Consultation Paper on the Licensing Framework for Cybersecurity Service Providers

Issued by the Cyber Security Agency of Singapore (CSA)

22 September 2025

Content

Part 1: INTRODUCTION

Background on the Licensing Framework

1. The establishment of the licensing framework for cybersecurity service providers in Singapore was first introduced in 2022 under Section 5 of the Cybersecurity Act 2018. It adopts a light-touch regulatory approach, targeting service providers that perform cybersecurity functions with significant access and potential impact on client systems.

2. The framework sought to achieve three key objectives:

   (a) Strengthening assurance on security and safety in the delivery of sensitive cybersecurity services

   (b) Raising the quality and professional standing of cybersecurity service providers in Singapore

   (c) Introducing licensing transparency to addressing information asymmetry between consumers and cybersecurity service providers

3. The framework covers two cybersecurity service categories:

   (a) Managed Security Operations Centre (SOC) Monitoring Service

   (b) Penetration Testing Service

   These services were prioritised because service providers providing such services have significant access into their clients' computer systems and sensitive information, which if abused, can lead to disruptions for their clients' operations. Such services are also widely available and used in the market, and thus have the potential to cause significant impact on the overall cybersecurity landscape.

Evolving Industry Context

4. Since the introduction of the framework, the cybersecurity landscape has evolved significantly. Cyber threats have become more frequent and sophisticated in nature with far-reaching consequences. Organisations in Singapore are now increasingly reliant on third-party cybersecurity service providers to effectively manage cybersecurity risks. The cybersecurity services industry is projected to grow substantially, alongside rapid digitalisation and growing threat exposure.

5. The role that cybersecurity service providers play in keeping organisations cybersafe will become more pronounced in contributing to Singapore's cyber resilience. As such, cybersecurity service providers must be held to appropriate standards of competence and trustworthiness.

Objective of Consultation

6. The Cyber Security Agency of Singapore ("CSA") seeks industry feedback on proposed changes to the existing licensing framework, with the intent to:
   - Raise baseline cybersecurity standards nationally; and
   - Enhance clarity on the licensing requirements

Part 2: PROPOSED CHANGES TO LICENSING FRAMEWORK

Introduction of Cyber and Data Hygiene Requirements

7. Ensuring cybersecurity service providers maintain strong internal cybersecurity and data protection standards is critical to national cyber resilience. To this end, CSA is proposing for cybersecurity service provider licensees to demonstrate their commitment to good cyber and data hygiene measures, by obtaining mandatory hygiene certifications. This aims to: (i) ensure licensed cybersecurity service providers are committed to protecting their own networks and client data, and (ii) establish a consistent and recognised standard of trustworthiness and professional conduct.

Mandatory Certification Requirements

8. Licensees will need to obtain and maintain the following certifications for the duration of their licence:

    i. *minimum* Cyber Trust Mark ("CTM") Promoter (Tier 3) or its equivalent; and

    ii. Data Protection Trust Mark ("DPTM") SS 714:2025 or its equivalent.

Cyber Trust Mark Promoter (Tier 3)

9. The CTM is published as Singapore Standards (SS) 712:2025, and it adopts a risk-based approach to cybersecurity certification, differentiating organisations by their risk profiles and cybersecurity maturity. CTM Promoter (Tier 3) strikes a balance by providing a robust and accountable cybersecurity framework that addresses critical risks without requiring the highest levels of strategic and threat intelligence capabilities that might be disproportionate to many licensees' current risk profiles or operational scale. Licensees have the flexibility to pursue higher tiers of CTM certification suited to their business needs.

10. For operational efficacy and efficiency, CSA will also recognise CTM-equivalent certifications including, but not limited to, ISO/IEC 27001.

11. Regardless of the standard, the scope of certification shall minimally include the environment (including people, process and technology) of the licensee supporting the delivery of the licensed service.

12. The certification body shall be accredited by Singapore Accreditation Council (SAC) or equivalent, the national accreditation body in Singapore. In the context of CTM, all certification bodies appointed by CSA are accredited.

13. While CTM certifications are typically issued to entities, CSA will work with the Certification Bodies so that individual licensees can also achieve the CTM Promoter (Tier 3) certification.

Data Protection Trust Mark SS 714:2025

14. The DPTM SS 714:2025 is an enterprise-wide certification for organisations to demonstrate accountable data protection practices, in compliance with the Personal Data Protection Act (PDPA) 2012. CSA has assessed that cybersecurity service provider licensees should achieve the DPTM SS 714:2025 to demonstrate their commitment to good data protection practices, given their access to privileged data in the course of their services.

