Residential Gateway ("RG") Supporting Document Submission Guideline

This document is to serve the guideline for validating the supporting document submitted for RG devices to compliance to IMDA Technical Specification for Security Requirements for Residential Gateways ("**IMDA TS RG-SEC**") under the equipment registration framework. Please note that CLS Level 2 certification is a mandatory prerequisite for equipment registration under TS RG-SEC Issue 2.

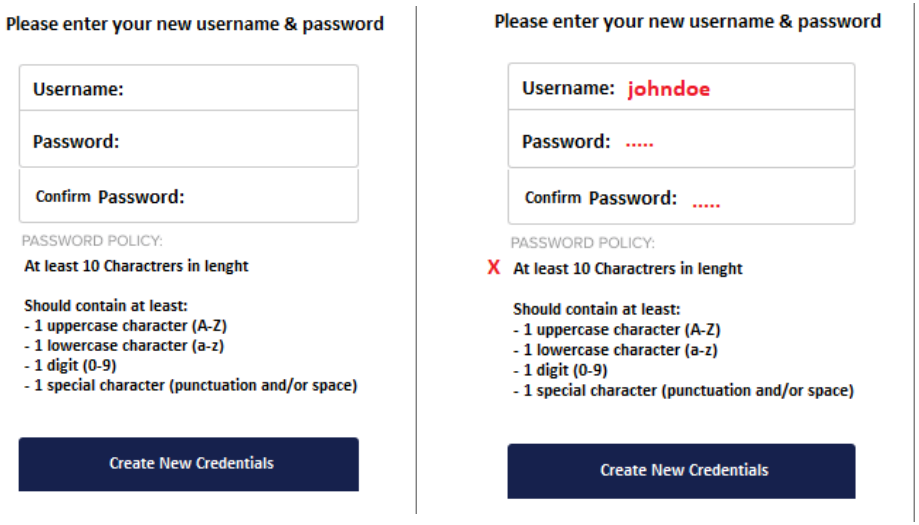
1. Under the mandatory requirement, the supporting document to proof the compliance shall be submitted for IMDA's assessments
2. Under the conditional requirement, the supporting document to proof the compliance shall be submitted (if applicable) for IMDA's assessments
3. Under the voluntary requirement, the supporting document to proof the compliance is optional for IMDA's assessments

Please refer to the respective sections when carrying out the verification of the submitted supporting documents.

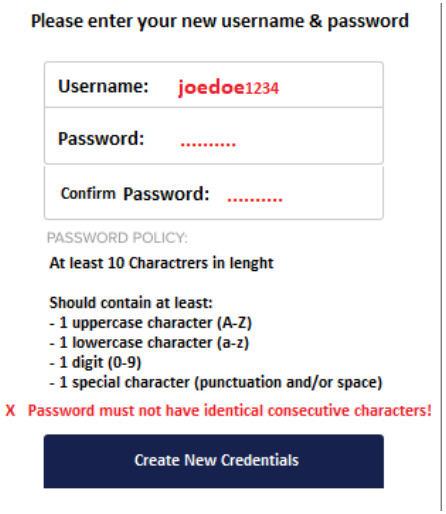
- 4.1 Minimum Password Strength
- 4.2 Device Setup & Administration
- 4.3 Firmware Updates
- 4.4 Data Protection
- 4.5 CLS Level 2 Requirements

4.1 Minimum Password Strength		
IMDA TS RG-SEC	**Parameter**	**Compliance**
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:

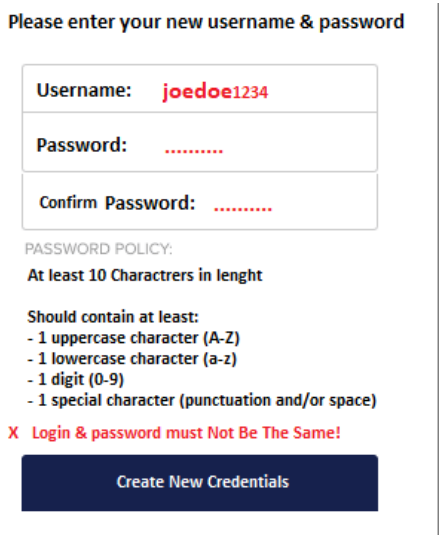
IMDA TS RG-SEC	Parameter	Compliance	CR
4.1	4.1.a	a. The minimum length of a password shall be 10, and shall meet at least 2 out of the following 4 complexity rules: i. Minimally 1 uppercase character (A-Z) ii. Minimally 1 lowercase character (a-z) iii. Minimally 1 digit (0-9) iv. Minimally 1 special character (punctuation and/or space)	M

