Security for Consumer Internet of Things, DTS/CYBER-0039, Version 1.1.1., February 2019, ETSI

[GSMA IoT Security Guidelines Endpoint]

IoT Security Guidelines Endpoint Ecosystem, Version 2.2, 29 February 2020, GSMA

[GSMA IoT Security Guidelines for IoT Service Ecosystem]

IoT Security Guidelines for IoT Service Ecosystem, Version 2.229, February 2020, GSMA

[IMDA IoT Cyber Security Guide]

IMDA IoT Cyber Security Guide V1, Mar 2020, Info-communications Media Development Authority, Singapore

[NIST 800-63B]

NIST Special Publication 800-63B, Digital Identity Guidelines Authentication and Lifecycle Management, June 2017, NIST

[Qatar 2022 Cybersecurity Framework]

Qatar Cybersecurity Framework, Version 1.0, August 2018, SCDL

[Qatar Cloud Security Standard]

Cloud Security Standard, V0.9, MOTC, **DRAFT**

[OAuth 2.0]

Request for Comments: 6749, The OAuth 2.0 Authorization Framework, Oct 2012, IETF

[SSQA]

Software Security and Quality Assurance, Levels 1-3, Oct 2018, Q-CERT

Contents

Definitions

The definitions used in this policy have been written to provide contextual clarity and where necessary specificity, and should not be interpreted to be contradictory to any laws in the State of Qatar.

[Analytics Data]

Refers to the collection of data that is used to support decision making and/or research in TASMU Systems:

- (E) Sector Platforms, and
- (F) Central Platform

[Anonymisation]

The process in which Personal Data is altered in such a way that it irreversibly prevents the identification of the Subscriber. Personal Data which has been irreversibly anonymised ceases to be Personal Data.

[Advanced Persistent Threat]

An advanced persistent threat (APT) is a stealthy computer network threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period.

[Consent]

Consent is an affirmative, freely given and informed agreement of a Subscriber for the Processing of their data. Natural persons ("individuals") must be able to control the Processing of their Personal Data within the TASMU Ecosystem and where necessary provide explicit Consent, which signifies their agreement, expressly confirmed in words, to specific Processing.

[Cyber Resilience]

This refers to the ability to continuously deliver the intended outcome, protecting data assets despite adverse cyber events.

[Internet of Things]

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, uniquely identified with the ability to transfer data over a network to Sector Platforms and/or the Central Platform.

[IoT Endpoint]

An IoT Endpoint is a physical computing device that performs a function or task as part of a TASMU Smart Service.

[Memorized Secret Authenticators]

A Memorized Secret authenticator, commonly referred to as a password or, if numeric, a PIN, is a secret value intended to be chosen and memorized by the user. Memorized secrets need to be of sufficient complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value.

[Multi-Factor Cryptographic Device]

A multi-factor cryptographic device is a hardware device that performs cryptographic operations using one or more protected cryptographic keys and requires activation through a second authentication factor.

[Multi-Factor One Time Password]

A multi-factor One Time Password (OTP) device generates OTPs for use in authentication after activation through an additional authentication factor. This includes hardware devices and software-based OTP generators installed on devices such as mobile phones.

[Personal Data]

Data of a natural person ('individual') which is specifically identifiable or can be reasonably identified either by the Personal Data itself or through a combination of other data. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[Presentation Attack Detection]

Automated determination of a presentation attack. A subset of presentation attack determination methods, referred to as liveness detection, involve measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, in order to determine if a biometric sample is being captured from a living subject present at the point of capture.

[Privacy By Design]

This is the integration or 'bake in' of Personal Data protection (including defaulting to privacy protection) into processing activities, business practices and information systems from the design stage right throughout their lifecycle.

[Privacy Notice]

A statement made to a data subject that describes how the organisation collects, uses, retains and discloses Personal Data. A privacy notice is sometimes referred to as a privacy statement, a fair processing statement or sometimes a privacy policy.

[Processing]

Any operation or set of operations which is performed on data, such as collecting; recording; organizing; storing; adapting or altering; retrieving; consulting; using; disclosing by transmission, dissemination or otherwise making the data available; aligning or combining data, or blocking, erasing or destroying data. Not limited to automatic means.

[Production]

This refers to the environment, system and/or data of a TASMU System that provides a "live" service to Subscribers. This includes pre-production and live disaster recovery environments and is in contrast to non-production environments such as test or development which are not used for "live" services.

[Software Security Development Lifecycle]

The security development lifecycle is a software development process that helps developers build more secure software, from the initial conception, and address security compliance requirements while reducing development cost.

[Special Personal Data]

Any Personal Data that includes the special nature data relating to:

- Children
- Spousal Relations
- Health, physical or psychological condition
- Religious Beliefs
- Racial or ethnic origin
- Criminal history

[Services Data]

Refers to the data that is collected, generated, and stored within TASMU Systems related to Smart Devices (H) or Subscribers. Examples include application data, history of service usage, search activities, cookies, transaction records, traffic and location data, etc.

[Static Analysis]

Static analysis, also called static code analysis, is a method of computer program debugging that is done by examining the code without executing the program. The process provides an understanding of the code structure, and can help to ensure that the code adheres to industry standards.

[Subscriber]

An organisation or individual who utilises a TASMU Smart Service. They subscribe to and are authenticated by the TASMU Ecosystem. In some contexts they may be referred to as consumers.

[TASMU Ecosystem]

This is the Smart Qatar (TASMU) platform and any TASMU Smart Service that is either connected to this Central Platform or is branded as TASMU compliant. Refer to (A) in the TASMU Conceptual Diagram.

[TASMU Service Operator]

This is the owner and operator of the TASMU System, who has overall responsibility for its secure, compliant operation.

[TASMU Smart Nation Regulator]

The entity in the State of Qatar who regulates the TASMU Ecosystem. It is responsible for drafting, promoting, governing, updating, monitoring compliance with, and enforcing this policy.

