Technical Specification

Security Requirements for Residential Gateways

Draft IMDA TS RG-SEC
Issue 2, April 2026

Info-communications Media Development Authority of Singapore
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Content

Security Requirements for Residential Gateways

1 Scope

In light of the vast and increasing deployment of Internet of Things ("IoT") devices in Singapore and globally, this Specification defines the minimum technical security requirements for design and management of Residential Gateways that are the gateways of home IoT devices, examples of which are as shown in Figure 1.

This IMDA Technical Specification sets out to minimise the vulnerabilities of Residential Gateways, ensuring that these devices are better protected when purchased and deployed by consumers, thus safeguarding both the Communication Networks and the home IoT devices from security threats on the Internet.

This Technical Specification shall be read in conjunction with the Cybersecurity Labelling Scheme (CLS) for IoT Publication No. 4A, which sets out the baseline requirements (refer to the CLS (IoT) Home Gateway Level 2 Mandatory Provisions under Table 1 "Provisions for Each CLS (IoT) Level", which is in line with CLS Level 2 requirements) applicable to the Residential Gateways. (All requirements stipulated in the referenced document shall continue to apply unless explicitly stated otherwise in Annex A.)

These controls are intended to strengthen the baseline requirements and address specific areas not fully covered in the Cybersecurity Labelling Scheme for IoT Publication No 4A and shall be implemented in addition to, and not in substitution of, the existing requirements.

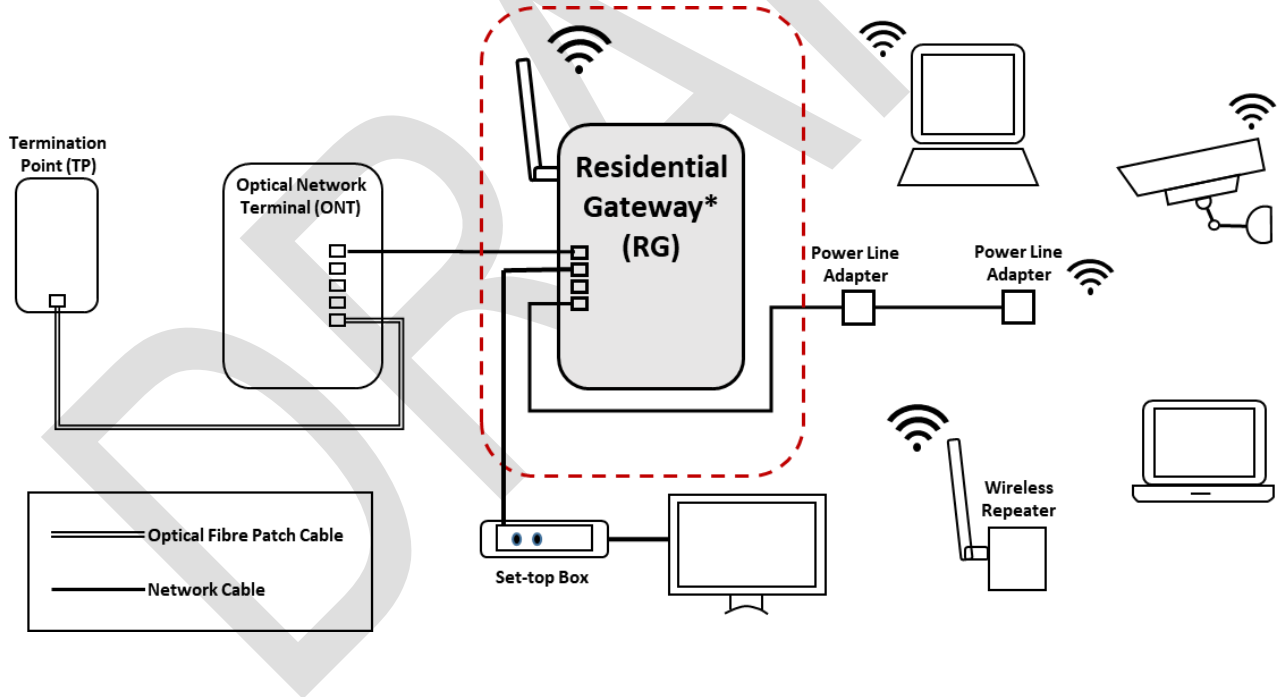

Figure 1: Typical Home Network Connection with Residential Gateway

2 References

For the technical requirements captured in this specification, references have been made to the following best practises and recommendations.

