Cybersecurity Labelling Scheme

FOR MEDICAL DEVICES

BY CYBER SECURITY AGENCY OF SINGAPORE

Draft Copy for Sandbox Use Only

Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)] Publication No. 1

Overview of the Scheme

October 2023
Version 0.5

FOREWORD

The Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)] is part of efforts from the Ministry of Health (MOH), Cyber Security Agency (CSA), Health Sciences Authority (HSA), and Synapxe to better secure Singapore's cyberspace and to raise cyber hygiene levels in medical devices.

Under the CLS(MD), the cybersecurity label for medical devices would provide an indication of the level of security in medical devices. It aims to improve security awareness by making such provisions more transparent to healthcare users and empowers them to make informed purchasing decisions for medical devices with better security using the information on the cybersecurity label.

The CLS(MD) seeks to incentivise manufacturers to develop and provide medical devices with enhanced cybersecurity provisions. The labels also serve to differentiate medical devices with better cybersecurity safeguards in the market, from their competitors.

At the same time, CSA intends to engage other like-minded partners for mutual recognition of the CLS(MD) with the objective of eliminating duplicated assessments across national boundaries.

The CLS(MD) is managed by the Cybersecurity Certification Centre (CCC) under the ambit of the Cyber Security Agency of Singapore (CSA). The CLS(MD) is jointly owned by MOH and CSA.

Draft Copy for Sandbox Use Only

AMENDMENT RECORD

Version	Date	Author	Changes
0.5	October 2023	Cyber Security Agency of Singapore	Draft

CONTENTS

1 INTRODUCTION 5

2 BACKGROUND 5
2.1 Impetus for CLS 5

3 DEFINITION OF TERMS 7

4 ORGANISATION AND MANAGEMENT OF CLS(MD) 8

5 SCOPE OF THE CLS(MD) 8

6 OVERVIEW OF THE CLS(MD) 9
6.1 Overview 9
6.2 Cybersecurity Labelling Levels 9

7 CYBERSECURITY LEVELS 10
7.1 Overview of CLS(MD) Cybersecurity Levels 10
7.2 Level 1 – Baseline Security Requirements 10
7.3 Level 2 – Enhanced Security Requirements 11
7.4 Level 3 – Enhanced Security Requirements, Software Binary Analysis, and Penetration Testing 11
7.5 Level 4 – Enhanced Security Requirements, Software Binary Analysis, Security Evaluation 13

8 GENERAL PROCESS FOR LABELLING OF MEDICAL DEVICE 14
8.1 Process Overview 14
8.2 Pre-Application Phase 16
8.3 Application for Labelling 17
8.4 Declaration of Conformity 18
8.5 Software Binary Analysis 18
8.6 Testing Phase (Only for Level 3 onwards) 18
8.7 Conclusion - Awarding of the CLS(MD) Label 18
8.8 Changes to Conditions for Labelling 18
8.9 Cryptography 18

9 SMALLEST ASSESSABLE MEDICAL DEVICE UNIT 19

10 GROUPING OF APPLICATIONS 19

11 APPLICANT OBLIGATIONS 20
11.1 Vulnerability Disclosure 20
11.2 Defined Support Period for Security Updates 20

12 CYBERSECURITY LABEL 21
12.1 Label 21
12.2 Label Validity 21
12.3 Requirements of the Cybersecurity Label 21

Draft Copy for Sandbox Use Only

12.4 Requirements on the Affixing of the Label for PUO and Non-PUO Medical Devices....22
12.5 Requirements on the Display of the Label for Software as a Medical Devices (SaMD)....22
12.6 How the Cybersecurity Label is to be Affixed or Displayed....22
12.7 Labelling Principles....23
12.8 CCC Audit and Testing....23
12.9 Revocation of the Cybersecurity Label....24

13 ASSURANCE CONTINUITY....25

14 RENEWAL OF LABEL....25

15 REQUIREMENTS FOR CLS(MD) TEST LABORATORY....25

16 MECHANISM FOR COMPLAINTS, DISPUTES AND APPEALS....27

17 FEES....28
17.1 General Policy....28

18 LIABILITY....29
18.1 Disclaimer....29

REFERENCES....30

ACRONYMS....30

Draft Copy for Sandbox Use Only

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

1 INTRODUCTION

1.0.1 This document provides an overview of the Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)]. It outlines the scheme objectives, description of the scheme, its organisation and management, as well as an overview of the testing process.

1.0.2 This document also sets out the requirements and procedures for the labelling of the medical device under the CLS(MD). It also establishes the technical oversight role of Cybersecurity Certification Centre (CCC) in the CLS(MD) and sets out general terms and conditions for the manufacturer and/or the Testing Laboratory (TL) that apply for such a label.

2 BACKGROUND

2.1 Impetus for CLS

2.1.1 The intent of the Cybersecurity Labelling Scheme is to improve the transparency of cybersecurity provisions. Under this scheme, the cybersecurity label would provide an indication of the level of security in the products. Consumers are thereby empowered to make informed purchasing decisions. By enhancing consumer security awareness, this scheme seeks to incentivise manufacturer to develop products with better security for the market, leading towards a safer and more secure cyber space.

2.1.2 The use of connected medical devices has gained momentum over the years worldwide to improve patients' health and lower care costs. However, connection of devices to networks or the internet also exposes devices to increased cyber risks. The cost of healthcare breaches worldwide is among the highest, if not the highest, among all sectors.

2.1.3 The integrity of medical devices is important to patient safety on three levels. First, unauthorised tampering of these devices e.g., insulin dosage settings of insulin pumps or pacing rate of pacemakers can harm patients directly. Second, the alteration of data could cause inappropriate treatment, thereby causing harm. Third, malicious activities spreading across corporate network either from the device or other entry points can cripple the entire healthcare IT network, thereby impacting patient care services beyond the affected healthcare facility.

2.1.4 Learning from the experience of recent global reported cybersecurity incidents, a pre-emptive approach to reduce the likelihood of a successful breach or, if it does happen, to reduce the impact, is critical.