[TASMU Smart Service]

A TASMU Smart Service is a national service, leveraging one or multiple technologies, to resolve an identified challenge or enable a desired outcome and that operates in the TASMU Ecosystem. Collectively, they focus on detailing and contextualizing services relevant for the State of Qatar.

[TASMU System]

This is owned by the Service Operator and refers to any of the following elements from the TASMU Conceptual Diagram:

- (C) Any TASMU Smart Service
- (D) Any networking between platforms and (C)
- (E) Sector data analytics platforms
- (F) Central data analytics platform
- (G) Any networking between platforms and devices (H)
- (H) Any smart devices
- (I) The TASMU Control Centre
- (K) Security Management of the TASMU Ecosystem
- (L) Operations Management of the TASMU Ecosystem

[TASMU Root of Trust]

The authoritative entity for the TASMU Ecosystem is the Qatar PKI IoT CA.

[Trust Anchor]

This is the authoritative entity for which trust is assumed and not derived. It will be issued by the TASMU Root of Trust. In X.509 architecture, a root certificate would be the trust anchor from which the whole chain of trust is derived.

[Trusted Computing Base]

The Trusted Computing Base (TCB) is a suite composed of hardware, software, and protocols that ensures the integrity of the IoT Endpoint, performs mutual authentication with network peers, and manages communications and application security.

[Virtual Components]

These are components such as virtual machines, containers, virtual network appliances/functions, serverless functions and virtual management systems.

1. Introduction

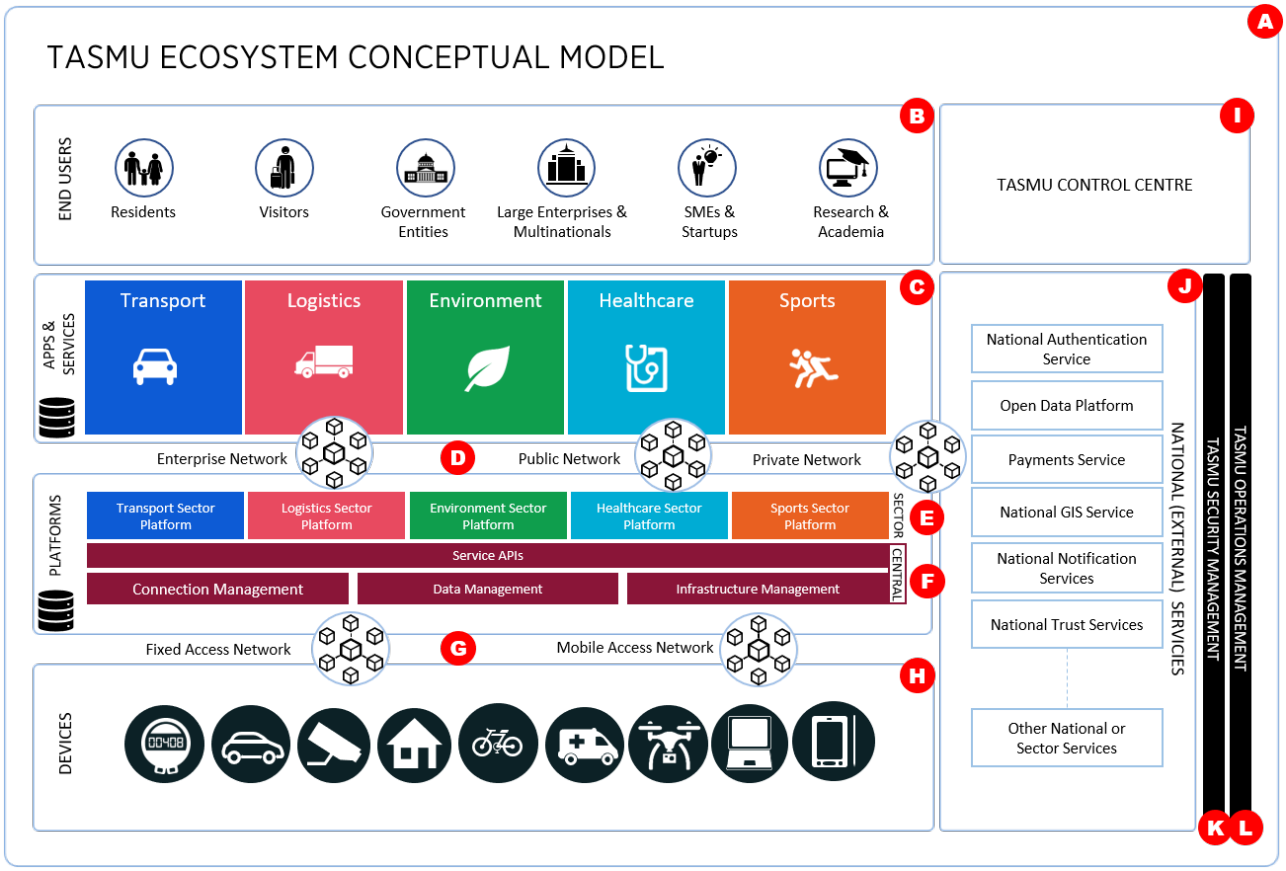
1.1 TASMU

The Qatar National Vision 2030 aims to "transform Qatar into an advanced society capable of achieving sustainable development." TASMU, or the Smart Qatar program, is a digital response to the goals that have been set out in the National Vision 2030. It is about harnessing technology and innovation to improve quality of life and help drive economic diversification.

TASMU aims to leverage innovative applications of technologies to provide targeted services for residents, businesses and government across priority sectors. The foundation of this whole-of-nation effort relies on the ability to collect and manage vast amounts of data, share and open it up for spawning broad-based innovation and entrepreneurship within a set of defined rules and regulations. This is then processed and analysed by different actors for the build-up of innovative services and applications. As such, governance of TASMU on a national level has been designed to harmonize efforts across the different actors and drive Smart Qatar development with a key focus on ensuring efficiency and building resilience and interoperability.