15. CSA will also recognise other certification schemes including but not limited to, APEC Cross-Border Privacy Rules and Global Cross-Border Privacy Rules. While licensees pursue the relevant data protection certifications, licensees are encouraged to reference the self-assessment framework of Data Protection Essentials to implement basic data protection and security practices.

16. Individual licensees will be exempted from data protection certifications as these certifications only apply to organisations.

Changes to licence validity, renewal and notification timeframes

17. CSA is proposing to introduce other changes to the licensing conditions, which aim to reduce regulatory friction and improve operational clarity for licensees without compromising oversight.

    i. **Extension of Licence Validity**: Licence validity will be extended from 2 years to 5 years, with no change in annual fee quantum. Licences with a 5-year validity will cost $ 2,500 for businesses, and $ 1,250 for individuals to be paid upon the approval of licence application and/or renewal application, as the case may be.

    ii. **Extension of Licence Renewal Timeframes**: Currently, a licence renewal application must be made no later than 2 months before the licence expiry. For operational flexibility, CSA proposes to do away with the 2-month advance renewal period and allow for renewal applications to be made any time before the licence expiry. By doing so, licensees can submit renewal applications up to the last day of the licence (i.e. as long as the licence is active), reducing the possibility of missing the renewal period.

    iii. **Simplified Notification Obligations**: CSA will be extending the reporting window for key information changes to the licence from the current 14 calendar days to 30 calendar days. This will provide licensees more time to report changes and bring notification timelines in alignment with that for material changes in the Cybersecurity Act;

    Requirements to report non-material changes will be removed. These include the change in designations of the Licensee and/or its Officers, addresses and contact particulars, which licensees are required to report to CSA within 14 calendar days currently. Such information would be updated systematically upon renewal, given that the information does not have material impact on the delivery of the licensed service.

iv. **Revision to Information required in a Licence Application**: Information for licence application is presently listed in the Regulations. CSA proposes to remove the list from the Regulations and for the information required to be indicated in the electronic application service (i.e. currently, the GoBusiness Licensing portal) instead. This will allow for CSA to reduce the information as necessary to streamline the application process; and

v. **Other Operative Changes**: Powers that are currently duplicated across both the amended Cybersecurity Act and Conditions of Licence will be removed with no operational impact on licensees.

Please refer to the **Annex A and Annex B** for the details of the proposed changes to the Conditions of Licence and Cybersecurity (Cybersecurity Service Providers) Regulations 2022 respectively.

Implementation Timeline

18. CSA intends to implement the changes to the licensing framework progressively from January 2026.

19. The cyber and data hygiene requirements will be implemented in phases to space out the increased regulatory requirements. This is to allow a more gradual transition period for licensees and the wider ecosystem, including the certification bodies, to fulfil the requirements.

    i. A grace period until 31 December 2026 will be in effect for both new licensees and those who renewed their licences in 2026 to obtain the required CTM certification. This means that licensees can continue to provide their services until 31 December 2026 while pending CTM certification. In order to provide licensable services from 1 January 2027, all licensees would be required to have an active CTM certification during licence application and/or renewal.

    ii. A grace period until 31 December 2027 will be in effect for all licensees to obtain the required DPTM SS 714:2025 certification. This means that licensees can continue to provide until 31 December 2027 while pending DPTM SS 714:2025 certification. In order to provide licensable services from 1 January 2028, all licensees would be required to have an active DPTM SS 714:2025 certification during licence application and/or renewal.

Part 3: INVITATION TO COMMENT

20. CSA would like to seek views and comments from the industry on the proposed changes to the licencing framework, which are set out in greater details in Annex A and Annex B. The draft licence conditions and Regulations may be further refined, based on feedback received during this consultation.

21. All submissions should be clearly and concisely written and should provide a reasoned explanation for any proposed revisions. Submissions are to be submitted through the **Consultation on Licensing Framework for Cybersecurity Service Providers** online form.

22. All submission should reach CSA within 4 weeks, no later than **5pm on 21 October 2025**. We regret that late submissions will not be considered.