[1] ENISA, Nov 2017: Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures

[2] GSMA CLP.13: IoT Security Guidelines Endpoint Ecosystem Version 2.0 31 October 2017

[3] CCC SP-151-4A CLS(IoT) Assessment Methodology For Home Gateway v1.1

3 Definitions and Abbreviations

For the purpose of this specification, the following terms and definitions apply.

3.1 Definitions

Residential Gateway	A powered home networking device, typically used as a gateway to connect devices in the home to the Internet Access Service Provider's ("IASP") network as shown in Figure 1.
Login Credential	A set of identity data such as username and password, used to obtain access to system or network resources.
Default Login Credential	A set of predesignated common identity data that is usually provided for initial setup or after factory reset.

3.2 Abbreviations

IoT	Internet of Things
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol

4 Security Requirements

4.1 Minimum Password Strength

Access to Residential Gateway's administrative login page and device's configuration settings shall only accept unique passwords that meet the following requirements:

a. The minimum length of a password shall be 10, and shall meet at least 3 out of the following 4 complexity rules:
    i. Minimally 1 uppercase character (A-Z)
    ii. Minimally 1 lowercase character (a-z)
    iii. Minimally 1 digit (0-9)
    iv. Minimally 1 special character (punctuation and/or space)
b. The password shall not have consecutive identical characters.
c. Values used in the login ID and password shall not be the same.

4.2 Device Setup & Administration

4.2.1 Device Pre-loaded Settings

a. The Residential Gateway shall disable feature(s) that collects and sends the device's network statistic data back to manufacturer by default.
b. The Residential Gateway shall disable IPv6 tunnelling mechanisms by default. Most modern operating systems use IPv6 by default and thus, some operating systems will attempt to pass IPv6 traffic in an IPv4 wrapper using tunnelling capabilities, such as Teredo, 6to4, or ISATAP. These tunnels could be used to create a hidden channel of communication to and from the Residential Gateway.

4.2.2 Authentication Handling

The Residential Gateway shall ensure strong authentication, and protect against brute force and/or other abusive login attempts to admin page/settings [ENISA GP-TM-25]:

a. Unprotected access to the Residential Gateway's management webpage shall be prohibited. Access to the Residential Gateway's management webpage shall be only via authenticated credentials.
b. The login account shall be blocked after a fixed number of unsuccessful login attempts.
c. Secure alternative authentication mechanism shall be provided to fall-back on, when a login account is blocked. [GSMA CLP.13]

4.2.3 Credentials Handling

The Residential Gateway shall ensure that the credentials are properly managed to avoid them being compromised when they are used:

a. Password fields shall prevent its contents from being copied.
b. Password shall never be displayed on a user's screen and shall always be masked with the asterisk character, or another benign glyph. [GSMA CLP.13]
c. Network management credentials, e.g., remote login credentials specified in Broadband Forum's Technical Report 069 ("TR-069")[1], shall not be displayed on the Residential Gateway's management web page.

4.3 Firmware Updates

The device manufacturer shall ensure the patches:

a. do not contain sensitive data such as hardcoded credentials; and
b. are transmitted via secured connection.

4.4 Data Protection

Encryption algorithms used shall be replaceable so that improved encryption algorithms can be adopted without significant change to existing device.

4.5 CLS Level 2 Requirements

The Residential Gateway shall comply with the CLS Level 2 baseline requirements set out under the Cybersecurity Labelling Scheme (CLS) for IoT Publication No. 4A. Refer to Annex A for the complete checklist of requirements.

[1] TR-069 is a technical specification of the Broadband Forum that defines an application layer protocol for remote management of customer-premises equipment (CPE) connected to an Internet Protocol (IP) network.

Annex A

Conformance Testing / Verification Checklist

This Checklist is intended for facilitating Supplier's Declaration of Conformity to the technical requirements defined in the IMDA Technical Requirements for Security Requirements for Residential Gateways ("IMDA TS RG-SEC")

Please note:

"**CR**" indicates that the technical requirement set out in a particular section or sub-section ("§") of the IMDA TS RG-SEC is a **Compliance Requirement**.

"**M**" means that it shall be **Mandatory** for the Residential Gateways to comply with the technical requirement set out in the IMDA TS RG-SEC § cited in this Checklist (Table given below).

"**C**" means that compliance with the technical requirement set out in the IMDA TS RG-SEC § cited in this Checklist is **Conditional**. In this case, the need to comply is contingent on the conditions as indicated in the remarks column.

"**V**" means that compliance with the requirement is **Voluntary**.