2.1.5 To tackle this cyber-risk, HSA has rolled out and implemented cybersecurity guidelines since 2016. Taking into consideration the increased connectivity and digitalisation of medical devices alongside the evolving threat

Draft Copy for Sandbox Use Only

landscape that could impact healthcare service delivery, the Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)] was formed as a joint initiative by MOH, CSA, HSA, and Synapxe. The CLS(MD) envisions to improve the visibility of medical devices security, raise overall cyber hygiene levels, and better secure Singapore's cyberspace for both data protection and patient safety in our healthcare sector.

2.1.6 It is important to note that the Cybersecurity Labelling Scheme for Medical Devices does not offer formal security assurance. Given sufficient time, determined adversaries who possesses advanced skillsets and tools would likely be capable of compromising these devices, regardless of whether it is labelled. Users seeking higher security assurance from what is offered within the CLS(MD) are strongly recommended to consider devices certified under formal evaluation and certification schemes such as Common Criteria. Details relating to these higher assurance schemes are available on the CSA website (https://www.csa.gov.sg/sccs).

Draft Copy for Sandbox Use Only

3 DEFINITION OF TERMS

3.1 For the purposes of the CLS(MD) publications, the following terms apply:

Medical Device: Medical devices as described in the First Schedule of the Health Product Act[1] (Cap122D, 2008 Rev Ed).

Professional Use Only Medical Device: As set out in the Health Products (Medical Devices) Regulations, a medical device that is to be used on an individual solely by, or under the supervision of, a qualified practitioner.

Qualified Practitioner: Qualified Practitioner as set out in the Health Products (Medical Devices) Regulations means:

i. A registered medical practitioner under the Medical Registration Act (Cap. 174), when acting in the course of providing medical treatment to a patient under his care; or

ii. A registered dentist under the Dental Registration Act (Cap. 76) whose name appears in the first division of the Register of Dentists managed and kept under section 13(1)(a) of that Act, when acting in the course of providing dental treatment to a patient under his care.

Draft Copy for Sandbox Use Only

[1] Health Products Act - https://sso.agc.gov.sg/SL-Supp/S320-2018/Published/20180525170000?DocDate=20180525170000#pr2-

4 ORGANISATION AND MANAGEMENT OF CLS(MD)

4.1 The CLS(MD) is jointly owned by the Cyber Security Agency of Singapore (CSA) and the Ministry of Health (MOH).

4.2 The overall policy of the CLS(MD) is set by the Cybersecurity Certification Centre (CCC). The CCC is responsible for the management and direction of the CLS(MD), ensuring that the organisation and management of the functions of testing achieve high standards of competency, impartiality, and consistency. The CCC approves standards, publications, and projects.

4.3 The CCC establishes the requirements for the testing laboratories and oversees the testing laboratory approval process. The testing laboratory is approved only after it is assessed to be compliant to the requirements specified in Chapter 15 – Requirements for CLS(MD) Test Laboratory.

5 SCOPE OF THE CLS(MD)

5.1 The scope of the CLS(MD) applies to medical devices as described in the First Schedule of the Health Product Act[2] (Cap122D, 2008 Rev Ed) and have any of the following characteristics:

- Handles personal identifiable information (PII) and clinical data and has the ability to collect, store, process, or transfer such data;
- Connects to other devices, systems, and services - Has the ability to communicate using wired and/or wireless communication protocols through a network of connections.

Draft Copy for Sandbox Use Only

[2] Health Products Act - https://sso.agc.gov.sg/SL-Supp/S320-2018/Published/20180525170000?DocDate=20180525170000#pr2-

6 OVERVIEW OF THE CLS(MD)

6.1 Overview

6.1.1 The Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)] is a **voluntary scheme**. Products that apply for the Cybersecurity Label shall undergo a series of assessments and tests, depending on the level of Cybersecurity Label that the manufacturer wishes to attain.

6.1.2 Manufacturers may supply their medical devices in Singapore upon the completion of their registration with HSA, and can choose to participate in the CLS(MD) on a voluntary basis.

- Unregistered medical devices intending to be imported and supplied in Singapore via approval of Special Access Routes by HSA may also choose to participate in the CLS(MD) on a voluntary basis. Such medical devices will be subjected to a label validity period of a maximum of 1 year.

6.2 Cybersecurity Labelling Levels

6.2.1 The CLS(MD) comprises four (4) cybersecurity levels, with each higher level being more comprehensive in the assessment. The requirements of testing under each of the cybersecurity levels are summarised in Chapter 7 - Cybersecurity Levels.

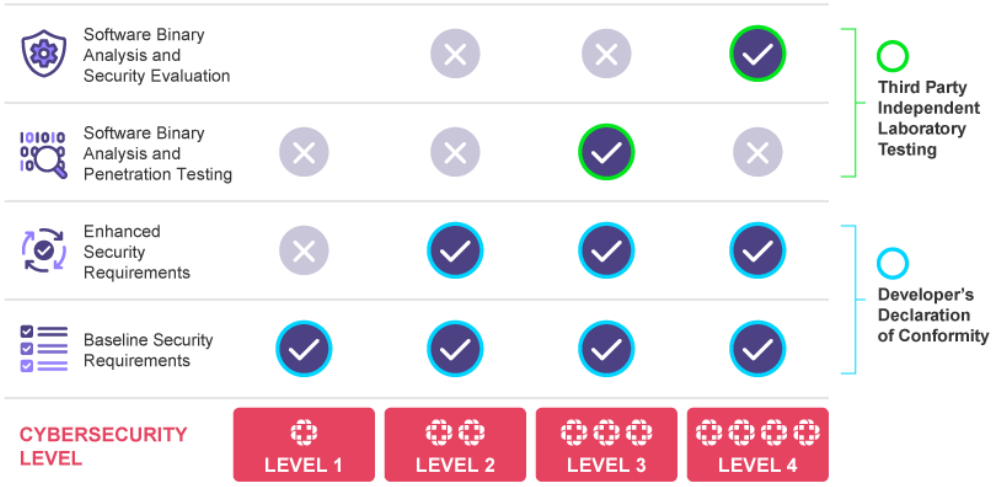


Figure 1 - Cybersecurity Levels

6.2.2 Under each labelling level, depending on the level of Cybersecurity Label that the manufacturer wishes to attain, the product shall be subjected to the applicable assessments and tests.

Dropbox Use Only

7 CYBERSECURITY LEVELS

This chapter seeks to provide an overview of the four levels within the CLS(MD).

