CCC SP-153-1


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

## Overview of the Scheme

October 2024
Version 1.0

# 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.

## AMENDMENT RECORD

| Version | Date | Author | Changes |
|---|---|---|---|
| 0.5 | October 2023 | Cyber Security Agency of Singapore | Draft |
| 1.0 | October 2024 | Cyber Security Agency of Singapore | Release |

# CONTENTS

# 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 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).

# 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.

[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 13 – Requirements of CLS(MD) Test Laboratory.

# 5 SCOPE OF THE CLS(MD)

5.1.1 The Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)] is a **voluntary scheme**.

5.1.2 **The CLS(MD) operates independently from the HSA registration process.** The HSA registration process, upon approval registers devices into the Singapore Medical Device Register (SMDR) or Class A Medical Device Database.

5.1.3 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 may apply to the CLS(MD):

- 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.

5.1.4 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.

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

## 5.2 Applications for Devices Listed on HSA Class A Medical Device Database or SMDR

5.2.1 Manufacturers may submit applications for the CLS(MD) for medical devices already listed on either the HSA Class A Medical Device Database (applicable to Class A devices) or the Singapore Medical Device Database (applicable to Class B, C, and D devices).

- For such applications, clauses VDP.1, CSUP.1, CSUP.4, RDMP.1 will be considered fulfilled and will not be assessed within the CLS(MD) application.

## 5.3 Applications for Devices Not Listed on HSA Class A Medical Device Database or SMDR

5.3.1 Manufacturers may also submit applications for the CLS(MD) for medical devices that are currently undergoing HSA registration or not yet listed in either the HSA Class A Medical Device Database (applicable to Class A devices) or the Singapore Medical Device Database (applicable to Class B, C, and D devices).

i. For devices **intended** for supply or use in Singapore:

- While an application for the CLS(MD) can be made for medical devices that are currently undergoing HSA registration or not yet listed in either the HSA Class A Medical Device Database or the Singapore Medical Device Database, the CLS(MD) label will be issued only upon confirmation of the device's listing in these databases.

- For such applications, clauses VDP.1, CSUP.1, CSUP.4, RDMP.1 will not be assessed during the CLS(MD) application.

- If a medical device fails to secure listing in either the HSA Class A Medical Device Database or the Singapore Medical Device Database, but the manufacturer would still like to obtain the CLS(MD) label, the manufacturer shall confirm that the medical device is not intended for supply or use in Singapore. Subsequently, the application will be processed according to section 5.3.1.ii.

ii. For devices **not intended** for supply or use in Singapore:

- The medical device will be included in the labelled product list on the CSA website, clearly designated as not registered with HSA and not intended for supply or use in Singapore.

- For such applications, clauses VDP.1, CSUP.1, CSUP.4, RDMP.1 will be assessed during the CLS(MD) application.

- The manufacturer shall not utilise the CLS(MD) label in any manner that CCC would deem to be misleading or unjustified, including any suggestion that the device is approved to be for supply or use in Singapore, or any representation that contradicts the device's non-registered status with HSA.

- Should the intention change, and these medical devices become intended for supply and use in Singapore after the label's issuance, the manufacturer is required to register the device with HSA prior to the supply and use in Singapore.