TASMU Smart Services are services designed to solve evolving challenges targeted constituents (people, businesses, or government) face, leveraging technology and innovation. TASMU Smart Services cut across industry sectors focusing on human, social, economic, and environmental development. They can be focused on providing convenience or entertainment, or could address critical needs such as national safety and security. As such, the type of information they leverage can range from publicly open to sensitive or private information.

The policy covers the TASMU Ecosystem and interactions with it. The diagram below shows the TASMU Ecosystem in the context of this policy.



Only the following elements are within the scope of this policy:

- A: is the overall ecosystem
- B: is the end-user ecosystem
- C: is the TASMU Smart Services and services ecosystem
- D: are the network connections from the Central Platform, over enterprise, public and private networks
- E: are the sector data analytics platforms ('Sector Platforms')
- F: is the central TASMU data analytics platform ('Central Platform')
- G: is the Internet of Things (IoT) access network, either over fixed or wireless networks
- H: is the IoT devices ecosystem
- I: is the TASMU Control Centre
- J: is the ecosystem of national services/platform that connects to the TASMU Central Platform and (C) above
- K: is the TASMU security management ecosystem
- L: is the TASMU operations ecosystem

1.2 TASMU Security Policy

To secure the TASMU Ecosystem, the TASMU Security Policy protects the confidentiality, integrity, and availability of information entering, residing or exiting the ecosystem and safeguards the ecosystem operations. It also ensures that the TASMU Ecosystem has mechanisms to gather cyber intelligence and respond to cyber incidents.

This policy provides minimal, baseline and enhanced controls, that are applicable generally, and specific controls covering Internet of Things (IoT) and Personal Data, which have particular applicability.

The objective of this policy is to ensure the TASMU Ecosystem is secure, trustworthy, and all entities operating within it, achieve a level of security commensurate to their criticality.

This TASMU Security Policy is regulated by the TASMU Smart Nation Regulator.

1.3 Compliance

All TASMU Service Operators SHALL:

1. Comply with this policy where they operate a TASMU System or provide a TASMU Smart Service to a Subscriber, prior to operating in the TASMU Ecosystem and on a regular basis as directed by the TASMU Smart Nation Regulator.
2. Ensure that this policy is applied to all aspects of the TASMU System, whether that is maintained or operated by a third party, prior to operating in the TASMU Ecosystem.
3. Ensure this policy is considered in conjunction with the specific TASMU Smart Service sector policy issued by the TASMU Smart Nation Regulator or the sector regulator, which will cover specific requirements of the TASMU Smart Service.
4. Allow for an independent audit to check compliance, as and when necessary, or as directed by the TASMU Smart Nation Regulator.
5. Undertake an initial assessment using the §Criticality Assessment to determine the level of compliance required for their TASMU System.

2. Criticality Assessment

Before any TASMU System within the TASMU Ecosystem can comply with this policy, the TASMU Service Operator SHALL assess their criticality within the TASMU Ecosystem using the methodology specified in this section. This criticality will help to determine the impact on the TASMU Ecosystem due to an attack on its Cyber Resiliency, and will help determine which set of security controls will be applicable for that TASMU System.

2.1 Criticality Factors

To determine criticality of the TASMU System, the following factors need to be evaluated for it:

- **Population Served**: The number of people served by the TASMU System, as a percentage of the total users of the TASMU Ecosystem
- **Service Frequency**: This is a proxy for understanding how critical the TASMU System is. It is measured by the peak frequency of service usage on a daily basis
- **Economy**: Annual revenue generated/forecasted by the TASMU Smart Service (QAR Millions)
- **Scope**: The number of TASMU industry sectors served by the TASMU System
- **Personal Data**: Whether the TASMU System processes Personal Data. This covers Personal Data with Special Personal Data as defined in the PIPP
- **Threat**: Where there is a highly perceived or known threat to the TASMU System due to its core function [1].

Impact Factor (weight)	High (5)	Medium (3)	Low (1)
Population (20)	>80%	20%-80%	<20%
Service Frequency (20)	All the time	10-1000	<10
Economy (20)	>100	10-100	<10
Scope (10)	All	2-3	1
Personal Data (20)	Yes [2]	Yes	No
Threat (10)	Yes	N/A	N/A

2.2 Criticality Calculation & Policy Application

Using the Criticality Worksheet, determine the rating for the TASMU System and apply the following:

- For any TASMU System with a criticality value of 100, all minimal security controls SHALL apply
- For any TASMU System with a criticality value between 100-250, all minimal and baseline security controls SHALL apply
- For any TASMU System with a criticality value > 250, all minimal, baseline and enhanced security controls SHALL apply
- For any TASMU System with any IoT devices the additional § IoT Controls SHALL apply
- For any TASMU System processing Personal Data, the additional § Personal Data Controls SHALL apply

Minimal controls are indicated by a [M]. Baseline controls are indicated by a [B]. Enhanced controls are indicated by a [E].

These controls are additive. As an example, if your TASMU System has a criticality > 250, and includes IoT devices and is processing Personal Data, all controls in this policy apply to you.

3. Minimal, Baseline & Enhanced Controls

The TASMU Service Operator is responsible for ensuring the applicable controls are implemented.

3.1 Governance

The TASMU Service Operator SHALL:

1. [M] Have a defined, approved and published Information Security policy for the TASMU System.
2. [M] Review the Information Security policy at least annually or if any significant change takes place.
3. [M] Undertake vulnerability scanning and penetration testing, by an independent third party, annually or if any significant change takes place in the TASMU System's infrastructure, systems, services or significant new, applicable, vulnerabilities are reported.
4. [M] Take adequate measures to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e. issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.
5. [B] Ensure all staff, contractors, and third parties are subject to background verification, proportional to the data sensitivity to be accessed, the business requirements, and acceptable risk.
6. [B] Develop and implement adequate segregation of responsibilities for sensitive security processes and tasks.
7. [E] Ensure they are compliant with the National Information Assurance Standard.