7.1 Overview of CLS(MD) Cybersecurity Levels

Cybersecurity Level	Assessment Tier	Mode of Assessment	Involved Roles
1	Baseline Security Requirements	Validated manufacturer's declaration of conformity. No independent check by the test laboratory.	CCC; Manufacturer
2	Enhanced Security Requirements		CCC; Manufacturer
3	Enhanced Security Requirements, Software Binary Analysis, and Penetration Testing	3rd party independent assessment by testing laboratory	CCC; Manufacturer; Testing Laboratory
4	Enhanced Security Requirements, Software Binary Analysis, and Security Evaluation	3rd party independent assessment by testing laboratory	CCC; Manufacturer; Testing Laboratory

Table 1 - Overview of Assessment Tiers

7.2 Level 1 – Baseline Security Requirements

7.2.1 CLS(MD) Level 1 seeks to ensure that medical devices conform to a set of 6 security requirements consisting of not having universal default passwords, implementing adequate anti-brute force mechanism on the authentication interface, as well as cybersecurity requirements currently in use by HSA in the review of medical devices seeking registration in Singapore. The HSA cybersecurity requirements consist of establishing a cybersecurity risk management process to identify and mitigate all known and foreseeable vulnerabilities affecting the medical device and implement a systematic product maintenance process. This ensures that the emerging vulnerabilities are identified and evaluated on an on-going basis and effectively managed throughout the medical device lifecycle.

7.2.2 The manufacturer shall complete and submit the declaration of conformity, together with supporting evidence, specifying conformity status to the security requirements as set out within this level. Non-conformity to the security requirements shall lead to the failure of this activity.

7.2.3 CCC shall review the declaration of conformity and supporting evidence prior to approval.

Draft Copy for Sandbox Use Only

7.2.4 The estimated turnaround for CLS(MD) Level 1 is around 2 working days and may take longer depending on the quality of the submission. The estimated turnaround excludes administrative project overheads and potential delays due to technical or application deficiencies.

7.3 Level 2 – Enhanced Security Requirements

7.3.1 CLS(MD) Level 2 seeks to ensure that medical devices conform to a set of 38 security requirements. The enhanced security requirements consist of the following:

- Level 1 requirements.
- Cybersecurity requirements covering areas such as:
    - Vulnerability Disclosure Policy
    - Management of Sensitive Data
    - Audit Controls
    - Authorisation
    - Cyber Security Product Upgrades
    - Data Backup and Disaster Recovery
    - Malware Detection/Protection
    - Node Authentication
    - Connectivity Capabilities
    - Person Authentication
    - Roadmap for Medical Device Life Cycle
    - Software Bill of Materials
    - System and Application Hardening
    - Security Guidance
    - Health Data Storage Confidentiality
    - Transmission Confidentiality
    - Transmission Integrity
    - Remote Service
    - Other security considerations.

7.3.2 The manufacturer shall complete and submit the declaration of conformity, together with supporting evidence, specifying conformity status to the security requirements as set out within this level. Non-conformity to the security requirements shall lead to the failure of this activity.

7.3.3 CCC shall review the declaration of conformity and supporting evidence prior to approval.

7.3.4 The estimated turnaround for CLS(MD) Level 2 is around 5 working days and may take longer depending on the quality of the submission. The estimated turnaround excludes administrative project overheads and potential delays due to technical or application deficiencies.

7.4 Level 3 – Enhanced Security Requirements, Software Binary Analysis, and Penetration Testing

7.4.1 There are 3 components within CLS(MD) Level 3:

a. Meeting Enhanced Security Requirements. To ensure that devices

Draft Copy for Sandbox Use Only

meet the set of enhanced security requirements.

b. Software Binary Analysis. To analyse the device's software (device firmware and companion applications such as desktop or mobile applications) for malware, known vulnerabilities in third party libraries used, and for software weaknesses.
c. Penetration Testing. To assert that the medical device is reasonably resistant to common attacks and to prove that there are no obvious or critical vulnerabilities.

Enhanced Security Requirements

7.4.2 The enhanced security requirements are defined within CLS(MD) Level 2.

Software Binary Analysis

7.4.3 The medical device's firmware and companion software (mobile applications, desktop applications, etc.) shall be analysed for malware, known vulnerabilities in third party libraries used, and for software weaknesses such as buffer overflow.

7.4.4 The analysis shall be performed with the aid of a combination of binary, malware, and mobile application scanners.

7.4.5 The manufacturer's testing laboratory of choice shall review and interpret the scan results. At the end of the activity, the testing laboratory shall submit a report outlining test results, identified issues and corresponding method of resolution to the CCC.

7.4.6 CCC shall review the testing laboratory's report prior to approval.

7.4.7 The expected median duration of time spent by the lab for the software binary analysis is around 5 days (assuming 8 man-hours per day, equating to a total of 40 man-hours).

Penetration Testing

7.4.8 The penetration testing shall consist of the following sub-activities:

i. Device setup and verification of the guidance documents
ii. Conformity verification against the manufacturer's declaration of conformity and supporting evidences
iii. Minimum Test Specifications
iv. Search for potential vulnerabilities in the public domain
v. Freeform penetration testing, devising test cases based on findings from the software binary analysis, known threat vectors, and the testing laboratory's expertise and experience.

7.4.9 The manufacturer shall provide sufficient production samples of the device and related user guidance documents to the testing laboratory to facilitate setup, configuration, and testing.

7.4.10 The TL shall provide a report summarising the penetration testing performed and the results.

7.4.11 CCC shall review the testing laboratory's penetration testing report prior to

Draft Copy for Sandbox Use Only

approval.

7.4.12 The expected median duration of time spent by the TL solely on penetration testing is around 1 month (assuming 8 man-hours per day, 5 man-days per week, for a period of 1 month, equating to a total of 160 man-hours), and this duration excludes administrative/logistical overheads such as project management and delivery/setup of test units. The manufacturer or the test laboratory may request for an extension of the penetration testing duration depending on the complexity of the device.