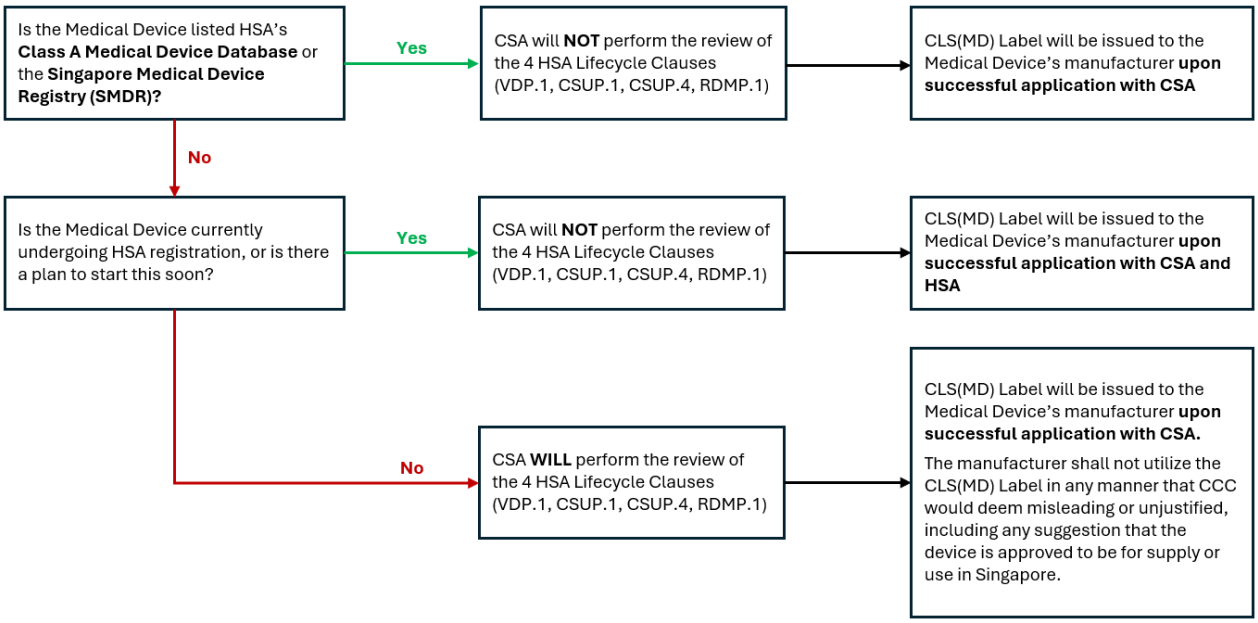



Figure 1 – Application Pathways

# 6 OVERVIEW OF THE CLS(MD)

## 6.1 Overview

6.1.1 Medical devices 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.

## 6.2 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.

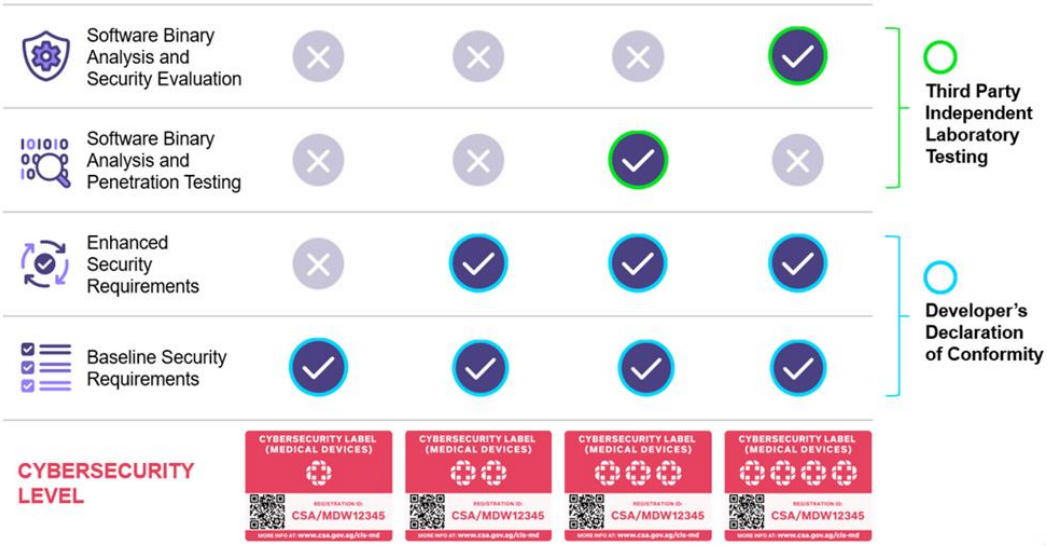



**Figure 2 - Cybersecurity Levels**

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

# 7 CYBERSECURITY LEVELS

7.1.1 This chapter seeks to provide an overview of the four levels within the CLS(MD). The full details of the requirements for each of the levels are provided in CCC SP-101-2 CLS(MD) Pub 2 - Scheme Specifications.

## 7.2 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. | CCC; Manufacturer; Testing Laboratory |
| 2 | Enhanced Security Requirements | | CCC; Manufacturer; Testing Laboratory |
| 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

## 7.3 Level 1 – Baseline Security Requirements

7.3.1 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.

7.3.2 The manufacturer shall engage an approved CLS(MD) Testing Laboratory and submit to them the completed declaration of conformity and supporting evidence, specifying conformity status to the security requirements set out within this level.

7.3.3 The declaration of conformity and supporting evidence shall be reviewed by the Testing Laboratory. If the Testing Laboratory determines that the declaration of conformity and supporting evidence meet the requirements, the manufacturer may submit a CLS(MD) application towards CCC.

7.3.4 The CLS(MD) application shall contain the following:

i. Declaration of Conformity

ii. Supporting Evidence

iii. Testing Laboratory's Assessment of the Declaration of Conformity and Supporting Evidence

7.3.5 CCC shall review the Testing Laboratory's assessment of the Declaration of Conformity and supporting evidence prior to approval. Non-conformity to the security requirements shall result in the failure of this activity.

7.3.6 After the declaration of conformity and supporting evidence have been submitted to CSA, the estimated turnaround for CLS(MD) Level 1 is around 1 working day 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 2 – Enhanced Security Requirements

7.4.1 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.

7.4.2 The manufacturer shall engage an approved CLS(MD) Testing Laboratory and submit to them the completed declaration of conformity and supporting evidence, specifying conformity status to the security requirements set out within this level.

7.4.3 The declaration of conformity and supporting evidence shall be reviewed by the Testing Laboratory. If the Testing Laboratory determines that the declaration of conformity and supporting evidence meet the requirements, the manufacturer may submit a CLS(MD) application towards CCC.

7.4.4 The CLS(MD) application shall contain the following:

i. Declaration of Conformity

ii. Supporting Evidence

iii. Testing Laboratory's Assessment of the Declaration of Conformity and Supporting Evidence

7.4.5 CCC shall review the Testing Laboratory's assessment of the Declaration of Conformity and supporting evidence prior to approval. Non-conformity to the security requirements shall result in the failure of this activity.

7.4.6 The estimated turnaround for CLS(MD) Level 2 is around 1-2 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.

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

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

a. Meeting Enhanced Security Requirements. To ensure that devices 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

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

Software Binary Analysis

7.5.3 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.

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

7.5.5 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.

7.5.6 CCC shall review the Testing Laboratory's report prior to approval.

7.5.7 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

7.5.8 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.

7.5.9 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.

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

7.5.11 CCC shall review the Testing Laboratory's penetration testing report prior to approval.

7.5.12 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.

## 7.6 Level 4 – Enhanced Security Requirements, Software Binary Analysis, Security Evaluation

7.6.1 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

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

Software Binary Analysis

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

Security Evaluation

7.6.4 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.

7.6.5 The manufacturer shall provide sufficient production samples of the device, related user guidance documents, and product security design documentation to the Testing Laboratory to facilitate testing.

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

7.6.7 CCC shall review the Testing Laboratory's report prior to approval.

7.6.8 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 GROUPING OF MODELS UNDER A SINGLE APPLICATION

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

8.1.2 The eligibility criteria are as follow:

- Different models from the same product family must utilise identical firmware code and hardware/software components that contribute to security (e.g., processor/SoC chipset, Wi-Fi/Bluetooth/Zigbee chipset, security modules, trusted platform modules).

- Hardware and software differences across models must be limited to components that do not affect device security, such as physical appearance, user functionalities, or the use of different drivers due to varying underlying hardware components (non-security contributing).

# 9 APPLICANT OBLIGATIONS

## 9.1 Vulnerability Disclosure

9.1.1 The manufacturer shall notify CCC as early as possible upon receiving any report of cybersecurity vulnerabilities or concerns related to their medical device. This notification shall include details of the vulnerability, its potential cybersecurity impact, proposed remediation plans and expected timeline for resolution.

