

CYBERSECURITY LABELLING SCHEME FOR INTERNET OF THINGS (IOT) CCC SP-151-7 DECLARATION OF CONFORMITY

Instructions for Use

The developer shall reference the ETSI EN 303 645 – Cyber Security for Consumer Internet of Things, IMDA IoT Cyber Security Guide published by IMDA, and CCC SP-151-4 – CLS (IoT) Assessment Methodology prior to declaring conformity to the requirements within this document.

The developer shall declare against **ALL** clauses even if the clauses may not be mandatory for the level the developer is applying. “M” refers to Mandatory, whereas “R” refers to “Recommended”. “C” refers to “Conditional” should a dependent provision is being implemented. The mandatory clauses for each CLS Level are marked in green.

The developer shall ensure that the information given in this declaration is true and return a signed document to the CCC.

The developer shall also provide supporting evidence via the use of the CLS (IoT) - Company - Supporting Evidence v1.0 template.

General Information

Company Name	
Device Proprietary / Brand Name	
Device Name and Model	

Clause	Provision	CLS Requirements				Developer's Conformity (Yes/No/Not Applicable)
		L1	L2	L3	L4	
5.1: No universal default passwords	5.1-1	M C (1)	M C (1)	M C (1)	M C (1)	
	5.1-2	M C (2)	M C (2)	M C (2)	M C (2)	
	5.1-3	M C (8)	M C (8)	M C (8)	M C (8)	
	5.1-4	M C (8)	M C (8)	M C (8)	M C (8)	
	5.1-5	M C (5)	M C (5)	M C (5)	M C (5)	
5.2: Implement a means to manage reports of vulnerabilities	5.2-1	M	M	M	M	
	5.2-2	R	R	R	R	
	5.2-3	R	R	R	R	
5.3: Keep software updated	5.3-1	R	R	R	R	
	5.3-2	M C (5)	M C (5)	M C (5)	M C (5)	
	5.3-3	M C (12)	M C (12)	M C (12)	M C (12)	
	5.3-4	R C (12)	R C (12)	R C (12)	R C (12)	
	5.3-5	R C (12)	R C (12)	R C (12)	R C (12)	
	5.3-6	R C (9, 12)	R C (9, 12)	R C (9, 12)	R C (9, 12)	
	5.3-7	M C (12)	M C (12)	M C (12)	M C (12)	
	5.3-8	M C (12)	M C (12)	M C (12)	M C (12)	
	5.3-9	R C (12)	R C (12)	R C (12)	R C (12)	
	5.3-10	M C (11, 12)	M C (11, 12)	M C (11, 12)	M C (11, 12)	
	5.3-11	R C (12)	R C (12)	R C (12)	R C (12)	
	5.3-12	R C (12)	R C (12)	R C (12)	R C (12)	
	5.3-13	M	M	M	M	
	5.3-14	R C (3, 4)	R C (3, 4)	R C (3, 4)	R C (3, 4)	
	5.3-15	R C (3, 4)	R C (3, 4)	R C (3, 4)	R C (3, 4)	
	5.3-16	M	M	M	M	

Clause	Provision	CLS Requirements				Developer's Conformity (Yes/No/Not Applicable)
		L1	L2	L3	L4	
5.4: Securely store sensitive security parameters	5.4-1	R C (14)	M C (14)	M C (14)	M C (14)	
	5.4-2	R C (10)	M C (10)	M C (10)	M C (10)	
	5.4-3	R	M	M	M	
	5.4-4	R C (15)	M C (15)	M C (15)	M C (15)	
5.5: Communicate securely	5.5-1	R	M	M	M	
	5.5-2	R	R	R	R	
	5.5-3	R	R	R	R	
	5.5-4	R C (16)	R C (16)	R C (16)	R C (16)	
	5.5-5	R C (17)	M C (17)	M C (17)	M C (17)	
	5.5-6	R C (18)	R C (18)	R C (18)	R C (18)	
	5.5-7	R C (19)	M C (19)	M C (19)	M C (19)	
	5.5-8	R C (20)	M C (20)	M C (20)	M C (20)	
5.6: Minimise exposed attack surfaces	5.6-1	R	M	M	M	
	5.6-2	R	M	M	M	
	5.6-3	R	R	R	R	
	5.6-4	R C (13)	M C (13)	M C (13)	M C (13)	
	5.6-5	R	R	R	R	
	5.6-6	R	R	R	R	
	5.6-7	R	R	R	R	
	5.6-8	R	R	R	R	
	5.6-9	R	R	R	R	
5.7: Ensure software integrity	5.7-1	R	R	R	R	
	5.7-2	R	R	R	R	
5.8: Ensure that personal data is protected	5.8-1	R C (21)	R C (21)	R C (21)	R C (21)	
	5.8-2	R C (22)	M C (22)	M C (22)	M C (22)	
	5.8-3	R C (23)	M C (23)	M C (23)	M C (23)	