Examples of Screenshots supporting compliance	Sample Screenshots
A screen that show minimum length of a password is 10, and meeting at least 2 out of the following 4 complexity rules	

IMDA TS RG-SEC	Parameter	Compliance	CR
4.1	4.1.b	b. The password shall not have consecutive identical characters.	M

Examples of Screenshots supporting compliance	Sample Screenshots
A screen that show the password shall not have consecutive identical characters.	

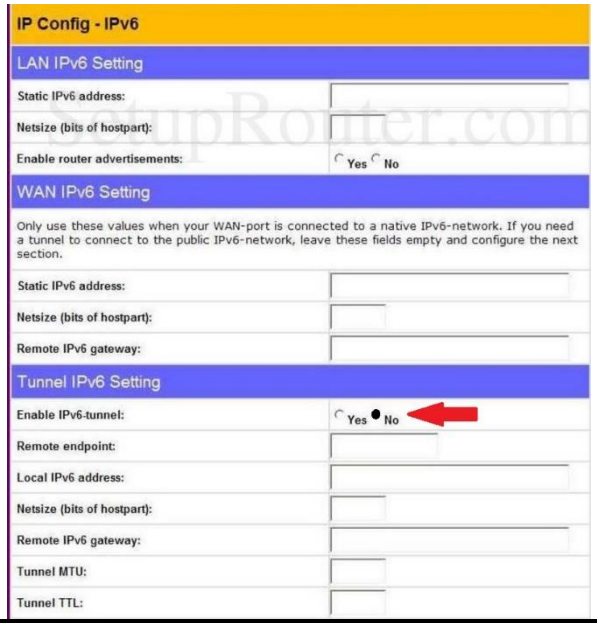
IMDA TS RG-SEC	Parameter	Compliance	CR
4.1	4.1.c	c. Values used in the login ID and password shall not be the same.	M

Examples of Screenshots supporting compliance	Sample Screenshots
A screen to show values used in the login ID and password shall not be the same.	

4.2 Device Setup & Administration			
IMDA TS RG-SEC	**Parameter**	**Compliance**	**CR**
4.2.1	4.2.1.a	a. The Residential Gateway shall disable feature(s) that collects and sends the device's network statistics data back to manufacturer by default.	C

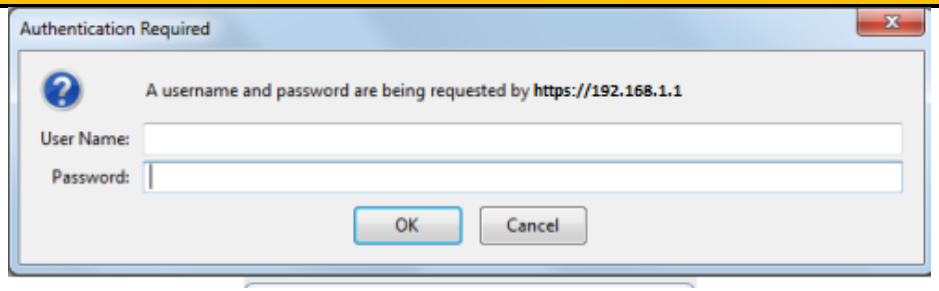
Examples of Screenshots supporting compliance	**Sample Screenshots**
Manufacturer is expected to provide proof from user manual, technical documents, web site or screenshots to comply to this clause.	No screenshots available.