7.5 Level 4 – Enhanced Security Requirements, Software Binary Analysis, Security Evaluation

7.5.1 There are 3 components within CLS(MD) Level 4

a. Meeting Enhanced Security Requirements. To ensure that devices are developed according to security-by-design framework and processes.
b. Software Binary Analysis. To analyse the device's software (Device firmware and companion mobile applications) for malware, known vulnerabilities in third party libraries used, and for software weaknesses.
c. Security Evaluation. To assert that the medical device is reasonably resistant to enhanced attacks and to prove that there are no obvious or critical vulnerabilities.

Enhanced Security Requirements

7.5.2 The enhanced security requirements are defined within CLS(MD) Level 2.

Software Binary Analysis

7.5.3 The software binary analysis requirements are defined within CLS(MD) Level 3.

Security Evaluation

7.5.4 The Security Evaluation shall consist of the following sub-activities:

a. Device setup and verification of the guidance documents
a. Conformity verification against the manufacturer's declaration of conformity and supporting evidence
b. Minimum Test Specifications
c. Search for potential vulnerabilities in the public domain
d. Analysis of product security design documentation on the medical device.
e. Vulnerability analysis of the medical device using the results from the software binary analysis, guidance documentation, and product security design documents to identify potential vulnerabilities in the medical device.
f. Penetration testing to confirm that the identified potential vulnerabilities cannot be exploited.

7.5.5 The manufacturer shall provide sufficient production samples of the device, related user guidance documents, and product security design

Draft Copy for Sandbox Use Only

documentation to the testing laboratory to facilitate testing.

7.5.6 The TL shall provide a report summarising the vulnerability analysis performed, penetration testing performed, and the corresponding results.

7.5.7 CCC shall review the testing laboratory's report prior to approval.

7.5.8 The expected median duration of time spent by the lab on security evaluation is around 3 months (assuming 8 man-hours per day, 5 man-days per week, for a period of 3 months, equating to a total of 480 man-hours), and this duration excludes administrative/logistical overheads such as project management and delivery of test units. The manufacturer or the test laboratory may request for an extension of the penetration testing duration depending on the complexity of the device.

8 GENERAL PROCESS FOR LABELLING OF MEDICAL DEVICE

8.1 Process Overview

8.1.1 The labelling of medical devices shall be performed within the framework of the CLS(MD).

8.1.2 The key roles and responsibilities within the CLS(MD) are as follows:

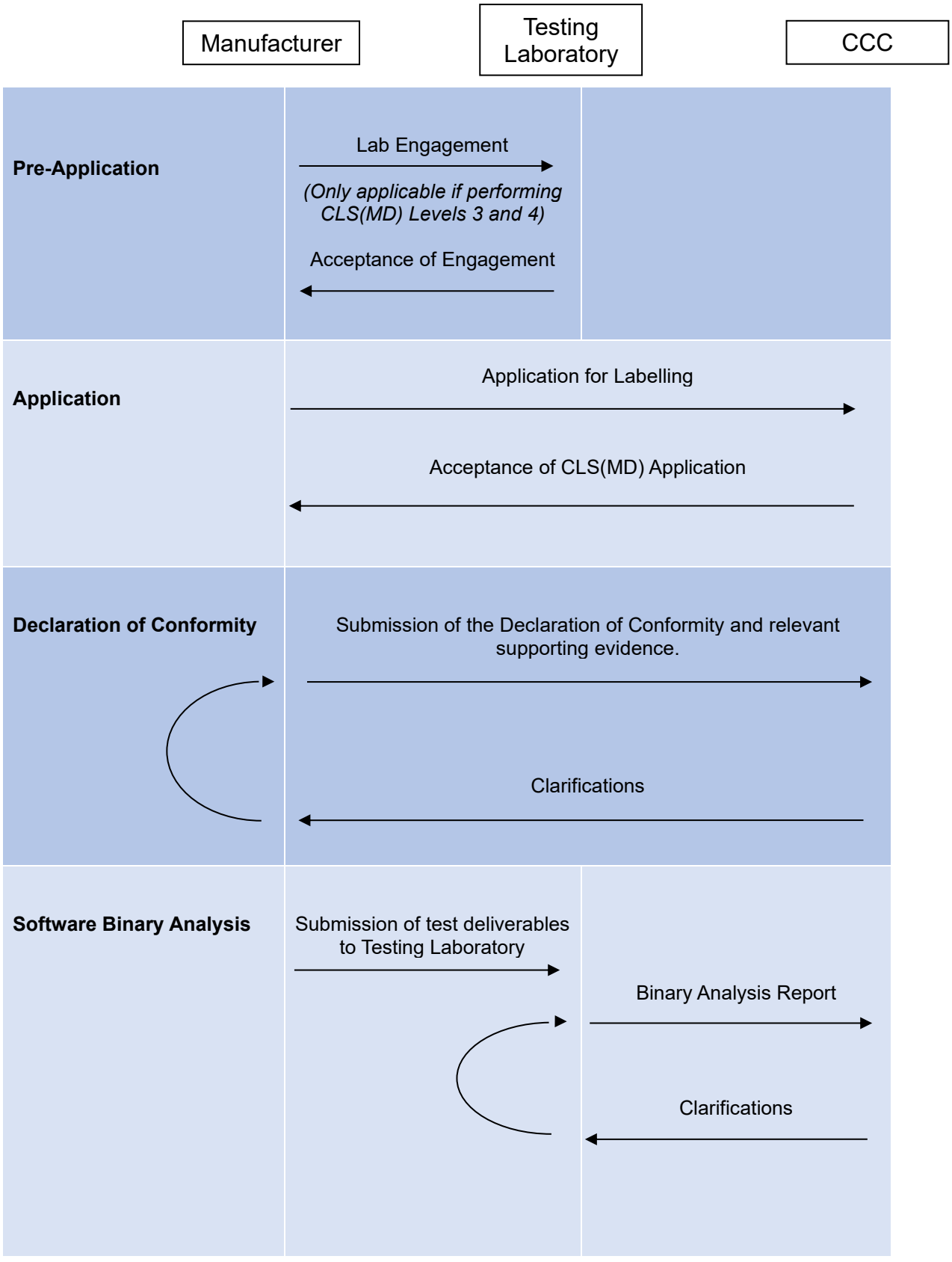
a. **CCC**: The Cybersecurity Certification Centre (CCC) operates under the ambit of CSA. CCC oversees the entire management and operations of the scheme, reviews and validates the work performed by the testing laboratory to ensure consistency and quality of the testing. CCC is the authority to issue the CLS(MD) label and to conduct random checks on manufacturers and retailers to ensure that the CLS(MD) labels are correctly used.