3.2 Business Continuity

1. [B] There SHALL be a defined and documented method for determining the impact of any disruption to a TASMU System.
2. [B] A consistent unified framework for business continuity planning and plan development SHALL be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. A Business Continuity Plan (BCP) for critical business processes based on Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each process, including dependent systems and data, SHALL be developed and implemented.

3. [B] Business continuity and security incident response plans SHALL be subject to testing annually or upon significant organizational or environmental changes. Incident response plans SHOULD involve impacted customers and other business relationships that represent critical intra-supply chain business process dependencies.

4. [E] Data centre utilities services and environmental conditions (e.g. water, power, temperature and humidity controls, telecommunications, and internet connectivity) SHALL be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.

5. [E] Based on a risk assessment and as applicable, physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster SHALL be anticipated, designed, and have countermeasures applied.

3.3 Change Management

1. [M] All changes to an operational TASMU System SHALL be planned, authorized, tested and assessed for security impact, before implementation.

2. [B] A defined quality change control and testing process (e.g. ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services SHALL be implemented.

3. [B] Policies and procedures SHALL be established for managing the risks associated with applying changes to:

    a. business-critical or TASMU System impacting (physical and virtual) applications and system-system interface (API) designs and configurations
    b. infrastructure network and systems components

4. [E] Technical measures SHALL be implemented to provide assurance that all changes directly correspond to a registered change request and/or a business-critical customer authorization request as per the agreement (e.g. SLA) prior to deployment.

3.4 Data Protection

1. [M] Backup, archiving and recovery processes for the TASMU System SHALL be clearly defined.

2. [M] Data related to electronic commerce (e-commerce) that traverses public networks SHALL be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data. The TASMU Electronic Commerce and Transaction Policy provides more details of this.

3. [B] An inventory of data flows for data that is resident (permanently or temporarily) within the TASMU System's geographically distributed (physical and virtual) applications, infrastructure network and systems components and/or shared with other third parties SHALL be maintained.

4. [B] Production data SHALL NOT be replicated or used in non-production environments. Any use of Personal Data in Non-Production environments is prohibited.

5. [B] Media with any TASMU related data SHALL be encrypted, sanitized (or destroyed) when it is taken out of service. This SHALL include a wiping solution or destruction process that renders recovery of information impossible which complies with NIAS for scrubbing of sensitive data elements.

6. [E] Policies and procedures SHALL be established for the labelling, handling, and security of data and objects which contain data.

7. [E] Data classification SHOULD be undertaken to ensure suitable protection for the following types of data:

    a. Personal Data
    b. Services Data
    c. Analytics Data

3.5 Physical Security

1. [B] Physical assets SHALL be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time SHALL be maintained and updated regularly, and assigned ownership.

2. [B] Physical security perimeters (e.g. fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols), based on a risk assessment, SHALL be implemented to safeguard sensitive data and information systems.

3. [B] Physical access to information assets and functions by users and support personnel SHALL be restricted. Ingress and egress to secure areas SHALL be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.

4. [E] Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises SHALL be monitored, controlled and, where possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.

3.6 Security Logging

1. [M] Logging SHALL be enabled on a TASMU System's infrastructure, data processing equipment and applications associated with the access, transmission, processing, security, storage and/or handling of TASMU information.

2. [M] Logs SHALL capture:

    a. date and time of event
    b. authentication activity
    c. privileged activity including sanitisation, maintenance, system recovery, special and out of hours activities
    d. security impacting change activities
    e. system startup and shutdown
    f. component or system failures
    g. DNS, DHCP, & security device(s) activities
    h. Any access to Special Personal Data

3. [M] Logs SHALL be retained for a minimum of 120 days and a maximum period determined by criticality assessments and sector specific laws and regulations.

4. [E] Anomalies that indicate adversarial behaviour e.g. increased network traffic, increased network traffic in an odd direction (especially egress), abnormal CPU utilization, abnormal changes in system time on a particular host, etc. SHALL be detected, logged and investigated.

3.7 Security Incident & Threat Management

TASMU Service Operators SHALL:

1. [M] Have the capability and processes to triage security-related events and ensure timely and thorough incident management.

2. [M] Ensure they, and any supporting third party can report all information security events in a timely manner. Any security incident that impacts the Cyber Resilience of the TASMU System SHALL be reported to the TASMU Smart Nation Regulator and competent authorities.

3. [M] Ensure they abide by Qatar's Cyber Crime Law by:

    a. keeping Subscriber information for one (1) year for evidentiary purposes
    b. keeping on a temporary and urgent basis configuration data, traffic data and content information for a period of 90 days renewable upon a request by the competent body
    c. cooperating with and helping the competent authority with collecting and recording electronic data or information and traffic data if ordered by judicial authorities
    d. promptly reporting to, and supporting, the competent authority when any malicious activity, including intrusions, data compromises, or espionage attacks, are detected

4. [E] Ensure they have proper forensic procedures, including chain of custody, for evidence gathering.

5. [E] Ensure that if they manage TASMU Systems D, E, F, G or I (see TASMU Conceptual Diagram) they:

    a. have robust threat intelligence, to aggregate, correlate, and analyse threat data from multiple sources in real time to support defensive actions
    b. ensure their threat data is contextualised by incorporation of Whois information, reverse IP lookup, website content analysis, and name servers
    c. have clear processes and resources to monitor and act on the threat intelligence
    d. have Advanced Persistent Threat (APT) detection capabilities

3.8 Supply Chain Management, Transparency, and Accountability

1. [B] Supply chain agreements (e.g. SLAs) between TASMU Service Operators and any supporting third party SHALL incorporate at least the following mutually-agreed upon provisions and/or terms:

    a. information security requirements, including governance, risk management, assurance and legal, statutory and regulatory compliance obligations
    b. assessment and independent verification of compliance with agreement provisions and/or terms including this policy
    c. reporting of any security incidents

2. [B] Third-party service providers SHALL demonstrate compliance with this policy and SHOULD be audited.