9.1.2 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.

## 9.2 Defined Support Period for Security Updates

9.2.1 The CLS(MD) requires manufacturers to provide information on the defined support period. The defined support period refers to the minimum duration in which security updates for the device will be provided by the manufacturer. The support period shall clearly indicate the minimum date (day, month, and year) until which security updates will be provided.

# 10 GENERAL PROCESS FOR LABELLING OF MEDICAL DEVICE

## 10.1 Process Overview

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

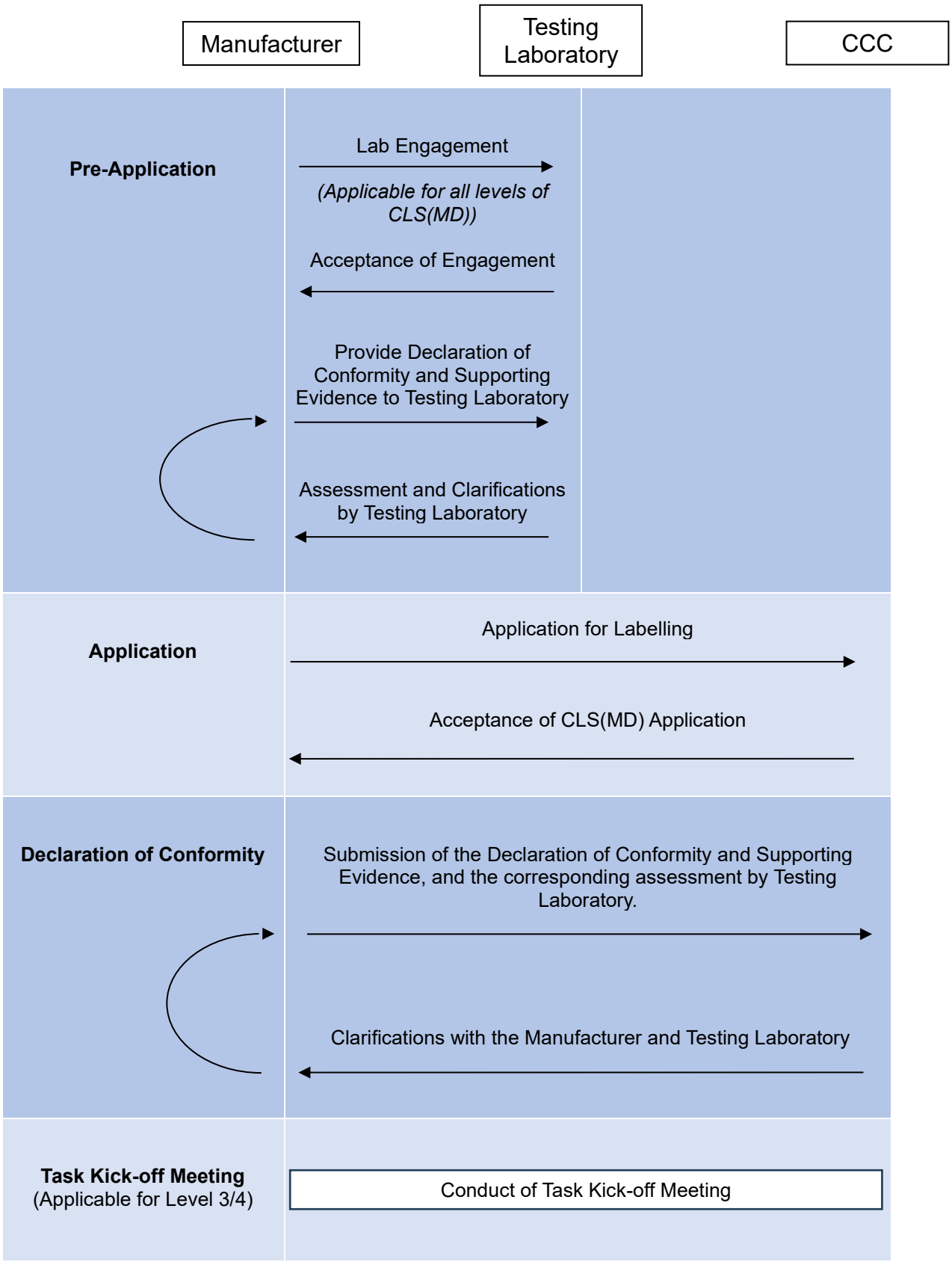
10.1.2 The key roles and responsibilities within the CLS(MD) are as follows:

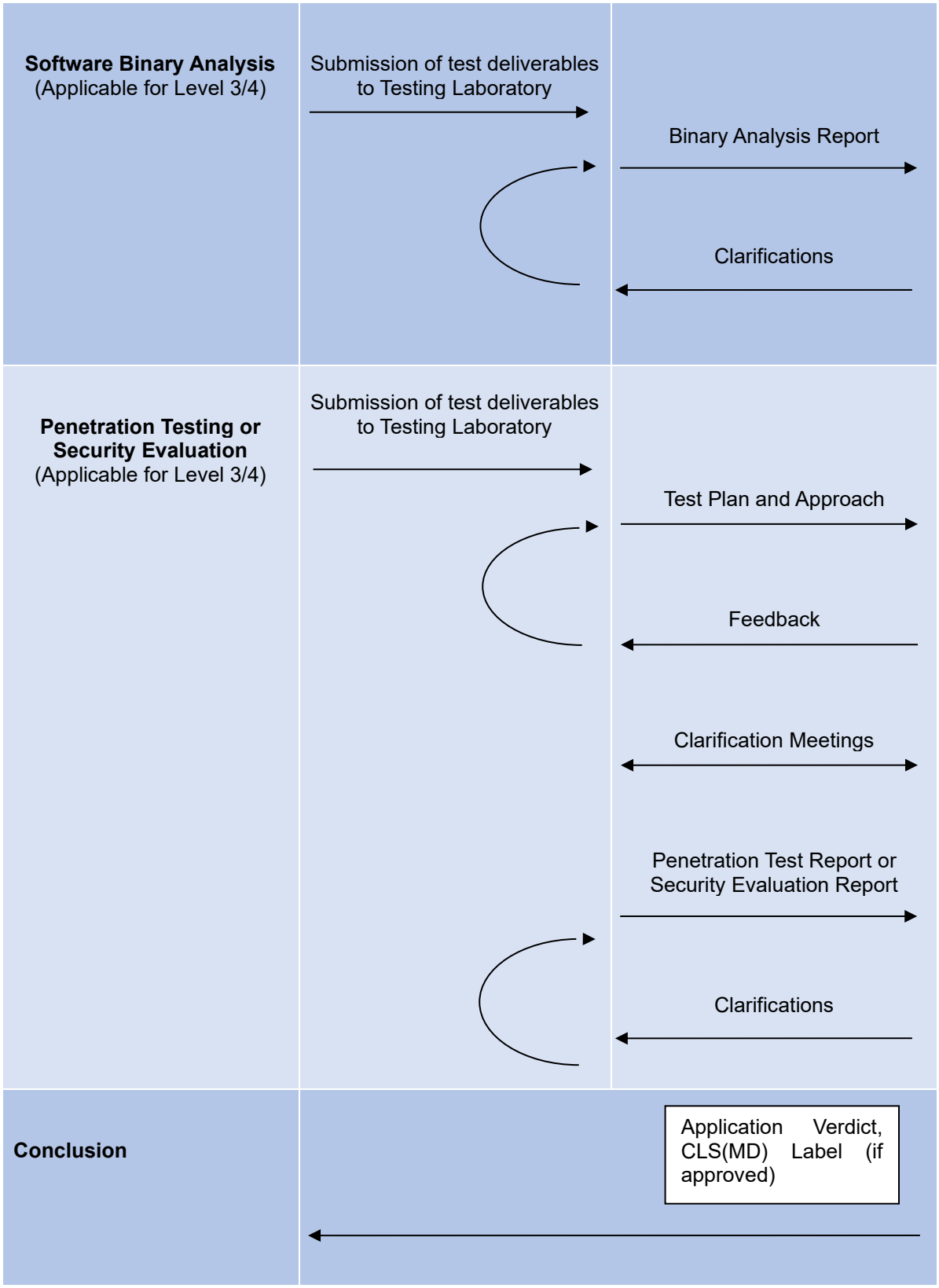
a. **CCC**: The Cybersecurity Certification Centre (CCC) operates under the ambit of CSA. CCC oversees the entire management and operations of the scheme, reviews and validates the work performed by the Testing Laboratory to ensure consistency and quality of the testing. CCC is the authority to issue 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.

10.1.3 The following diagram illustrates the main phases to the entire labelling process.




Software Binary Analysis
(Applicable for Level 3/4)
Submission of test deliverables to Testing Laboratory
Binary Analysis Report
Clarifications
Penetration Testing or Security Evaluation
(Applicable for Level 3/4)
Submission of test deliverables to Testing Laboratory
Test Plan and Approach
Feedback
Clarification Meetings
Penetration Test Report or Security Evaluation Report
Clarifications
Conclusion
Application Verdict, CLS(MD) Label (if approved)

## 10.2 Pre-Application Phase

### 10.2.1 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 Testing Laboratory 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, devices, 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.

### 10.2.2 Lab Engagement

For all levels of the CLS(MD), the manufacturer is required to engage a TL to perform the associated tasks required at the specific levels. The terms of engagement and relevant non-disclosure agreement 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.

### 10.2.3 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

via email at cls_md@csa.gov.sg.

## 10.3 Application for Labelling

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

10.3.2 The registrant company specified in the application must match the company indicated in the device's HSA registration.

10.3.3 The following deliverables (depending on the intended CLS(MD) label level) shall be submitted using the template (available at https://www.csa.gov.sg/cls-md) during the online application:

| CLS(MD) Label | Assessment Tiers and Submission Requirements |
|---|---|
| Level 1 | • Declaration of Conformity and Supporting Evidence<br>• Testing Laboratory's assessment of the Declaration of Conformity and Supporting Evidence |
| Level 2 | • Declaration of Conformity and Supporting Evidence<br>• Testing Laboratory's assessment of the Declaration of Conformity and Supporting Evidence |
| Level 3 | • Provisional Application Work Plan (AWP), outlining the tasks to be performed according to the CLS(MD) requirements and a timeline.<br>• Declaration of Conformity and Supporting Evidence<br>• Testing Laboratory's assessment of the Declaration of Conformity and related Supporting Evidence<br>• Binary Files (Device firmware and companion applications are to be provided to the TL) |
| Level 4 | • Provisional Application Work Plan (AWP), outlining the tasks to be performed according to the CLS(MD) requirements and a timeline.<br>• Declaration of Conformity and Supporting Evidence<br>• Testing Laboratory's assessment of the Declaration of Conformity and Supporting Evidence<br>• Binary Files (Device firmware and companion mobile applications are to be provided to the TL) |

Table 2 - Application Submission Requirements

10.3.4 All documents and deliverables to be submitted shall be provided in English.

10.3.5 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.

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

10.3.7 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.

### 10.4 Declaration of Conformity

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

### 10.5 Task Kick-off Meeting (TKM)

10.5.1 After the application has been accepted under the CLS(MD), the CCC will contact the testing laboratory and the manufacturer for the Task Kick-off Meeting (TKM). The outline for a typical TKM agenda is as follow:

- For all parties to introduce and identify the point-of-contacts (CCC, testing laboratory, manufacturer) involved in the application
- For the CCC to provide a brief description of the CLS(MD) scheme, the application process, and to outline objectives, expectations, limitation and issues.
- For the manufacturer to provide a brief description of the medical device, including how the medical device is used, what are the various components, and the corresponding interfaces/connections.
- For the testing laboratory to provide a brief description of the application work plan, to explain the scope of evaluation and the timeline, to outline the objectives/expectations/limitation/issues, and to schedule relevant dates, frequency and venue for subsequent meetings.