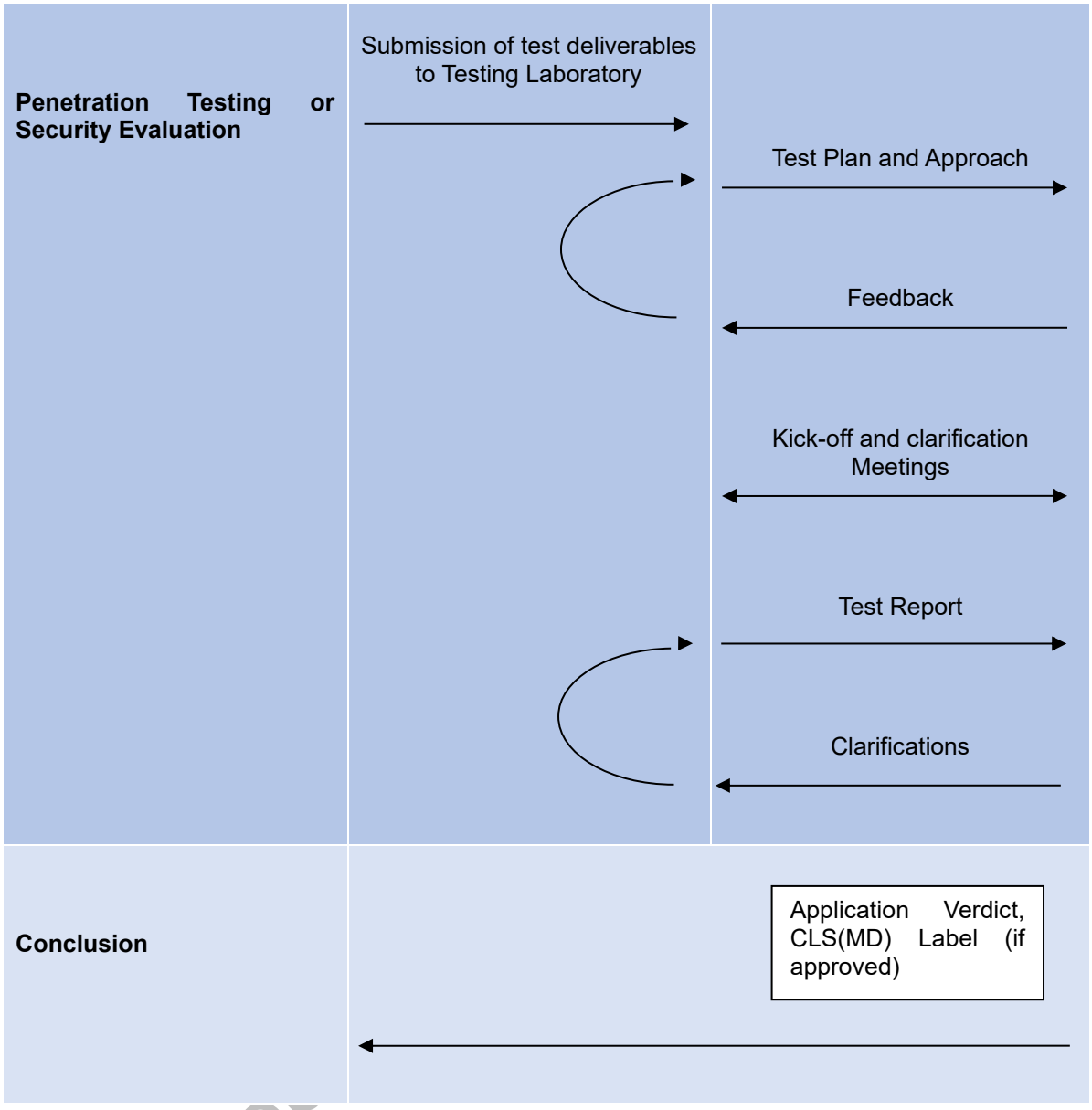
b. **Manufacturer**: The manufacturer is the applicant who develops, manufactures, or creates the consumer product. The manufacturer is responsible for providing the information required by the CLS(MD) and supports the TL for the conduct of the testing.

c. **Testing Laboratory (TL)**: The TL is an independent commercial testing laboratory which is approved under the CLS(MD). The TL is involved only in Tier 3 and Tier 4. The TL conducts assessment tests on the consumer product provided by the manufacturer and reports its results to the CCC and the manufacturer.

Draft Copy for Sandbox Use Only

8.1.3 There are four main phases to the entire labelling process.





Draft Co

8.2 Pre-Application Phase

8.2.1 Feasibility Study

Apart from commercial considerations, a manufacturer intending to apply for label should carefully study the requirements of the CLS(MD) and determine which level of the labelling scheme is suitable for the product.

The manufacturer shall ensure that the required supporting evidence are available before making an application.

If the intended application is for Level 3 and 4, prior to the application, the TL shall conduct a readiness assessment of the manufacturer and the Device Under Test (DUT). The intention of this procedure is to prevent project delays by ensuring that required components (documentation, etc.)

of the projects are available, and that the device's security is adequate to meet the requirements Level 3 or 4 and is in a suitable state for testing.

8.2.2 Lab Engagement

For Level 3 and 4, the manufacturer is required to engage a TL to perform the associated tasks required at the specific tiers. The terms of engagement shall be as negotiated between the manufacturer and the TL. CCC will not be involved in any contractual arrangements between the manufacturer and the TL, nor shall CCC be a party to the contract between the manufacturer and the TL.

The list of approved TLs for CLS(MD) are available at https://www.csa.gov.sg/cls-md.

8.2.3 Enquiry for Labelling

a. Enquiry for labelling under the CLS(MD) should be addressed to the CCC at the following address:

The Technical Manager,
Cybersecurity Labelling Scheme for Medical Devices
Cybersecurity Certification Centre
Cyber Security Agency of Singapore (CSA)
5 Maxwell Road MND Complex #03-00 Tower Block
Singapore 069110

Or

cls_md@csa.gov.sg

8.3 Application for Labelling

8.3.1 All applications for labelling are to be made via the GoBusiness Licensing Portal at https://www.gobusiness.gov.sg.