3. [E] Third-party service providers SHALL be validated to ensure that they do not pose any strategic/political risk to the State of Qatar.

3.9 Infrastructure & Asset Management

This section is specifically for those TASMU Systems providing infrastructure for the TASMU Ecosystem or managing their own infrastructure.

1. Wireless 802.11x networks SHALL be secured by:

    a. [M] ensuring guest networks are segregated from the main network
    b. [M] using strong wireless security protocols such as WPA2 and EAP-TLS
    c. [E] using wireless intrusion detection system (WIDS) and a wireless intrusion prevention system (WIPS) on every network
    d. [E] using AP-TLS certificate-based methods (or better) to secure the entire authentication transaction and communication

2. [M] An inventory of all Virtual Components and data assets that formulate the TASMU System SHALL be maintained.

3. [M] The baseline configuration of the TASMU System SHALL be maintained to support roll-back or forensic analysis.

4. [M] The following or more secure communications protocols SHALL be used internally and for data ingress/egress from the TASMU System:

    - **web traffic:** TLS v1.3 (128+ bits) [RFC8446]

- **file transfers:** SFTP [SFTP]
- **remote access:** SSH v2 [RFC4253] or IPSEC [IPSEC]

5. [M] Access to all Virtual Components, including administrative consoles SHALL be restricted to personnel based upon the principle of least privilege and follow the policies outlined in § Identity & Access Management.

6. [B] The integrity of all Virtual Components SHALL be ensured at all times. Any changes made to the images of Virtual Components SHALL be logged and an alert raised regardless of their running state (e.g. dormant, off, or running) to customers.

7. [B] Image registries SHALL be restricted to approved sources for the TASMU Ecosystem.

8. [B] A reliable external time source SHALL be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.

9. [B] Network environments and Virtual Components instances SHALL be designed and configured to restrict and monitor traffic between trusted and untrusted connections.

10. [B] All operating systems SHALL be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.

11. [B] Production and non-production environments SHALL be separated to prevent unauthorized access or changes to information assets.

12. [B] Separate logical security zones, including Demilitarized Zones for externally facing systems, SHALL be used to isolate the following elements (see TASMU Conceptual Diagram):

    - (C) Any TASMU Smart Service
    - (E) Sector Platforms (each in a separate zone)
    - (F) Central Platform
    - (I) The TASMU Control Centre
    - (K) Security Management of the TASMU Ecosystem
    - (L) Operations Management of the TASMU Ecosystem

    This will ensure that provider and customer user access is appropriately segmented from all others.

13. [B] Physical and virtual networks SHALL be protected by:

    a. perimeter firewalls implemented and configured to restrict unauthorized traffic
    b. web application firewalls (WAFs) at public ingress points
    c. deploying intrusion detection and prevention capabilities
    d. implementing network level access controls
    e. implementing network security devices

14. [B] Dedicated private network connections and/or encrypted links SHOULD be used for any sensitive or backend system connections.

15. [E] Network architecture diagrams SHALL clearly identify high-risk environments and data flows that may have legal or regulatory compliance impacts. Technical measures SHALL be implemented and SHALL apply defence-in-depth techniques (e.g. deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g. MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.

3.10 Software Security

TASMU Service Operators SHALL validate the following for both bespoke software or Commercial-Of-The-Shelf (COTS) products used in their TASMU Systems:

1. [M] Identify implementations of all open-source components, including those used in COTS products and any dependencies that may be dated or present a security concern.
2. [M] Implement one or more black-box security testing tools as part of the QA/testing process, including testing against [OWASP] Top 10 and/or [OWASP Mobile Top 10 as applicable.
3. [M] Implement both syntactical and semantic level input validation.
4. [B] Establish a suitable Software Security Development Lifecycle (SSDL) methodology and tailor this to the requirements of the development process.
5. [B] Implement a process for architectural security analysis and apply this to the design review process.
6. [B] Use code protection to protect intellectual property and make exploit development harder (e.g. anti-tamper, debug protection, anti-piracy features, runtime integrity).
7. [B] Incorporate static analysis and fuzz testing into the code review process to make the review more efficient and consistent.
8. [E] Adopt Secure Coding Standards for each programming language or platform that the organization utilizes to enhance manual and automated testing activities.
9. [E] Undertake code reviews of security functions within the SSDL.
10. [E] Implement automated code review to identify dangerous code (e.g. back doors, logic bombs, time bombs, nefarious communication channels, obfuscated program logic, and dynamic code injection, etc.).
11. [E] Automate verification of operational infrastructure security using machine-readable policies and configuration standards to automatically detect and report on infrastructure that does not meet expectations.

3.11 Application Interface Security and Portability

1. [M] Application Programming Interfaces (APIs) SHALL be designed, developed, deployed, and tested in accordance with leading industry standards and adhere to applicable legal, statutory, or regulatory compliance obligations. Security verification against [OWASPAPI] SHOULD be undertaken.
2. [B] Data input and output integrity routines (i.e. reconciliation and edit checks) SHALL be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.
3. [B] TASMU infrastructure providers SHALL use open and published APIs and these SHALL be used to ensure support for interoperability between components and to facilitate migrating applications. See the TASMU Interoperability Policy for further policy guidance.
4. [B] The TASMU Service Operator SHALL ensure all structured and unstructured data is available to the customer and provided to them upon request in an industry-standard format (e.g. .doc, .xls, .pdf, logs, and flat files).
5. [B] The TASMU Service Operator SHALL use secure (e.g. non-clear text and authenticated) standardized network protocols (see §Infrastructure & Asset Management) for the import and export of data and to manage the service, and make available a document to customers detailing the relevant interoperability and portability standards that are involved.
6. [B] TASMU infrastructure providers SHALL use industry-recognized Virtual Components and have documented custom changes to them if necessary.

7. [E] Policies and procedures SHALL be established and maintained in support of data security to include confidentiality, integrity, and availability across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.