### 10.6 Software Binary Analysis

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

### 10.7 Penetration Testing or Security Evaluation (Only for Level 3 onwards)

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

### 10.8 Conclusion - Awarding of the CLS(MD) Label

10.8.1 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.

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

## 10.9 Changes to Conditions for Labelling

10.9.1 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.

## 10.10 Cryptography

10.10.1 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.

# 11 ASSURANCE CONTINUITY

11.1.1 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.

11.1.2 For devices labelled at Level 1 and Level 2, the label will remain valid without the need for reassessment on the condition that the device continues to meet the conditions under which the label was granted, and including any changed conditions introduced after the device was originally labelled.

11.1.3 For devices labelled at Level 3 and 4, the label will remain valid unless changes to the device invalidate the previous test results, such as a change in the implementation of its security functionalities. To maintain the validity of the label, the manufacturer must engage the Testing Laboratory used during the original application for retesting.

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

# 12 RENEWAL OF LABEL

12.1.1 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.

12.1.2 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.

# 13 REQUIREMENTS FOR CLS(MD) TEST LABORATORY

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

13.1.2 The Testing Laboratory is allowed to provide both consultancy and evaluation services for the product under the CLS(MD) if the Testing 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.

13.1.3 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.

# 14 CYBERSECURITY LABEL

## 14.1 Label

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


Figure 3 - Sample of CLS(MD) Labels

14.1.2 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.

## 14.2 Label Validity

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

14.2.2 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 14.9.2 is met.

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

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

## 14.3 Requirements of the Cybersecurity Label

14.3.1 The Cybersecurity Label must:

a. Be of the following dimensions:
   i. Small: 2cm (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;

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.

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

14.4.1 The digital copy of the label will be provided in .png and .pdf formats.

14.4.2 For the affixing of the labels to the medical device, manufacturers may print out the physical label and affix it to their devices and/or packaging. Manufacturers may also include the label as part of the device's packaging design. Manufacturers may use the label in the marketing collaterals.

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

14.4.4 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 14.5 shall be followed.

14.4.5 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.

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

14.5.1 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.

## 14.6 How the Cybersecurity Label is to be Affixed or Displayed

14.6.1 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**.

14.6.2 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.

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

14.6.4 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.

## 14.7 Labelling Principles

14.7.1 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 level 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, the Ministry of Health, and the Cybersecurity Labelling Scheme for Medical Devices.

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

## 14.8 Provision for Variations of Medical Devices

14.8.1 The CLS(MD) label is specifically awarded to and valid only for the exact scope (or components) of the medical device that was assessed; consequently, if the device is offered in any other form, configuration, or combination – be it as software, hardware or a mix of both – the issued CLS(MD) label cannot be applied to these variations or used to promote them as being labelled under the CLS(MD).

14.8.2 This restriction is in place because any additional components, altered configurations, or bundled items such as a workstation or computer added to the original device, were not within scope of the scope of assessment when the CLS(MD) label was issued.

14.8.3 For instance, a Software as a Medical Device (SaMD) that achieve a CLS(MD) level 1 label cannot use this same label when the software is sold in a different configuration or bundled with a workstation or computer, nor can the manufacturer represent such variations as being CLS(MD) labelled.

## 14.9 CCC Audit and Testing

14.9.1 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.

14.9.2 For this purpose, CCC may choose to re-test the labelled device using a separate Testing Laboratory that was not used during the application.

# 15 USE OF PROTECTIVE MARKS, LOGOS AND ADVERTISEMENT

## 15.1 Advertisement and promotion of labelled devices

15.1.1 Proper and appropriate use of marks/labels is contractually imposed on the applicant, see 14.7 above.

15.1.2 The following guidelines apply to the CLS(MD) Label:

a. The CLS(MD) Label may be used by a manufacturer in conjunction with advertising, marketing, and selling of its devices, where such products have successfully attained the CLS(MD) label under the CLS(MD) and are listed on the Labelled Product List (LPL).

b. The labelled product name and model number, as listed on the LPL, must be included in any product packaging or publicity materials in which the CLS(MD) Label also appears.

c. Where any product packaging or publicity material refers to the labelled product and to other products, the layout of information relating to the products relative to the position of the CLS(MD) Label should not be used in a manner that would or would likely mislead the public into thinking that a product is labelled under the CLS(MD) when in fact it is not.

d. In relation to product displays, the CLS(MD) Label should be displayed near the labelled product or its replica or image in a manner that makes it clear that the CLS(MD) Label refers to the labelled product.

e. The CLS(MD) Label must be used in the form depicted above. It shall not be altered in any way except for size and monochromatic colour schemes.

f. CSA reserves the right to require the manufacturer to submit samples of their proposed use of the CLS(MD) Label for prior approval.

15.1.3 The following are examples of acceptable promotional language that can be used in conjunction with the advertising, marketing, and sale of a product for which the label is issued:

- “Labelled in conformity with the CLS(MD) [Level 1/2/3/4]”

- “[Product Name and Model Number] by [Manufacturer] has been labelled under the Cybersecurity Labelling Scheme for Medical Devices, CLS(MD), to meet [Level 1/2/3/4] requirements. Conditions for the Label can be found at https://www.csa.gov.sg/cls-md.”

- "[Product Name and Model Number] by [Manufacturer] has been labelled under the terms of the Cybersecurity Labelling Scheme for Medical Devices. Conditions for the label can be found at https://www.csa.gov.sg/cls-md."

15.1.4 As show above, all promotional language must include a statement to inform the audience of the website address https://www.csa.gov.sg/cls-md at which the conditions of the label under the CLS(MD) can be found.

15.1.5 Labelling under the CLS(MD) merely indicates that a product meets with specifically identified criteria under the CLS(MD). It is not a guarantee or assurance by CSA or an assumption by CSA of any responsibility toward any person of the quality of the product or effects of using the product. Manufacturers and Testing Laboratories must avoid making statements that indicate this or may give this impression.