23. CSA reserves the right to make public all or parts of any submission and to disclose the identity of the source. Respondents may request confidential treatment for any part of the submission that the respondent believes to be proprietary, confidential or commercially sensitive. Any such information should be clearly marked and identified. Respondents are also required to substantiate with reasons any request for confidential treatment. If CSA grants confidential treatment, it will consider, but will not publicly disclose, the information. If CSA rejects the request for confidential treatment, it will return the information to the respondent that it submitted and will not consider this information as part of its review. As far as possible, respondents should limit any request for confidential treatment of information submitted. CSA will not accept any submission that requests confidential treatment for all, or a substantial part, of the submission.

24. For the avoidance of doubt, all the information provided and views expressed in this consultation paper are for purposes of discussion and consultation only. Nothing in this consultation paper represents or constitutes any decision made by CSA. The consultation contemplated by this consultation paper is without prejudice to the exercise of powers by CSA under the Cybersecurity Act or any subsidiary legislation thereunder.

Annex A – Proposed Changes to the Conditions of Licence

S/N	Current	Proposed (changes as highlighted)
1	**CONDITIONS OF LICENCE** The following conditions are imposed under Section 27 of the Cybersecurity Act 2018 (the "**Act**") as conditions for the grant of a licence to provide licensable cybersecurity services. The conditions apply in addition to any requirements under the Act and the Cybersecurity (Cybersecurity Service Providers) Regulations 2022. 1. **Definitions and interpretation** 1.1. In these conditions, unless the context otherwise requires: "Cybersecurity Services Regulation Office" (hereinafter referred to as "CSRO") means the office through which the Licensing Officer administers Part 5 of the Act; "Officer" refers to "officer of a business entity" as defined in Section 26(10) of the Act, namely, any director or partner of the business entity or other person who is responsible for the management of the business entity; "Licence" means the licence granted or renewed by the Licensing Officer to the Licensee to provide the relevant Service as stated therein; "Licensee" means the holder of a Licence;	**CONDITIONS OF LICENCE** The following conditions are imposed under Section 27 of the Cybersecurity Act 2018 (the "**Act**") as conditions for the grant of a licence to provide licensable cybersecurity services. The conditions apply in addition to any requirements under the Act and the Cybersecurity (Cybersecurity Service Providers) Regulations 2022. 1. **Definitions and interpretation** 1.1. In these conditions, unless the context otherwise requires: "Cybersecurity Services Regulation Office" (hereinafter referred to as "CSRO") means the office through which the Licensing Officer administers Part 5 of the Act; "Officer" refers to "officer of a business entity" as defined in Section 26(10) of the Act, namely, any director or partner of the business entity or other person who is responsible for the management of the business entity; "Licence" means the licence granted or renewed by the Licensing Officer to the Licensee to provide the relevant Service as stated therein; "Licensee" means the holder of a Licence;

	"Licensing Officer" means the Commissioner of Cybersecurity appointed under section 4(1)(a) of the Act; and "Service" means the licensable cybersecurity service that the Licensee is licensed to provide under the Licence, and refers EITHER to penetration testing service OR managed security operations centre (SOC) monitoring service, as respectively defined in paragraph 2 of the Second Schedule of the Act. 1.2. Apart from the definitions in paragraph 1.1 above, any other word or expression used in these conditions shall have the same meaning as in the Act unless the context otherwise requires. 1.3. This Licence is subject to the provisions of the Act and of any law amending, modifying or replacing the same. Any reference to the Act shall include any subsidiary legislation, rules, regulations and directions or orders made pursuant thereto. 1.4. For the avoidance of doubt, the Licensee shall comply with all obligations under the Act and this Licence at its own costs, unless otherwise specified in writing by the Licensing Officer.	"Licensing Officer" means the Commissioner of Cybersecurity appointed under section 4(1)(a) of the Act; and "Service" means the licensable cybersecurity service that the Licensee is licensed to provide under the Licence, and refers EITHER to penetration testing service OR managed security operations centre (SOC) monitoring service, as respectively defined in paragraph 2 of the Second Schedule of the Act. 1.2. Apart from the definitions in paragraph 1.1 above, any other word or expression used in these conditions shall have the same meaning as in the Act unless the context otherwise requires. 1.3. This Licence is subject to the provisions of the Act and of any law amending, modifying or replacing the same. Any reference to the Act shall include any subsidiary legislation, rules, regulations and directions or orders made pursuant thereto. 1.4. For the avoidance of doubt, the Licensee shall comply with all obligations under the Act and this Licence at its own costs, unless otherwise specified in writing by the Licensing Officer.
2	2. **Licence Period** 2.1. The Licence is valid for the period stated therein, unless revoked or suspended by the Licensing Officer in accordance with Section 30 of the Act.	2. **Licence Period** 2.1. The Licence is valid for the period stated therein, unless revoked or suspended by the Licensing Officer in accordance with Section 30 of the Act.