3.12 Identity & Access Management

1. [M] Any TASMU System that is requiring positive identification of a natural person, resident in Qatar, SHALL use the National Authentication Service (Tawtheeq). For any other natural person, including guests, the controls specified in federated identification §3.12(7) apply.

2. [M] Privileged access to the TASMU System SHALL use one of the following authenticators:

    a. Multi-factor OTP authenticators
    b. Multi-factor cryptographic devices

3. [M] Verifiers of privileged access SHALL:

    a. ensure the symmetric keys used by authenticators are strongly protected against compromise
    b. use approved encryption and an authenticated protected channel when collecting the OTP in order to provide resistance to eavesdropping and MitM attacks
    c. ensure that if the authenticator output or activation secret has less than 64 bits of entropy, the verifier implements a rate-limiting mechanism that effectively limits the number of failed authentication attempts (e.g. CAPTCHA, timeouts, IP white listing, adaptive techniques, etc.)

4. [M] Where any Memorized Secret Authenticators that are used either in conjunction with (1) or (2) above, or by themselves, they SHALL:

    a. be at least 12 characters in length if chosen by the Subscriber
    b. where the TASMU System generates the secret, be chosen randomly, time limited, and be at least 6 characters in length and MAY be entirely numeric
    c. not impose additional complexity requirements for memorized secrets on Subscribers

5. [M] Verifiers of Memorized Secret Authenticators SHALL:

    a. prevent the Subscriber to store a “hint” that is accessible to an unauthenticated claimant
    b. compare (and reject) prospective secrets against, at least, the following:

        - passwords obtained from previous breach databases
        - dictionary words
        - repetitive or sequential characters (e.g. ‘aaaaaa’, ‘1234abcd’)
        - context-specific words, such as the name of the service, the username, and derivatives thereof

    c. implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the Subscriber’s account (e.g. CAPTCHA, timeouts, IP white listing, adaptive techniques, etc.)
    d. use approved encryption and an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks
    e. store memorized secrets in a form that is resistant to offline attacks. Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function

6. [M] Session bindings between the TASMU System and a Subscriber SHALL be:

    a. generated by the session host during an interaction, typically immediately following authentication
    b. erased or invalidated by the session subject when the Subscriber logs out
    c. sent to and received from the device using an authenticated protected channel
    d. reauthenticated at least once per 12 hours, regardless of user activity or at least after 15 minutes (or longer) of inactivity. The verifier MAY prompt the user to cause activity just before the inactivity timeout
    e. prevent fall back to an insecure transport, such as from https to http, following authentication

7. [M] For federated identification in the TASMU Ecosystem the following applies:

    a. use of specific Identity Providers (IdPs), apart from (1) above, SHALL be authorised by the TASMU Smart Nation Regulator
    b. the IdP SHALL ensure that all assertions are cryptographically protected with a digital signature
    c. the IdP SHALL ensure that it follows all relevant privacy requirements, specified in § Personal Data Controls. Specifically, positive Consent SHALL be obtained from the Subscriber before any attributes about the Subscriber are transmitted to any Relying Party (RP)
    d. a Subscriber's information SHALL be transmitted between IdP and RP only for identity federation transactions or support functions such as identification of compromised accounts. A Subscriber's information SHALL NOT be transmitted for any other purposes.
    e. the IdP SHALL, by default, mask sensitive information displayed to the Subscriber. The IdP SHALL provide mechanisms for the Subscriber to temporarily unmask such information in order for the Subscriber to view full values
    f. the IdP SHALL provide effective mechanisms for redress of applicant complaints or problems
    g. if the protocol in use allows for optional attributes, the Subscriber SHALL be given the option to decide whether to transmit those attributes to the RP
    h. protocols requiring the transfer of keying information SHALL use a secure method during the registration process to exchange keying information needed to operate the federated relationship
    i. TASMU Systems using OAuth 2.0 for OpenID Connect, SHOULD implement the recommendations outlined in [OAUTHSEC]

8. [M] User access to diagnostic and configuration ports SHALL be restricted to authorized individuals and applications.

9. [M] All user accounts SHALL be disabled if they have been inactive for more than ninety (90) days.

10. [M] Individual accounts SHALL be provisioned for system administrators for administrative tasks, unless a mechanism for temporary elevated privilege is used instead.

11. [B] Where biometrics are used (not as part of multi-factor authentication with a physical authenticator):

    a. an authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier SHALL be established and the sensor or endpoint SHALL be authenticated prior to capturing the biometric sample from the claimant
    b. the biometric system SHALL implement Presentation Attack Detection (PAD)
    c. the biometric system SHALL NOT allow more than ten (10) consecutive failed attempts if PAD is implemented

12. [B] Revocation of the binding of authenticators SHALL be carried out promptly when an identity ceases to exist (e.g. Subscriber's death, discovery of a fraudulent Subscriber), when requested by the Subscriber, or when the TASMU Service Operator determines that the Subscriber no longer meets its eligibility requirements.

3.13 Cryptography

1. [M] The TASMU System SHALL ONLY incorporate cryptographic algorithms compliant to the [Qatar National Cryptographic Standard].

2. [B] Key management SHALL be clearly defined using the Qatar National Cryptographic Standard, covering the following functions:

    a. Key Custodians' Roles and Responsibilities
    b. Key Generation
    c. Dual Control and Split Knowledge
    d. Secure Key Storage
    e. Key Usage
    f. Secure Key Distribution and in Transit
    g. Key Backup and Recovery
    h. Periodic Key Status Checking
    i. Key Compromise

j. Key Revocation and Destruction
k. Key Escrow
l. Audit Trails and Documentation

3. [B] Where HSMs are used by the TASMU Service Operator they SHALL be certified to at least FIPS 140-2 Level 3 or Common Criteria EAL 4.

4. [B] Any digital certificate used in the TASMU System SHOULD be issued by a licensed Certificate Service Provider (CSP) in Qatar.