IMDA TS RG-SEC	Parameter	Compliance	CR
4.2.1	4.2.1.b	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.	C

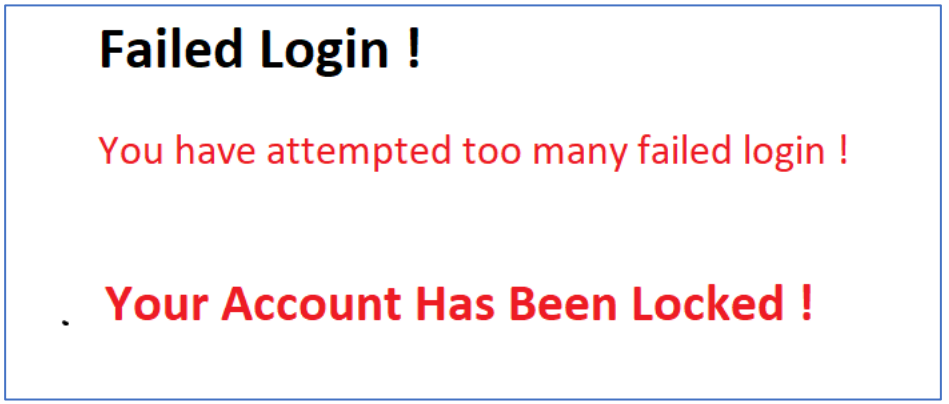
Examples of Screenshots supporting compliance	Sample Screenshots
A screen that show the Residential Gateway disable IPv6 tunnelling mechanisms by default.	

IMDA TS RG-SEC	Parameter	Compliance
4.2.2	Authentication Handling	The Residential Gateway shall ensure strong authentication, and protect against brute force and/or other abusive login attempts to the administration page/settings [ENISA GP-TM-25]:

IMDA TS RG-SEC	Parameter	Compliance	CR
4.2.2	4.2.2.a	a. Unprotected access to the Residential Gateway's management webpage shall be prohibited. Access to the Residential Gateway's management webpage shall only via authenticated credentials.	M

Examples of Screenshots supporting compliance	Sample Screenshots
A screenshot to show unprotected access to the Residential Gateway's management webpage is prohibited. Access to the Residential Gateway's management webpage shall only via authenticated credentials.	

IMDA TS RG-SEC	Parameter	Compliance	CR
4.2.2	4.2.2.b	b. The login account shall be blocked after a fixed number of unsuccessful login attempts.	M

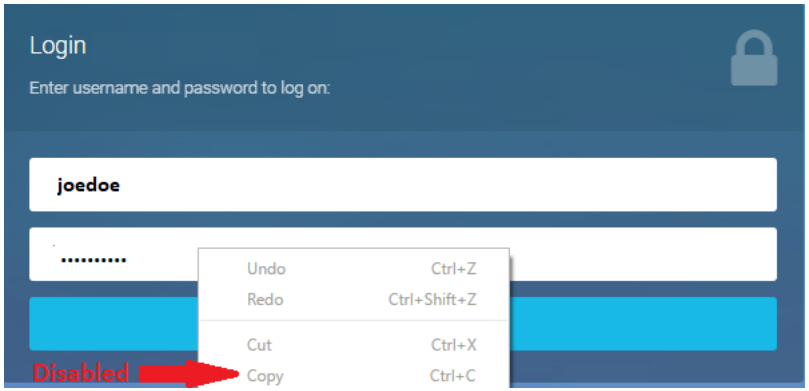
Examples of Screenshots supporting compliance	Sample Screenshots
A screenshot to show login account shall be blocked after a fixed number of unsuccessful login attempts.	

IMDA TS RG-SEC	Parameter	Compliance	CR
4.2.2	4.2.2.c	c. Secure alternative authentication mechanism shall be provided to fall-back on, when a login account is blocked.	M

Examples of Screenshots supporting compliance	Sample Screenshots
Manufacturer is expected to provide proof from user manual, technical documents, web site or screenshots to comply to this clause.	No screenshots available.

IMDA TS RG-SEC	Parameter	Compliance
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:

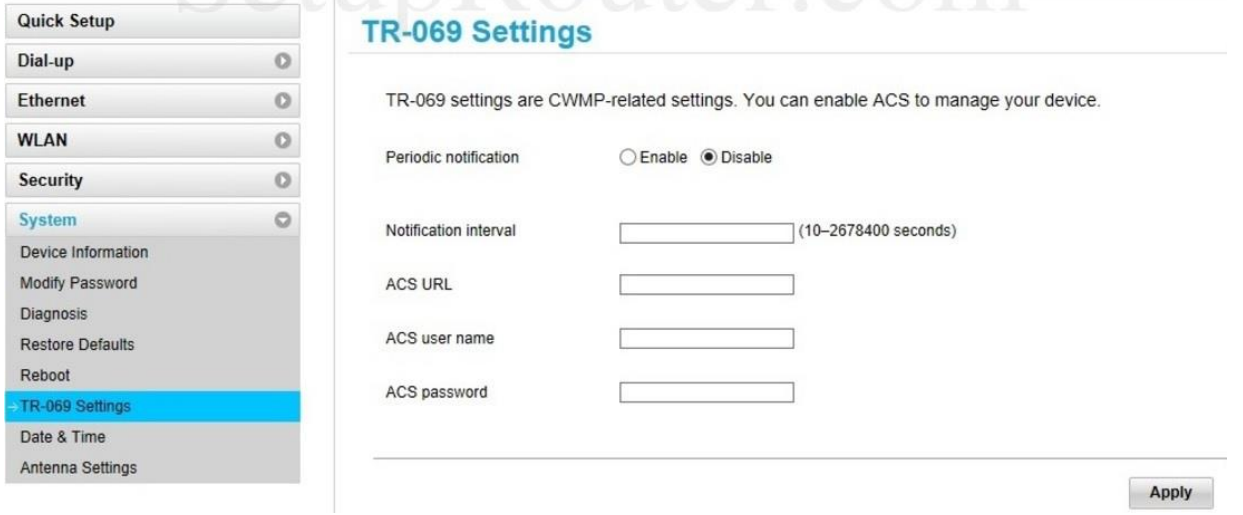
IMDA TS RG-SEC	Parameter	Compliance	CR
4.2.3	4.2.3.a	a. Password fields shall prevent its contents from being copied.	M

Examples of Screenshots supporting compliance	Sample Screenshots
A screenshot to show password fields shall prevent its contents from being copied.	

IMDA TS RG-SEC	Parameter	Compliance	CR
4.2.3	4.2.3.b	b. Password shall never be displayed on a user's screen and shall always be masked with the asterisk character, or another benign glyph.	M

Examples of Screenshots supporting compliance	Sample Screenshots
A screenshot to show that password is not displayed by default on a user's screen and shall be masked with the asterisk character, or another benign glyph. Residential Gateway may have an option to unmask passwords at user's own discretion.	

IMDA TS RG-SEC	Parameter	Compliance	CR
4.2.3	4.2.3.c	c. Network management credentials, e.g., remote login credentials specified in Broadband Forum's Technical Report 069 ("TR-069"), shall not be displayed on the Residential Gateway's management web page.	M

Examples of Screenshots supporting compliance	Sample Screenshots
A screenshot to show network management credentials, e.g., remote login credentials specified in Broadband Forum's Technical Report 069 ("TR-069") , shall not be displayed on the Residential Gateway's management web page.	

4.3 Firmware Updates		
IMDA TS RG-SEC	**Parameter**	**Compliance**
4.3	Firmware Updates	The device manufacturer shall ensure the patches:

IMDA TS RG-SEC	Parameter	Compliance	CR
4.3	4.3.a	a. Do not contain sensitive data such as hardcoded credentials	M

Examples of Screenshots supporting compliance	Sample Screenshots
Manufacturer is expected to provide proof from user manual, technical documents, web site or screenshots to comply to this clause.	No screenshots available.

IMDA TS RG-SEC	Parameter	Compliance	CR
4.3	4.3.b	b. Are transmitted via secured connection.	M

Examples of Screenshots supporting compliance	Sample Screenshots
Manufacturer is expected to provide proof from user manual, technical documents, web site or screenshots to comply to this clause.	No screenshots available.

4.4 Data Protection			
IMDA TS RG-SEC	**Parameter**	**Compliance**	**CR**
4.4	Data Protection	Encryption algorithms used should be replaceable so that improved encryption algorithms can be adopted without significant change to existing device.	M

Examples of Screenshots supporting compliance	Sample Screenshots
Manufacturer is expected to provide proof from user manual, technical documents, web site or screenshots to comply to this clause.	No screenshots available.

4.5 CLS Level 2 Requirements			
IMDA TS RG-SEC	**Parameter**	**Compliance**	**CR**
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.	M