15.1.6 The following are examples of unacceptable promotional language:

- "[Manufacturer or its product or service] is endorsed/ recommended/ approved/ sponsored/supported/ guaranteed by the Cyber Security Agency of Singapore"

- "[Manufacturer or its product or service] is under a guarantee/warranty by the Cyber Security Agency of Singapore"

## 15.2 Response to Misuse

15.2.1 Any misuse of CLS(MD) label shall, without prejudice to any other rights and remedies of CSA or its licensor(s), entitle CSA to take any or all of the following actions:

a. CSA will inform the relevant party to adopt the correct use;

b. CSA will remove all reference and material from the CLS(MD) website mentioning the affected product or label;

c. CSA will publish on its website a note regarding any misuse.

15.2.2 Any false, misleading or improper statement about the CLS(MD) shall, without prejudice to any other rights and remedies of CSA or its licensor(s), entitle CSA to take any or all of the following actions:

a. CSA will inform the relevant party to correct such false, misleading or improper statements about the CLS(MD);

b. CSA will publish on its website a note regarding any misuse.

# 16 REVOCATION, TERMINATION AND WITHDRAWAL

## 16.1 Revocation of the Cybersecurity Label

16.1.1 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.

16.1.2 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).

16.1.3 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).

## 16.2 Termination of On-Going Applications

16.2.1 The CCC is entitled to terminate an ongoing application procedure without issuing a label at any stage forthwith by notice in writing to the manufacturer if:

a. The manufacturer has not paid any sums due to CCC in respect of the application;

b. The Testing Laboratory or the manufacturer has not engaged in any testing or application activity for more than 8 consecutive calendar weeks;

c. The application process extends beyond 6 calendar months from the date of acceptance from the CCC without a timely extension request (which must be submitted before the 6-month mark);

d. The application process exceeds 1 full calendar year from the date of acceptance from the CCC;

e. All necessary fixes, mitigations or changes to meet requirements are not completed within the allowed timeframe (either the initial 6 months or the extended periods, if approved). In addition, if the CCC deems the implemented resolutions insufficient (e.g., due to high residual risk) or inappropriate;

f. The Testing Laboratory or the manufacturer fails to take any action within the requisite timeframe in the application work plan, or otherwise stated by the CCC, and has not obtained the approval of the CCC to a revised timeframe;

g. The scope of the application changes such that the medical device under application no longer fulfils the requirements for admittance into the scheme.

h. The manufacturer or the Testing Laboratory has suspended or terminated a project in accordance with the terms of the contract entered between them. In that event, the party that has suspended or terminate the project shall notify the CCC in writing of the suspension or termination within seven (7) calendar days thereof;

i. The Testing Laboratory’s quality of work or intermediate reports is/are repeatedly insufficient, the CCC requires frequent corrections, and/or the Testing Laboratory fails to meet the deadlines as outlined in the application work plan.

j. The manufacturer’s submissions repeatedly fail to address corrective actions, to provide required clarity, and/or fail to meet deadlines as outlined in the application work plan.

16.2.2 The CCC may also suspend or terminate an on-going application procedure under the CLS(MD) for reasons given in 16.1.1 above. Suspension means that the CCC may allocate its resources to other projects. Suspension can apply for the same reasons as termination but may also apply in cases where the manufacturer and the Testing Laboratory need to change the application work plan due to findings or other reasons for project delay, and where the updated application work plan cannot be established within 30 calendar days after the CCC has requested a new version of the application work plan from the Testing Laboratory. Suspension aims to allow the developer to focus on issues of testing and/or planning without the need for the CCC to keep resources allocated. The application procedure can resume after the CCC has sufficient evidence that the application work plan can be achieved and has the same or equivalent resources available as before suspension.

16.2.3 The CCC may consult with the Testing Laboratory and the manufacturer to confirm the status of the project before proceeding to inform them in writing of the decision to terminate the application procedure.

16.2.4 Upon the termination of an application procedure under the CLS(MD), the CCC will close its file and the CCC resources assigned to the project will be released.

### 16.3 Withdrawal from On-Going Application Procedure

16.3.1 Where a manufacturer wishes to terminate its appointment of a Testing Laboratory and wishes to engage another Testing Laboratory to continue an application procedure under the CLS(MD), such replacement shall be subject to the prior written approval of the CCC and on such terms and conditions as the CCC shall deem fit. The CCC reserves the right to reject a replacement of Testing Laboratory and to require the manufacturer to re-apply to the CCC and go through a fresh application process.

16.3.2 When a manufacturer wishes to withdraw an ongoing application procedure, the manufacturer shall inform the CCC in writing.

16.3.3 Nothing in this CLS(MD) publication prevents a Testing Laboratory from withdrawing from an application procedure. The Testing Laboratory's rights to withdraw from an application procedure is subject to the terms of the agreement between the Testing Laboratory and the manufacturer. The Testing Laboratory shall give the manufacturer and the CCC advanced written notice of any withdrawal from an application procedure. Upon the withdrawal of the Testing Laboratory from an application procedure, the manufacturer may decide to try to continue the project with another Testing Laboratory or withdraw the project. The manufacturer shall inform the CCC of its decision in writing and obtain the CCCs approval of the replacement Testing Laboratory within such time as the CCC shall specify, failing which the application procedure shall be deemed withdrawn from the CLS(MD).

## 16.4 Survival

16.4.1 Any obligations of a manufacturer or Testing Laboratory under the CLS(MD) or their respective agreements with the CCC which by their nature would continue beyond termination or expiration thereof, including without limitation the obligations set out in sections 17, 19, 20, 23 of this publication, shall survive such termination or expiration.

# 17 INFORMATION PROVIDED BY/TO THE CCC

## 17.1 Public Information

17.1.1 CSA maintains a public website that contains a broad range of information about the CLS(MD), including the publish of the labelled product list (LPL) and the archived product list (APL) containing information of the medical devices labelled under the CLS(MD). Information that will be made publicly available includes the device's details (product naming, model number, etc.), device's HSA risk classification, HSA registration number, device's product website, and support duration,

17.1.2 The information informs the public of the labelled medical devices that are available and provides a source of reference for users to verify the current status of issued labels.