5. [E] Master keys stored in the cloud SHALL be stored in Hardware Security Modules (HSM), but MAY be maintained by the cloud consumer or trusted key management provider.

4. IoT Controls

The following controls apply to all TASMU Systems with IoT Endpoints functioning in the TASMU Ecosystem.

4.1 Minimal Controls

1. [M] TASMU Systems SHALL use the defined Root of Trust, together with a TASMU IoT Trust Anchor. Online revocation, where applicable, SHOULD be used.

2. [M] For publicly accessible IoT services, the following protections SHALL be used to secure the infrastructure. Refer to §Infrastructure & Asset Management for more details.

   a. DDoS-resistant infrastructure
   b. Load-Balancing infrastructure
   c. Traditional Firewalls

3. [M] Secure, proven transport layer protocols SHALL be used to transfer data within and between systems, ensuring authentication of network peers, confidentiality of data and integrity of messages. Examples include:

   - DTLS
   - TLS
   - QuiC
   - IPv6

4. [M] IoT Endpoints SHALL NOT use hard-coded, default passwords or have back-door passwords. The rules specified in §Identity & Access Management SHALL apply.

5. [M] Application images on IoT Endpoints SHALL be cryptographically signed, which can be verified before their execution.

6. [M] Over The Air (OTA) application updates SHALL be designed to ensure they are fail safe, integral and can not be intercepted or modified.

7. [M] Where the TASMU Service Operator is providing consumer IoT devices the following additional controls apply:

   a. all software components in consumer IoT devices SHALL be securely updateable, in a timely manner
   b. the IoT device SHALL be supported, and receive any necessary security updates for at least three (3) years if it is a component of a TASMU Smart Service with a criticality < 250. For any other TASMU Smart Service security updates SHALL be provided until it reaches end of life
   c. the consumer SHALL be informed that an update is required
   d. the consumer SHALL be provided the ability to easily erase all Personal Data from the device (see Personal Data Controls for more details)
   e. credentials and security-sensitive data SHALL be stored securely within services and on devices
   f. hardware SHOULD NOT unnecessarily expose attack surfaces and code SHOULD be minimised, including removal of unused software

g. installation and maintenance of IoT devices SHALL employ minimal steps and should follow security best practice on usability

8. [M] The physical security requirements of IoT Endpoints SHALL be risk assessed on a case by case basis, depending on the use case of the IoT Endpoints, and be covered in the specific TASMU Smart Service policy. The risk assessment SHOULD include the following considerations:

    - How will the device be used? (e.g. single/multiple purpose, embedded, single user/customer or multiple users, private or commercial use)
    - What environments will the device be used in, including any specific Qatari environmental conditions? (e.g. inside or outside, stationary or moving, public or private, movable or immovable, extreme or specific physical and weather conditions)
    - How long is the device expected to be used for? (e.g. a few hours, or several years)
    - What dependencies on other systems will the device likely have?
    - How might attackers misuse and compromise the device?
    - What other aspects of device use might be relevant to the device's cyber security risks? (e.g. operational characteristics of the device that may have safety, privacy, or other implications for consumers)

4.2 Baseline Controls

1. [B] A Trusted Computing Base (TCB) SHALL be used which uses strong cryptography, either in the form of unique symmetric keys, certificates, or public keys, compliant to the Qatar National Cryptographic Standard. Perfect Forward Secrecy SHOULD be used.

2. [B] The TCB SHALL protect all sensitive data including keys, credentials, codes/firmware, Personal Data, inputs/commands and sensing data, etc. Access to this data SHALL require assurance and/or verification that it originates from authentic sources, and be protected from tampering, modification and/or disclosure to unauthorised parties.

3. [B] A TCB SHALL use a proven random number generator.

4. [B] The TCB SHALL provide at least the following security functions:

    - **Bootstrap process:** ensures a consistent way to load and execute an application on a reliable, high quality, and secure platform
    - **Executable image validation:** secures the IoT Endpoint by cryptographically verifying each executable image to be loaded and executed by the device
    - **Mutual authentication of peers:** helps provide a root of trust for the authentication of components, and cryptographically authenticates itself to peers
    - **Provisioning and personalisation:** ensures that an IoT Endpoint has an identity that is cryptographically unique from every other IoT Endpoint of its type

5. [B] The TCB SHALL use Personalised Keys ensuring each IoT Endpoint can be uniquely identified and communicated to.

6. [B] The TCB SHALL use secure, well defined protocols for the security functions. Examples are:

    a. oneM2M SM UICC
    b. IoT SAFE
    c. Generic Bootstrapping Architecture (GBA)

7. [B] The TCB SHOULD ONLY be accessible from privileged applications running on the IoT Endpoint. A TCB interface SHOULD NOT be accessible from an unprivileged or untrusted (third party) application running on the IoT Endpoint.

8. [B] IoT Endpoints SHALL ensure that they have security logging capability, that can be centrally uploaded on regular intervals. See §Security Logging for further details.

9. [B] IoT Endpoints or IoT Endpoints acting as Gateways, SHOULD be capable of enforcing communications security even in environments where connectivity to the back-end network is unavailable.

4.3 Enhanced Controls

1. [E] Memory protection at the processor level SHALL be used when unprivileged applications or untrusted, third-party applications are to be part of the system.
2. [E] Bootloaders SHALL ONLY reside on internal processors, secure, permanent memory or on memory that can be locked, to prevent untrusted modification.
3. [E] Sensitive cryptographic data SHALL be processed in the processor's internal memory.
4. [E] IoT Endpoints SHALL ensure that they are carrying out anomaly detection, to detect patterns of abnormal activity.
5. [E] IoT Endpoints SHALL use tamper resistant casings of all sensitive electronics. Tamper evident casings SHOULD be used.
6. [E] Applications running on IoT Endpoints SHOULD ensure each unique process has a unique identity.

5. Personal Data Controls

These Personal Data controls are based on the requirements of Qatar's Personal Information and Privacy Protection (PIPP) law. They apply to all TASMU Service Operators processing Personal Data.