8.3.2 The following deliverables (depending on the intended CLS(MD) Label level) shall be submitted during the online application:

CLS(MD) Label	Assessment Tiers and Submission Requirements
Level 1	Declaration of Conformity and related Supporting Evidence
Level 2	Declaration of Conformity and related Supporting Evidence
Level 3	Declaration of Conformity and related Supporting Evidence, Binary Files (Device firmware and companion applications are to be provided to the TL)
Level 4	Declaration of Conformity, Binary Files (Device firmware and companion mobile applications are to be provided to the TL)

Table 2 - Application Submission Requirements

8.3.3 All documents and deliverables to be submitted shall be provided in

Draft Copy for Sandbox Use Only

English.

8.3.4 For devices intended for Level 4, the CCC reserves the right to request for a unit of the DUT to be provided to the CCC.

8.3.5 More specific application requirements are available in CLS(MD) Publication #2 – Scheme Specifications [1].

8.3.6 Upon the submission of the application, CCC shall review the application and inform the applicant via email of the acceptance or rejection of the application.

8.4 Declaration of Conformity

8.4.1 The specific requirements on the Declaration of Conformity are specified in CLS(MD) Publication #2 – Scheme Specifications [1].

8.5 Software Binary Analysis

8.5.1 The specific requirements on Software Binary Analysis are specified in CLS(MD) Publication #2 – Scheme Specifications [1].

8.6 Testing Phase (Only for Level 3 onwards)

8.6.1 The required testing tasks are dependent on the CLS(MD) level that the manufacturer wishes to attain. Detailed requirements of the each of the levels are detailed in CLS(MD) Publication #2 – Scheme Specifications [1].

8.7 Conclusion - Awarding of the CLS(MD) Label

8.7.1 Upon completion of testing, and if the product is deemed to fulfil CLS(MD) requirements, CCC will issue the CLS(MD) label and update the list of labelled products that is published on the CLS(MD) website.

8.7.2 The labelled consumer product shall be listed on CSA's website.

8.8 Changes to Conditions for Labelling

8.8.1 CCC reserves the right to make changes to CLS(MD) Publications and to any conditions for labelling under the CLS(MD). If such changes substantially affect ongoing test activities, CCC shall be entitled to require the manufacturer to submit a fresh application for labelling.

8.9 Cryptography

8.9.1 The CLS(MD) does not address the inherent qualities of cryptographic algorithms. Manufacturers are encouraged to implement cryptographic algorithms based on industry standards. Proprietary cryptographic algorithms are generally discouraged.

Draft Copy for Sandbox Use Only

9 SMALLEST ASSESSABLE MEDICAL DEVICE UNIT

9.1.1 Applications to the CLS(MD) shall be for each individual smallest assessable medical device unit(s). The CLS(MD) does not allow for applications to be made for medical device system(s) which comprises of multiple smallest assessable medical device units.

9.1.2 The smallest assessable medical device unit are typically characterised by the following:

- Is not an analogue device or a peripheral.
- Has its own firmware or operating system, and has the ability to communicate with other medical device units or peripherals.

10 GROUPING OF APPLICATIONS

10.1.1 The CLS(MD) allows models from the same product family to be grouped together under a single application to facilitate application efficiency.

10.1.2 The eligibility criteria are as follow:

- For Level 1 and 2 applications, the different models from the same product family shall utilise similar firmware code with the same functionalities contributing to security. The differences in the firmware shall be minor, limited to differences in user interface (look and feel) and differences in the drivers due to the different underlying hardware chipsets used.

- For Level 3 and 4 applications, the hardware and software components that contribute to the security (e.g., processor/SoC chipset, Wi-Fi/Bluetooth/Zigbee chipset, security modules, trusted platform modules, etc.) must be the same across models.
    - If there are differences in the hardware and software across the models, they shall be limited to components that do not contribute to the security of the device. For example, these differences shall be limited to physical look & feel, supported Wi-Fi/LAN connection speed, or user functionalities. For devices with different hardware and software components that contribute to the security of the device, these devices shall not be grouped.

Draft Copy for Sandbox Use Only

11 APPLICANT OBLIGATIONS

11.1 Vulnerability Disclosure

11.1.1 Whenever a vulnerability is reported to the manufacturer, the manufacturer shall notify CCC as early as possible, detailing the vulnerability, the impact, remediation plans and timeline.

11.1.2 For vulnerabilities that result in the medical devices to be suspected of being potentially harmful to users, as per HSA requirements, the manufacturer shall report a Field Safety Corrective Action (FSCA) to HSA.

11.2 Defined Support Period for Security Updates

11.2.1 Another fundamental requirement under the CLS(MD) is for the manufacturer to provide information on the defined support period. The defined support period refers to the minimum period in which security updates for the device will be provided by the manufacturer.

Draft Copy for Sandbox Use Only

12 CYBERSECURITY LABEL

12.1 Label

12.1.1 A sample of the CLS(MD) label as follows:

Figure 2 - Sample of CLS(MD) Labels

12.1.2 The following details are provided in the label:

a. Cybersecurity level as denoted in the number of cross symbols present on the label.

b. Registration Identifier in the format of “CSA/MDxxxxxx”.

c. QR code containing the URL to the medical device’s listing on the CLS(MD) labelled product list webpage.

12.2 Label Validity

12.2.1 Labels are valid for the period in which the manufacturer will support the device with security updates, up to a maximum of 3 years.

12.2.2 While the general validity is for a period of a maximum of 3 years, the label could be revoked if any of the conditions in Section 12.9 is met.

12.2.3 Upon the expiry of the label, a new CLS(MD) application is required to obtain a new label.

12.2.4 Information on the validity period of the label will be provided on the CLS(MD) product list webpage.

12.3 Requirements of the Cybersecurity Label

12.3.1 The Cybersecurity Label must:

a. Be of the following dimensions:
   i. Small: 2.5cm (width) by 1cm (height)
   ii. Regular: 4cm (width) by 3cm (height)
   iii. Large: 6cm (width) by 4.5cm (height)

b. Be of font, typeface, font colour as indicated in the label guide;

Draft Copy for Sandbox Use Only

c. Be of the shape, colour and contain text that is of the typeface as what is specified by the label guide, legible and in the English language only;

d. Contain information that is consistent with or drawn from the test report for the tested good to which the Cybersecurity Label relates;

e. Be printed in an indelible manner and with a minimum resolution of 300 pixels per inch; and

f. Be made of such material as CCC may approve.