## 17.2 Confidential Information

17.2.1 The manufacturer or the Testing Laboratory shall review and confirm promptly in writing the release of information by the CCC before it is made available to the public. Such confirmation shall be provided within the time stipulated by the CCC, failing which the information may be released by the CCC free from any obligation of confidentiality.

17.2.2 It is the responsibility of the manufacturer and the Testing Laboratory (as the case may be) to ensure that any information published by the CCC does not contain any proprietary or protected information.

17.2.3 Any information that is not publicly releasable must be explicitly marked or labelled as such by the manufacturer or the Testing Laboratory (as the case may be) before being delivered to the CCC.

17.2.4 Notwithstanding any of the above, the CCC will not be liable for the disclosure of information designated as confidential or proprietary if the CCC determines that withholding the information is contrary to law.

17.2.5 Except with the written consent of the CCC, the manufacturer and the Testing Laboratory shall not disclose to any person any information, documents, materials provided by the CCC where the same has not been made publicly available by CSA ("CCC Confidential Information").

17.2.6 The manufacturer and the Testing Laboratory shall not, without the prior written consent of the CCC make use of any CCC Confidential Information other than for the purposes of the project for which the CCC Confidential Information was disclosed to them.

17.2.7 The manufacturer and the Testing Laboratory shall keep confidential the CCC Confidential Information and shall only disclose it to their employees on a need-to-know basis for the purposes of the project for which the CCC Confidential Information was disclosed. Without prejudice to the generality of the foregoing, no CCC Confidential Information shall be stored or distributed by the manufacturer or the Testing Laboratory outside its local protected IT infrastructure. The manufacturer and the Testing Laboratory each undertake to take such steps as shall be necessary to protect the CCC Confidential Information and to notify the CCCC as soon as it becomes aware of any unauthorised use of the whole or any part of the CCC Confidential Information.

17.2.8 All documents and other materials containing the CCC Confidential Information shall, at the CCC's request, be returned or otherwise disposed of in the manner specified by the CCC.

### 17.3 Proprietary Information

17.3.1 Nothing in this document shall affect any person's ownership rights in and title to that person's pre-existing Intellectual Property (IP) or IP independently brought into existence or acquired by that person without reliance on any CLS(MD) IP. The term "IP" is defined in 20.3 below. All documents and other materials provided by the CCC to the manufacturer, or the Testing Laboratory shall remain property of CSA and shall at the CCC's request be returned to the CCC or disposed of in the manner specified by the CCC.

17.3.2 Before delivering any IP to the CCC, the manufacturer and the Testing Laboratory shall ensure that it owns or has all the necessary right, power and authority to disclose such IP to the CCC.

17.3.3 Before requesting for the labelling of a medical device under the CLS(MD), each manufacturer shall ensure that it owns the medical device or has all the necessary right, power and authority to make such a request.

17.3.4 The manufacturer and the Testing Laboratory shall, if required by the CCC, do all acts and execute or procure the execution of such documents as may reasonably be required in order to perfect, protect or enforce any of the CCC's rights hereunder to the IP provided by the manufacturer or the Testing Laboratory.

### 17.4 Retention of Records

17.4.1 CCC will maintain a record system providing a retention period of 5 years for documents related to the applications. The record system will be managed with procedures for the access to protected information, and for the creation, marking, storage, transmission, copying and disposal of protected information.

# 18 MUTUAL COOPERATION

18.1.1 The manufacturer and Testing Laboratory shall adhere to the timeframes set out in the application work plan (where applicable) or otherwise approved by the CCC for the performance of their respective obligations in relation to applications under the CLS(MD) or (where applicable) activities under the Assurance Continuity.

18.1.2 The manufacturer and Testing Laboratory shall provide each other and the CCC, as applicable, with such information, documentation, and materials as they shall each require with reasonable promptness and attend such meetings with each other and/or the CCC as required from time to time.

18.1.3 The manufacturer and Testing Laboratory shall, as applicable, co-operate with each other and the CCC in order to fulfil their respective obligations under the CLS(MD) in a timely and efficient manner.

18.1.4 The manufacturer and Testing Laboratory shall, as applicable, co-operate with the CCC in any promotional activities for the CLS(MD) undertaken by the CCC and render such support and assistance as the CCC may reasonably require from time to time.

# 19 CONFLICTS OF INTEREST

## 19.1 General Obligation to Avoid Conflicts of Interests

19.1.1 As noted above, the manufacturer may hire a Testing Laboratory to provide advice, assistance and consultancy services in the course of preparing for an application or Assurance Continuity under the CLS(MD). Such services may include reviewing and preparing supporting evidence and assisting in resolving testing issues. As used in this section, the term “consultancy services” shall refer to the services described in this paragraph.

19.1.2 Hiring a Testing Laboratory to provide consultancy services is not strictly required, nor is the CCC involved in any party’s decision to do so. The scope of the consultancy services is a matter for negotiation between the Testing Laboratory and the party hiring it for such consultancy services.

## 19.2 Duty to Disclose Conflict of Interests

19.2.1 For each application under the CLS(MD), the Testing Laboratory shall notify the CCC of any known or potential conflict of interests relevant to that application.

19.2.2 The CCC will determine whether a conflict of interest exists on a case-by-case basis. The CCC is the final arbiter in determining whether a potential or actual conflict of interest exists and whether the Testing Laboratory should or should not participate in the application under the CLS(MD).

## 19.3 Conflict of Interest Guidelines

19.3.1 The guidelines in this section are intended to assist Testing Laboratories to avoid conflict of interest situations but are not exhaustive.

19.3.2 The Testing Laboratory shall not accept the of testing any product developed, manufactured, or sold by an entity that possesses an ownership interest in the Testing Laboratory or in which the Testing Laboratory has an ownership interest. The term “ownership interest” shall include any percentage of ownership which is greater than 5%.

19.3.3 The Testing Laboratory must not have entered into an agreement that would result in the Testing Laboratory directly benefitting financially from commercial sales of the device being evaluated or in which the Testing Laboratory has sole distributorship for the labelled device.

19.3.4 Neither the Testing Laboratory nor its parent company, affiliates or any individual Testing Laboratory staff member concerned with a particular testing shall have a vested interest in the outcome of that evaluation.

