SN	IMDA Requirements	Compliance Requirement	Clarification Question	Comment/s and Proposed Solution
4.1	Login Credentials Management The Residential Gateway with default login credentials, such as usernames and passwords, can be easily compromised, thereby allowing an attacker to gain access and use the device for malicious activities such as participation in botnets to perform DDoS attacks, Man-in-the-Middle attacks and/or through it to infiltrate other connected home IoT devices. The following measures are typical of industry practices to ensure that login credentials used for access controls are adequately protected.	-	-	-
4.1.1	Factory Pre-loaded Login Credentials Factory pre-loaded login credentials such as passwords shall be randomised and unique for each Residential Gateway. If default login credentials are used, the Residential Gateways shall be in a disabled state (non-functioning) until the user successfully set new login credentials upon first attempt to access the device's administration login page and the device's configuration settings.	Mandatory	Does it mean that user can never be allowed to go internet as long as he has not set new login credentials, regardless of even if different unit will have a unique admin login credential ?	1. Each unit out of the box shall have unique password to login, for both Login Credential and WiFi Password. This information shall be printed on the respective product label. 2. As long as the RG obtains valid IP Address and able to resolve DNS, connected user shall be able to surf the internet; regardless of whether he go through the Setup attempt. => With this, while we can ensure that each unit has different password, it will be more user friendly for non-Tech-savyy users.
4.1.2	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)	Mandatory		Recommend not to include space as user may easily forget space as part of his set password resulting in unnecessary support call.
	b. The password shall not have consecutive identical characters.	Mandatory	Please confirm if this password string is allowed: **Pa11111111" -> This password string meets requirement 4.1.2.a.**	1. Password String shall meet 4.1.2.a requirement and that should allow user to set password such as: Pa11111111" or A12345678p~ 2. User is allowed to set the same unique password as what he previously set as long as it meets 4.1.2.a requirement.
	c. Values used in the login ID and password shall not be the same.	Mandatory	Please confirm that this is refering to Login ID Username and Login ID Password shall not be the same	1. Login ID and Login Password values shall be different. 2. Login Password and WiFi Password can be the same , as long as it meets 4.1.2.a requirement.
4.2	Device Setup & Administration The Residential Gateway needs to manage and control the access to device's administration page; ensuring only authorised personnel are able to edit the configuration settings. While it is important to restrict intruder access, the Residential Gateway also needs to protect the device from being	-		
4.2.1	Device Pre-loaded Settings			

	a. The Residential Gateway shall turn off the following system services by default: i. WPS ii. HNAP	Conditional (If the features are available in the Residential Gateway)	-	-
	b. The Residential Gateway shall turn off the following Residential Gateway WAN interfaces by default: i. Remote Administration ii. SNMP iii. NAT-PMP iv. Telnet	Conditional (If the features are available in the Residential Gateway)	UPnP will be turned off or on by default @LAN site ?	All WAN interfaces listed are disabled by default. Recommend to enable UPnP on LAN side.
	c. The Residential Gateway shall disable feature(s) that collects and sends the device's network statistics data back to manufacturer by default.	Conditional (If the features are available in the Residential Gateway)	-	-
	d. The Residential Gateway shall turn on its firewall by default and support NAT to prevent its internal systems from being accessed directly from the Internet.	Conditional (If the features are available in the Residential Gateway)	-	-
	e. 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	Conditional (If the features are available in the Residential Gateway)	Please confirm if this is for both WAN side and LAN side	-
4.2.2	Initial Setup Handling First attempt to access to the Residential Gateway's administration page/settings should be conducted through a wired connection. If a wireless connection is used, the wireless communication should leverage on at least AES encryption, with at least WPA2 protection	Voluntary	-	-
4.2.3	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]:	Mandatory	-	-
	a. Unprotected access to the Residential Gateway's management webpage shall be prohibited.	Mandatory	-	-
	b. Authentication credentials shall be salted, hashed and/or encrypted. [ENISA GP-TM-24].	Mandatory	-	-
	c. Incremental prolong periods of login delay shall be employed after each subsequent failed	Mandatory	-	-
	d. The login account shall be blocked after a fixed number of unsuccessful login attempts.	Mandatory	For products that do not have Cloud Login access as the user ID - what shall be the recovery method in order for user to use this RG. Or is the recommended recovery method is to Reset the RG to Factory Default.	To prompt user to do a Reset to Factory default setting after a number of fail trials to login
	e. Secure alternative authentication mechanism shall be provided to fall-back on, when a login account is blocked. [GSMA CLP.13]	Mandatory		
4.2.4	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.	Mandatory	-	-
	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]	Mandatory	-	-
	c. Password recovery or reset mechanism shall be protected and does not supply an attacker with any form of information indicating a valid account [ENISA GP-TM-26]	Mandatory	-	-