12.4 Requirements on the Affixing of the Label for PUO and Non-PUO Medical Devices

12.4.1 Non-Professional Use Devices. It is a requirement for manufacturers to affix the CLS(MD) labels on non-professional use medical devices.

12.4.2 Professional Use Devices. It is optional for manufacturers to affix the CLS(MD) labels on professional use medical devices. If the manufacturer chooses to affix the CLS(MD) labels, the guidelines within Chapter 12.5 shall be followed.

12.4.3 The affixing of the CLS(MD) label can be conducted prior to or after importation into Singapore. The manufacturer's licence is not required for the affixing of the CLS(MD) label on the device packaging, provided there is no breach to the primary packaging that maintains the sterility or integrity of the medical device. However, the conduct of this activity should follow the Good Distribution Practice for Medical Devices (GDPMDS) principles.

12.5 Requirements on the Display of the Label for Software as a Medical Devices (SaMD)

12.5.1 For Software as a Medical Devices (SaMD) that are supplied without a physical form, the SaMD may implement electronic labelling as an alternative to physical labelling. Electronic labelling can be implemented by displaying the CLS(MD) label on the equipment's built-in display screen or graphical user interface, or by including the CLS(MD) label within the compliance label section of the software.

12.6 How the Cybersecurity Label is to be Affixed or Displayed

12.6.1 The Cybersecurity Label shall be affixed on either the product's primary packaging or on the product itself **within 6 months from the date of issue**.

12.6.2 The Cybersecurity Labels can be displayed in all advertisements and promotional material of labelled products in local print, broadcast and digital media. This includes, but is not limited to websites, online stores and printed catalogues.

Draft Copy for Sandbox Use Only

12.6.3 In cases where the available space is too small for the Cybersecurity Label to be seen clearly, the rating must be prominently displayed.

12.6.4 If the devices are to be affixed with the Cybersecurity Label, they must have affixed to each of them a Cybersecurity Label that satisfies the following requirements:

a. The Cybersecurity Label is not damaged, defaced or obliterated so as to prevent any information on the Cybersecurity Label from being read;

b. The Cybersecurity Label is affixed in a conspicuous and unobstructed position on the product.

12.7 Labelling Principles

12.7.1 Upon receipt of the CLS(MD) label, the manufacturer agrees to continuously adhere to the following principles:

a. The labelled product continues to fulfil the security requirements for the tier that the product is being labelled with.

b. CCC shall be informed immediately of any changes that could affect the ability of the manufacturer/product to fulfil the CLS(MD) requirements.

c. The manufacturer must not make any statements about its product labelling that CCC deems to be misleading or unjustified. Examples include all models labelled when it is only a specific model that has been issued with the label; claiming the product received a label of higher rating than what is being issued.

d. The manufacturer must not use the cybersecurity label in any way that could discredit the Cyber Security Agency of Singapore and the Cybersecurity Labelling Scheme for Medical Devices.

e. The label must not be modified and shall be used exactly as issued by CCC.

12.8 CCC Audit and Testing

12.8.1 CCC reserves the right to conduct random checks / surveillance and testing of the labelled products. The purpose of the audit is to ensure that labelled products are compliant to the requirements of the CLS(MD) publications. Manufacturers are **not** expected to pay for the random check / surveillance.

12.8.2 For this purpose, CCC may choose to re-test the labelled device using a separate testing laboratory that was not used during the labelling process.

Draft Copy for Sandbox Use Only

12.9 Revocation of the Cybersecurity Label

12.9.1 CCC is entitled to revoke a CLS(MD) label issued under the CLS(MD) forthwith if:

a. The TL or manufacturer is in breach of any terms of CLS(MD) Publications, and/or any other terms as agreed to in writing with CCC;

b. The manufacturer has failed to disclose any known or discovered vulnerabilities that, in CCC's opinion, can undermine the CLS(MD) label;

c. The manufacturer fails to take any corrective measures during the period of grace given by CCC, to the satisfaction of CCC;

d. The manufacturer misuses the CLS(MD) label, CLS(MD) status, or any proprietary names and marks associated with CCC or CLS(MD);

e. The manufacturer makes any statement that misrepresents any aspect of testing or the effect of the labelling under the CLS(MD);

f. CCC finds that the TL was in a position of conflict that impaired its ability to conduct a fair and impartial testing of the device;

g. The labelled device no longer meets the conditions under which the label was granted or does not meet any changed conditions for labels introduced by CCC after the device was originally labelled.

h. CCC discovered that the manufacturer has made a false statement or declaration in any deliverables submitted to CCC.

12.9.2 Upon the revocation of a CLS(MD) label, the manufacturer and the testing laboratory shall immediately cease all use of the CLS(MD) label, or any proprietary names and marks associated with CSA, CCC, or the CLS(MD), and desist from holding the applicable products out as being labelled under the CLS(MD).

12.9.3 CCC will inform the manufacturer and the testing laboratory in writing of the revocation of the CLS(MD) label and will remove the listing of the labelled product from the Labelled Product List (LPL). The project details will be put into the common Historical Product List (HPL).

Draft Copy for Sandbox Use Only

13 ASSURANCE CONTINUITY

13.1.1 Assurance Continuity defines the approach to minimise redundancy in product assessment, allowing a determination to be made as to whether independent assessments need to be re-performed as changes are made to a labelled product to address security issues, minor bugs, improve the operation of the hardware or peripherals, and to add support for new models of equipment.

13.1.2 For major changes that would invalidate the previous test results (i.e., a change in the underlying operating system used, use of a different programming language, the firmware has been reprogramed from scratch, use of a different security architecture), the manufacturer shall subject the CLS(MD) Level 3 or Level 4 product to retesting with a Testing Laboratory.

CLS(MD) Level / Type of changes	**Level 1**	**Level 2**	**Level 3**	**Level 4**
Major change	Label remains valid		Retesting is required.	
Minor change/patch	Label remains valid.			