5.1 Governance of Personal Data

The TASMU Service Operator SHALL:

1. Ensure the adequate implementation of oversight and management reporting for data protection related complaints.
2. Implement periodic assessments and/or audits to measure the compliance posture of the TASMU System against these Personal Data requirements.
3. Ensure data transfer mechanisms are determined and agreed with all stakeholders, and records of transfer mechanism used for international data flows are maintained.
4. Notify the competent authority of all processing activities related to Special Personal Data
5. Undertake a Privacy Impact Assessment (PIA) for the TASMU System, covering:
    a. an inventory of all Personal Data assets being processed (type data, category (Standard/SpecialPersonal Data) & volume)
    b. reason for processing Personal Data
    c. the identification of any privacy risks raised for individuals
    d. current technical & non-technical controls for safeguarding Personal Data are in place
    e. identification of the person and their department, who has overall responsibility over the Personal Data
    f. any situation where Personal Data is leaving or residing outside of the State of Qatar
    g. any applicable rules that are being adhered to (e.g. sector data requirements) where Personal Data must only reside in the State of Qatar
6. Implement the following Privacy By Design principles:
    a. privacy as the default setting
    b. privacy embedded into design
    c. end-to-end security
    d. visibility and transparency
    e. respect for individual's privacy
7. Ensure that any data egress from the TASMU Ecosystem that contains Personal Data is Anonymised.

5.2 Transparency

The TASMU Service Operator SHALL:

1. Implement mechanisms to ensure individuals have provided Consent for the collection and use of Personal Data.
2. Obtain explicit Consent:
    a. from the parent before processing any Personal Data related to a minor
    b. from the individual before processing any Special Personal Data
3. Document clear guidelines on when Personal Data will be collected and used based on legitimate purpose (performance of contract, regulatory obligation, legitimate interest etc.).
4. Notify and obtain Consent from individuals before conducting any direct marketing activities.
5. Create and implement Privacy Notices for all channels that are used to collect Personal Data outlining:
    a. name and contact details of the TASMU Service Operator
    b. description of the categories of Personal Data processed
    c. purposes of the processing
    d. if Personal Data is collected from a third party
    e. if Personal Data is shared with a third party
    f. any relevant individuals' rights related to Personal Data processing

6. Visually summarise the purpose, technology type, accountable organisation and a link to the Privacy Notice using the DTPR Scheme.

7. Ensure that all channels of communication with individuals provides them with an option to opt-out of any targeted marketing activities leading to potential revocation of their Consent to the collection and use of Personal Data.

8. Implement adequate mechanisms to record and track Consent obtained from individuals.

9. Ensure that the processing of Personal Data from telemetry data collected from IoT devices and services is kept to a minimum and such data is Anonymised.

10. Ensure that Subscribers have provided explicit Consent for any TASMU Smart Service whose data contains Personal Data and will be aggregated either in Sector Platforms and/or the Central Platform. If explicit Consent has not be obtained, all their data on Sector Platforms and/or the Central Platform shall be Anonymised.

5.3 Personal Data Management

The TASMU Service Operator SHALL:

1. Implement mechanisms to ensure that Personal Data is not processed, stored and retained in the organisational systems beyond the fulfilment of its purpose to support the principle of minimisation.

2. Implement mechanisms to ensure that the identity of an individual can no longer be traced after the fulfilment of the purpose for which its data was processed by the organisation by adopting the relevant Anonymisation and/or pseudonymisation techniques.

3. Implement mechanisms to review the usage of Personal Data related to tracking of individuals or their devices, and for research purposes unless the processing is explicitly needed for the correct functioning of the TASMU System.

4. Implement and maintain mechanisms and measures to ensure that Personal Data is protected (e.g. encryption, pseudonymisation, other technical controls, etc.) and kept confidential across the data lifecycle, i.e. from collection/ creation to destruction/archiving.

5. Ensure that any interference to Personal Data such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing by persons other than Subscribers, is prohibited, except when it is necessary for detecting faults or permitted by the law of the State of Qatar.

6. Ensure that Special Personal Data is strongly encrypted (see §Cryptography) across the data lifecycle, i.e. from collection/creation to destruction/archiving.

7. Ensure access to Personal Data is provided on a 'need to have' basis, it is role-based and avoids any conflicts by implementing segregation of duty.

5.4 Requests from Individuals

The TASMU Service Operator SHALL:

1. Implement adequate mechanisms to facilitate individuals' right to:

    a. file a complaint for which corrective measures can be undertaken
    b. access their Personal Data
    c. update and correct their Personal Data
    d. request for information related to the purpose of Personal Data collection, or disclosure of inaccurate Personal Data
    e. request for erasure or Anonymisation of data
    f. object to processing of Personal Data if it is not compatible to the original purpose for which it was collected

5.5 Respond and Manage Personal Data Incidents & Breaches

The TASMU Service Operator SHALL:

1. Have a formally defined and implemented data protection incident and/or breach response plan, including communication to affected individuals, notification to the competent authority and reporting to the TASMU Smart Nation Regulator.
2. Notify the competent authority and the TASMU Smart Nation Regulator within seventy-two (72) hours from when the TASMU Service Operator was made aware of the breach.
3. Notify the individuals affected by the breach without undue delay.
4. Implement mechanisms to log all data protection incidents and/or breaches, and maintain adequate information supporting its resolution to assess the effectiveness of implemented measures.

5.6 Third Party Processing

The TASMU Service Operator SHALL:

1. Have adequate arrangements (contracts, processes, etc.) and mechanisms in place to ensure that Personal Data processed by a third party is adequately protected.
2. Review the adoption of cloud services to process Personal Data, and ensure that it adequately supports compliance with the (PIPP) law.
3. Ensure long term contracts and agreements related to processing of Personal Data are periodically reviewed against new or evolving data protection risks and threats.

---

1. Competent authorities can help provide threat levels against specific services
2. Special Personal Data in the Personal Data