IMDA TS RG-SEC §	Parameter	CR	Remarks
4.1	Minimum Password Strength		
	4.1.a	M	
	4.1.b	M	
	4.1.c	M	
4.2	Device Setup & Administration	-	
4.2.1	Device Pre-loaded Settings	-	
	4.2.1.a	C	If the features are available in the Residential Gateway
	4.2.1.b	C	If the features are available in the Residential Gateway
4.2.2	Authentication Handling	-	
	4.2.2.a	M	
	4.2.2.b	M	
	4.2.2.c	M	
4.2.3	Credentials Handling	-	
	4.2.3.a	M	
	4.2.3.b	M	
	4.2.3.c	M	
4.3	Firmware Updates	-	
	4.3.a	M	
	4.3.b	M	
4.4	Data Protection	M	
4.5	CLS Requirements	-	
	5.1 – No Universal Default Passwords	-	
	Provision 5.1-1	M	
	Provision 5.1-2	M	
	Provision 5.1-3	M	
	Provision 5.1-4	M	
	Provision 5.1-5	M	
	5.2 – Implement a Means to Manage Reports of Vulnerabilities	-	
	Provision 5.2-1	M	
	5.3 – Keep Software Updated	-	
	Provision 5.3-1	M	
	Provision 7.3-1	M	
	Provision 5.3-2	M	

	Provision 5.3-3	M	
	Provision 7.3-4	M	
	Provision 5.3-6	M	
	Provision 7.3-6	M	
	Provision 5.3-7	M	
	Provision 7.3-7	M	
	Provision 5.3-8	M	
	Provision 5.3-9	M	
	Provision 5.3-10	M	
	Provision 5.3-13	M	
	Provision 5.3-16	M	
	5.4 – Securely Store Sensitive Security Parameters	-	
	Provision 5.4-1	C	If the features are available in the Residential Gateway
	Provision 7.4-1	M	
	Provision 5.4-2	M	
	Provision 7.4-2	M	
	Provision 5.4-3	M	
	Provision 7.4-3	M	
	Provision 5.4-4	M	
	5.5 – Communicate Securely	-	
	Provision 5.5-1	M	
	Provision 5.5-5	M	
	Provision 7.5-6	C	If the features are available in the Residential Gateway
	Provision 5.5-7	M	
	Provision 7.5-7	M	
	Provision 5.5-8	M	
	5.6 – Minimise Exposed Attack Surfaces	-	
	Provision 5.6-1	M	
	Provision 7.6-1	M	
	Provision 5.6-2	M	
	Provision 7.6-2	M	
	Provision 7.6-3	C	If the features are available in the Residential Gateway
	Provision 5.6-4	M	
	Provision 7.6-4	M	
	Provision 5.6-5	M	
	Provision 7.6-9	M	
	5.8 – Ensure that Personal Data is Protected	-	
	Provision 5.8-2	M	
	Provision 5.8-3	M	
	5.9 – Make Systems Resilient to Outages	-	
	Provision 5.9-2	M	
	5.11 – Make It Easy for Consumers to Delete Personal Data	-	
	Provision 5.11-1	M	
	5.13 – Validate Input Data	-	
	Provision 5.13-1	M	
	6.1 – Data Protection Provisions for Consumer	-	
	Provision 6.1	M	
	Provision 6.2	M	
	Provision 6.3	M	
	Provision 6.5	M	

Annex B

Corrigendum / Addendum

Revised TS Reference	Items Changed	Date of Issue
Changes to IMDA TS RG-SEC Issue 1, Oct 2020		
	The IMDA TS RG-SEC Issue 1 has been replaced by the IMDA TS RG-SEC Issue 2. Due to the uplifting of CLS Level 1 to CLS Level 2, the TS RG-SEC has been updated to reference the Cybersecurity Labelling Scheme for IoT Publication No 4A. Clauses not covered under the Cybersecurity Labelling Scheme for IoT Publication No 4A have been retained within TS RG-SEC Issue 2. Main changes include: a. Removal of clause 4.1, except clause 4.1.2 b. Changes to clause 4.2.1 c. Removal of clause 4.2.2 d. Changes to clause 4.2.3 e. Changes to clause 4.2.4 f. Removal of clause 4.2.5 g. Changes to clause 4.3 h. Removal of clause 4.4 i. Changes to clause 4.5 and rename as clause 4.4 j. Removal of 4.6 k. Removal of 4.7 l. Added new clause for CLS Level 2 requirements m. Changes to annex A for clause 4 changes n. Added Annex B	April 2026
§4 Annex A		