13.1.3 For minor software updates/patches that does not invalidate the previous test results, the CLS(MD) label will continue to remain valid, on the condition that the product continues to meet the conditions under which the label was granted and any changed conditions introduced by CCC after the device was originally labelled.

13.1.4 The assurance continuity procedures defined in this chapter does not negate HSA's requirements on manufacturers regarding change notifications.

14 RENEWAL OF LABEL

14.1.1 Manufacturers are allowed to apply for a renewal of the current valid CLS(MD) label up to 6 (six) months prior to its expiry, and retain the existing Label ID.

14.1.2 An expired label cannot be renewed. In this scenario, the manufacturer will be required to apply for a new label, and a new label will be issued.

15 REQUIREMENTS FOR CLS(MD) TEST LABORATORY

15.1.1 The testing laboratory must satisfy all requirements as stated in CLS(MD) Publication #3 – Requirements for Testing Laboratory [2].

15.1.2 The testing laboratory is allowed to provide both consultancy and evaluation services for the product under the CLS(MD) if the testing

Draft Copy for Sandbox Use Only

laboratory is able to demonstrate with clear role and logical separation procedures in place as well as appointing qualified evaluators and qualified consultants for the project.

15.1.3 If the testing laboratory is part of an organisation that performs activities other than IT security evaluation (e.g., consultation to product manufacturer), the testing laboratory shall identify actual and potential conflicts of interest and ensure clear separation of control to ensure that there is no undue influence on the evaluation activities.

Draft Copy for Sandbox Use Only

16 MECHANISM FOR COMPLAINTS, DISPUTES AND APPEALS

16.1.1 The objective of the CLS's Complaints, Disputes and Appeals process[3] is to track feedback from stakeholders and to ensure that issues are resolved:

a. Manufacturers may contact CCC directly if they are dissatisfied with any services provided by the testing laboratories regarding their project. CCC holds all raised concerns in strict confidence.

b. Manufacturers or testing laboratories may contact the Head of Cybersecurity Certification Centre directly if they disagree with a decision. CCC holds all raised concerns in strict confidence.

16.1.2 CCC shall acknowledge the receipt of a formal complaint, dispute or appeal and looks into the content of the complaint, dispute or appeal to determine whether the complaint, dispute or appeal relates to test activities for which CCC is responsible.

a. If CCC does not accept the complaint, dispute or appeal, this is explained in writing to the party lodging the complaint.

b. If CCC accepts the complaint, dispute or appeal, it then processes it, recording and verifying all the necessary information (as far as possible) in order to reach a decision regarding the complaint, dispute or appeal.

16.1.3 To begin with, an attempt is made to reach an agreement regarding the disputed matter with the certifier responsible for the procedure concerned.

16.1.4 If any issue cannot be resolved to the satisfaction of the originating party, the originating party may contact CCC. Resolution of the issue is under the responsibility of the Head of the Cybersecurity Certification Centre, whose decision made on any issue raised is final.

Draft Copy for Sandbox Use Only

[3] A dispute is a written statement to CCC indicating disagreement with a decision made by CCC. A complaint is a written statement to the CCC indicating dissatisfaction with a service provided by CCC or the Testing Laboratory. An appeal is a written statement to CCC indicating dissatisfaction with the resolution of a complaint or dispute.

17 FEES

17.1 General Policy

17.1.1 The fees for CCC's work in connection with the labelling process shall be prescribed by CCC and published on the CSA website. CCC reserves the right to review the fees as and when necessary. These costs are based primarily on the type of procedure requested, the specific object to be labelled, the scope desired and the degree of assessment envisaged or required. However, the procedure costs are charged irrespective of the ordering party's attributes (company name, company size, registered office, division, etc.).

17.1.2 All fees are in Singapore dollars and are subjected to GST.

17.1.3 Labelling fees are always charged as agreed – regardless of whether a label has been issued or could not be issued due to technical deficiencies or other deficiencies, the applicant cancelled the procedure or CCC suspended the procedure due to failure to provide the necessary information.

17.1.4 If the manufacturer requires modifications to reports, expert opinions or labels that CCC has already approved, the additional effort will be charged to the manufacturer. This also applies to performing re-labelling, if these become necessary due to reasons caused by the manufacturer.

17.1.5 All fees mentioned in CLS(MD) publications are exclusive of fees charged by testing laboratories for testing work performed.

Draft Copy for Sandbox Use Only

18 LIABILITY

18.1 Disclaimer

18.1.1 CSA makes no representations, warranties or covenants of any kind, whether express, implied or statutory, with respect to the CLS, TLs, or any testing conducted or labels awarded under the CLS, including without limitation any warranties of merchantability, satisfactory quality, fitness for a particular purpose or non-infringement of third party rights and any warranties that they are accurate, reliable or error-free. All implied warranties of any kind are excluded to the maximum extent permitted by law. Any person's use of and/or reliance on the CLS, TLs, or testing conducted, or labels awarded under the CLS(MD) shall be at their own risk.

18.1.2 To the extent permissible by law, in no event will CSA, its officers, directors, employees or any other person acting under the direction of CSA be liable to a manufacturer, manufacturer, TL or any other person for any loss or damage under any theory of liability, whether direct, indirect, incidental, special, consequential or exemplary in nature, arising out of or in connection with the CLS(MD) or any decisions by CSA or any such person in relation to the CLS(MD) if made in good faith in the ordinary course of the discharge of the CSA's duties under the CLS, including but not limited to lost profits, loss of goodwill and business opportunities, costs of procurement of substitute goods or services, business interruption or loss of business information and data, even if the CSA has been advised of the possibility of such damages.

Draft Copy for Sandbox Use Only

References

[1] Cyber Security Agency of Singapore, “CLS(MD) Publication #2 - Scheme Specifications,” Version 0.5, October 2023.

[2] Cyber Security Agency of Singapore, “CLS(MD) Publication #3 - Requirements for Testing Laboratory,” Version 0.3, September 2023.

ACRONYMS

The following acronyms are used in CLS(MD) Publications 1 and 2:

CCC	Cybersecurity Certification Centre
CSA	Cyber Security Agency of Singapore
DUT	Device Under Test
HPL	Historical Product List
LPL	Labelled Product List
TL	Testing Laboratory

Draft Copy for Sandbox Use Only