	d. 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	Mandatory	-	-
4.2.5	Device Management Interface The Device management interface to the Residential Gateway shall be protected via secure communication protocol such as SSH or HTTPS to prevent the communication channel from being sniffed by unauthorised actors with malicious intent. Signed certificates from a Certification Authority ("CA") and self-signed certificates can be considered for this purpose.	Mandatory	Upon implementation of HTTPS with self signed CA for this purpose, user will always get an empty page telling him that the page is 'Not Trusted' and that he has to click 'Advanced' which is a greyed link by default when attempting to go to the RG page and will result in major increment in support calls.	Since User can only login to the RG by default through Local LAN / WIFI connected network plus implementation of item 4.2.3 requirement - it should be deemed safe enough whilst not compromising too much on user experience - user needs to accept safety warning to proceed for https as most of router with self-signed certificates. The same applies, if assuming we allowed a stranger to enter our house - there has to be a certain level of trust that he/she does not have malicious intent before we let him/her in. both http and https supported will be good for user.
4.3	Firmware Updates			
	a. The Residential Gateway shall automatically download the latest security patches.	Mandatory		
	b. The Residential Gateway shall be updated with the latest security patches automatically. Patching could be carried out through different means and mechanisms, e.g., when Residential Gateway is	Mandatory		
	c. The Residential Gateway should also provide means for users to manually run and install the downloaded security patches.	Voluntary	-	-
	d. The Residential Gateway shall verify the patches are digitally signed before installing them.	Mandatory	-	-
	e. Minimum period of the firmware support received by the Residential Gateway shall be provided upfront to the user.	Mandatory	All our products comes with minimum 1 year warranty or within the product lifetime. Any differences will be published on our website.	FW support will be within the stated Warranty Period. or as the product has not been declared End Of Life and that there is No more support. Alternatively, we will recommend user to upgrade to next similar / better new model.
	f. The device manufacturer should ensure the patches: i. do not contain sensitive data such as hardcoded credentials; and ii. are transmitted via secured connection.	Voluntary	-	-
	g. Security updates for the Residential Gateway should be provided in a timely manner. "Timely" in this context varies with the criticality of the identified vulnerability, the availability of a fix and the complexity of fix. The complexity of the fix is dependent on factors, such as constrained devices, involvement of multiple stakeholders, hardware versus software fix, etc.	Voluntary	-	-
4.4	Wireless Access Protection			
	a. The Residential Gateway should employ strong passwords as described in Section 4.1.2 for Wi-Fi	Voluntary	-	-
	b. The Residential Gateway shall use AES encryption, with at least WPA2 protection by default. If weaker security protection such as WEP or WPA is chosen by users, warning(s) of the higher security risk to use these encryption algorithms shall be displayed.	Mandatory	-	-
	c. The Residential Gateway shall allow and recommend to the user to setup guest networks with separate passwords for authorised guest users & guest IoT devices of the home network, isolating these accounts from the main home network.	Mandatory	-	-
4.5	Data Protection			
	a. The Residential Gateway shall encrypt the data elements that it uses and stores with standardised encryption algorithms (e.g., AES) with no known vulnerability.	Mandatory	-	-
	b. Encryption algorithms used should be replaceable so that improved encryption algorithms can be adopted without significant change to existing device	Voluntary	-	-
4.6	Validation of Data Inputs Data input to the device via all interfaces shall be validated, to protect the Residential Gateway from actions such as information leakage, remote code execution and cross-site scripting.	Mandatory	-	-

4.7	Vulnerabilities Reporting A point of contact, e.g., email address and contact number shall be provided to allow the reporting of security vulnerabilities relating to the Residential Gateway	Mandatory	Please advise if there is a specific platform we need to follow. E.g. by posting this information on our Support website or on the Quick Installation Guide of RG.	