19.3.5 A Testing Laboratory staff member or testing team member cannot, under any circumstances:

- Be concurrently employed/appointed in another unit of the organisation or another organization which develops medical devices;
- Own shares of organization which develops medical devices; and
- Develop medical devices for public circulation (e.g. open source) or commercial purposes.\

19.3.6 The Testing Laboratory must ensure that there is sufficient separation of control and influence in order that its parent company or affiliates cannot exert undue influence on the outcome of testing activities and proprietary or confidential testing information cannot be inappropriately accessed by its parent company or affiliates.

19.3.7 The Testing Laboratory shall only used the staff members as named in the application work plan and approved by the CCC. Any changes to the team must be communicated and approved by the CCC in advance. In addition, any new staff assigned to the project and approved by the CCC must submit an additional declaration of not having any conflict of interest in the project. A director of the Testing Laboratory or such other person in a similar capacity with authority to bind the Testing Laboratory must also provide a declaration that such new staff are not in a position of conflict.

# 20 MECHANISM FOR COMPLAINTS, DISPUTES AND INTELLECTUAL PROPERTY

## 20.1 CLS(MD) IP

20.1.1 The entire right, title and interest (including without limitation intellectual property rights) in and to any and all trademarks and logos of the CCC and CLS(MD) (the “CLS(MD) Marks”), CLS(MD) labels and other IP (defined below) provided by or obtained from CSA (collectively the “CLS(MD) IP”) belong to CSA and/or its licensor(s).

20.1.2 The manufacturer may use the CLS(MD) label and such CLS(MD) Marks as the CCC may specify in writing from time to time strictly for the purpose of indicating that the medical device named in the CLS(MD) label has been tested and labelled under the CLS(MD) at the designated level.

20.1.3 The Testing Laboratory may use such CLS(MD) Marks as CSA may specify in writing from time to time strictly for the purpose of indicating that the Testing Laboratory has the approval of CSA to conduct testing in Singapore under the CLS(MD) at the designated levels.

20.1.4 Any goodwill generated by the use of the CLS(MD) Marks shall accrue to CSA and its licensor(s).

20.1.5 Any rights granted to use any CLS(MD) IP are personal to the manufacturer and the Testing Laboratory. The manufacturer and the Testing Laboratory shall not grant sub-licenses to or otherwise authorise any third party or otherwise assign its right to use the CLS(MD) IP for any purpose whatsoever.

20.1.6 The manufacturer and Testing Laboratory shall immediately discontinue the use of the CLS(MD) IP) and return to CSA or destroy all materials bearing CLS(MD) IP upon written notice by CSA.

## 20.2 CLS(MD) IP Guidelines

20.2.1 Manufacturers and Testing Laboratories shall comply with any applicable guidelines in the CLS(MD) publications or issued by CSA from time to time regarding their use of any of the CLS(MD) IP.

### 20.3 IP

20.3.1 In this document, “IP” means any ideas, data, inventions, discoveries, developments, enhancements, works of authorship, programs, and technical, business and other information and any property rights protected under the patent, copyright, mask work rights, trade secret, trademark or other intellectual property or moral rights law of any state or national government including all rights under any registrations issued by any governmental authority with respect to the said ideas, data, inventions, discoveries, developments, enhancements, works of authorship, programs, and technical, business and other information, and the said property rights as well as all rights under any pending applications for registration and any applications for registration.

## 21 APPEALS

21.1.1 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.

21.1.2 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.

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

[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.

21.1.4 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.

# 22 FEES

## 22.1 General Policy

22.1.1 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.).

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

22.1.3 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.

22.1.4 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.

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

22.1.6 Upon withdrawal, suspension, or termination of an application, there will be no refund of any fees or payments received by CCC, and no demands or claims shall be made against the CCC in connection with such withdrawal, suspension or termination of the application. Outstanding payments (if any) shall become immediately due and payable by the applicant. To subsequently obtain the cybersecurity label for the same device, a fresh application must be made.

# 23 LIABILITY

## 23.1 Disclaimer

23.1.1 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.

23.1.2 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.

## 23.2 Indemnity

23.2.1 To the extent permissible by law, each Testing Laboratory shall indemnify, defend and hold harmless and release CSA and its agents, directors, officers, employees, successors, assigns and representatives thereof (collectively the "Releasees") from and against any and all claims, demands, suits, actions, judgments, damages, costs, losses, expenses (including all legal fees and expenses) and other liabilities arising from, in connection with or related in any way, directly or indirectly, to the breach of any warranties or obligations of the Testing Laboratory under the CLS(MD) Terms, any act, neglect or omission by the Testing Laboratory or its agents, directors, officers, employees, successors, assigns and representatives and/or any dispute between the Testing Laboratory and a developer or any other third party arising out of or in connection with the foregoing or the CLS(MD).

23.2.2 To the extend permissible by law, each manufacturer shall indemnify, defend and hold harmless and release CSA and its agent, directors, officers, employees, successors, assigns and representatives thereof (collectively the “Releasees”) from and against any and all claims, demands, suits, actions, judgements, damages, costs, losses, expenses (including all legal fees and expenses) and other liabilities arising from, in connection with or related in any way, directly or indirectly, to the breach of any warranties or obligations of the manufacturer under the CLS(MD) Terms, any act, neglect or omission by the developer or its agent, directors, officers, employees, successors, assigns and representatives and/or any disputes between the developer with a Testing Laboratory or any other third party arising out of or in connection with the foregoing or the CLS(MD).

## REFERENCES

[1] Cyber Security Agency of Singapore, “CCC SP-153-2 - CLS(MD) Publication #2 - Scheme Specifications,” Version 1.0, October 2024.

[2] Cyber Security Agency of Singapore, “CCC SP-153-3 - CLS(MD) Publication #3 - Requirements for Testing Laboratory,” Version 1.0, September 2024.

[3] Cyber Security Agency of Singapore, “CCC SP-153-1 - CLS(MD) Publication #1 - Overview of CLS(MD),” Version 1.0, October 2024.

## 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 |