Clause	Provision	CLS Requirements				Developer's Conformity (Yes/No/Not Applicable)
		L1	L2	L3	L4	
5.9: Make systems resilient to outages	5.9-1	R	R	R	R	
	5.9-2	R	R	R	R	
	5.9-3	R	R	R	R	
5.10: Monitor system telemetry data	5.10-1	R C (6)	R C (6)	R C (6)	R C (6)	
5.11: Make it easy for consumers to delete personal data	5.11-1	R C (24)	M C (24)	M C (24)	M C (24)	
	5.11-2	R C (25)	R C (25)	R C (25)	R C (25)	
	5.11-3	R C (26)	R C (26)	R C (26)	R C (26)	
	5.11-4	R C (26)	R C (26)	R C (26)	R C (26)	
5.12: Make installation and maintenance of devices easy	5.12-1	R	R	R	R	
	5.12-2	R	R	R	R	
	5.12-3	R	R	R	R	
5.13: Validate input data	5.13-1	R C (27)	M C (27)	M C (27)	M C (27)	
6: Data protection provisions for consumer IoT	6.1	R C (28)	M C (28)	M C (28)	M C (28)	
	6.2	R C (7)	M C (7)	M C (7)	M C (7)	
	6.3	R C (7)	M C (7)	M C (7)	M C (7)	
	6.4	R C (6)	R C (6)	R C (6)	R C (6)	
	6.5	R C (6)	M C (6)	M C (6)	M C (6)	
Lifecycle Requirements	CK-LP-01	-	-	M	M	
	CK-LP-02	-	-	M	M	
	CK-LP-03	-	-	M	M	
	CK-LP-04	-	-	M	M	
	CK-LP-05	-	-	M	M	
	CK-LP-06	-	-	M	M	
	CK-LP-07	-	-	M	M	

Clause	Provision	CLS Requirements				Developer's Conformity (Yes/No/Not Applicable)
		L1	L2	L3	L4	
	CK-LP-08	-	-	M	M	

Note: Where the conditional notation is used, this is conditional on the text of the provision. The conditions are provided below with references provided for the relevant provisions to help with clarity.

Conditions:

- 1) passwords are used,
- 2) pre-installed unique per device passwords are used,
- 3) software components are not updateable,
- 4) the device is constrained,
- 5) the device is not constrained,
- 6) telemetry data being collected,
- 7) personal data is processed on the basis of consumers' consent,
- 8) the device allowing user authentication,
- 9) the device supports automatic updates and/or update notifications,
- 10) a hard-coded unique per device identity is used for security purposes,
- 11) updates are delivered over a network interface,
- 12) an update mechanism is implemented,
- 13) a debug interface is physically accessible,
- 14) sensitive security parameters are stored persistently,
- 15) critical security parameters used for integrity and authenticity checks of software updates in device software or for protection of communication with associated services in device software exist,
- 16) access to device functionality via a network interface in the initialized state is possible,
- 17) device functionality that allows security-relevant changes in configuration via a network interface exists,
- 18) critical security parameters are transmitted,
- 19) critical security parameters are transmitted via remotely accessible network interfaces,
- 20) critical security parameters relating to the device exist,
- 21) personal data is transmitted between a device and a service,
- 22) sensitive personal data is transmitted between a device and a service,
- 23) external sensing capabilities exist,
- 24) user data is stored on the device,

Clause	Provision	CLS Requirements				Developer's Conformity (Yes/No/Not Applicable)
		L1	L2	L3	L4	
	25) personal data is stored on associated services,					
	26) personal data is stored,					
	27) data input via user interfaces or transferred via APIs or between networks in services and devices is supported,					
	28) personal data is processed.					

Declaration of Conformity

We declare that all information given in this document is true and correct and that we have not and will not wilfully omit or suppress any material facts.

Authorised Signature & Date

Name & Designation

Company's Stamp