	2.2. Any application to renew the Licence shall be made in accordance with the requirements and timelines prescribed in the Act. 2.3. Where an application to renew the Licence is made after the time prescribed by the Act, the application will be treated as a fresh application for grant of a licence.	2.2. Any application to renew the Licence shall be made in accordance with the requirements and timelines prescribed in the Act. 2.3. Where an application to renew the Licence is made after the time prescribed by the Act, the application will be treated as a fresh application for grant of a licence.
3	3. **Professional Conduct of Licensee** 3.1. In relation to the Service it provides, the Licensee shall: a. Not make any false representation in the course of advertising or providing the Service; b. Comply with all applicable laws in the course of providing the Service, including, but not limited to, the Computer Misuse Act (Cap. 50A) and all obligations relating to confidentiality and data protection; c. Exercise due care and skill, and act with honesty and integrity in the course of providing the Service; d. Not act in a manner where there is a conflict between its interests and that of the person procuring or receiving the Service (the "Customer"); and e. Collect, use, or disclose any information about (i) a computer or computer system of any Customer, or (ii) the business, commercial or official affairs of any Customer,	3. **Professional Conduct of Licensee** 3.1. In relation to the Service it provides, the Licensee shall: a. Not make any false representation in the course of advertising or providing the Service; b. Comply with all applicable laws in the course of providing the Service, including, but not limited to, the Computer Misuse Act (Cap. 50A) and all obligations relating to confidentiality and data protection; c. Exercise due care and skill, and act with honesty and integrity in the course of providing the Service; d. Not act in a manner where there is a conflict between its interests and that of the person procuring or receiving the Service (the "Customer"); and e. Collect, use, or disclose any information about (i) a computer or computer system of any Customer, or (ii) the business, commercial or official affairs of any Customer,

	only for the purposes of providing the Service to the relevant Customer. The Licensee shall not collect, use or disclose any such information for other purposes, unless appropriate written consent has been obtained from the relevant customer, or such collection, use, or disclosure is lawfully required by any court, or lawfully required or allowed under law. 3.2. The Licensee shall also take all reasonable steps in the circumstances to ensure that its Officers, employees and/ or contractors also comply with the matters listed in paragraphs 3.1(a) to (e) above, with all references to the Licensee to be read as references to such persons.	only for the purposes of providing the Service to the relevant Customer. The Licensee shall not collect, use or disclose any such information for other purposes, unless appropriate written consent has been obtained from the relevant customer, or such collection, use, or disclosure is lawfully required by any court, or lawfully required or allowed under law. 3.2. The Licensee shall also take all reasonable steps in the circumstances to ensure that its Officers, employees and/ or contractors also comply with the matters listed in paragraphs 3.1(a) to (e) above, with all references to the Licensee to be read as references to such persons.
4	4. **Provision of Information** 4.1. The Licensee shall furnish, within a reasonable period specified by CSRO, information which CSRO considers to be relevant to – a. the Licensee's application for grant or renewal of the Licence; b. any breach (whether known or reasonably suspected by CSRO) by the Licensee of the Act or any licence conditions imposed on the Licensee; or c. the Licensee's continued eligibility to be the holder of the Licence.	~~4. **Provision of Information**~~ ~~4.1. The Licensee shall furnish, within a reasonable period specified by CSRO, information which CSRO considers to be relevant to –~~ ~~a. the Licensee's application for grant or renewal of the Licence;~~ ~~b. any breach (whether known or reasonably suspected by CSRO) by the Licensee of the Act or any licence conditions imposed on the Licensee; or~~ ~~c. the Licensee's continued eligibility to be the holder of the Licence.~~

	4.2. The Licensee shall produce at its own expense any such information, records, documents, data or other materials relevant to any investigation under this paragraph 4 (referred to collectively in this paragraph as the "Relevant Information"). 4.3. The Licensee shall keep confidential any information relating to such investigations, including but not limited to the fact that investigations are being conducted, or details regarding any Relevant Information provided by the Licensee to CSRO. All reasonable care must be taken to safeguard the confidentiality of the information, and Licensees shall not communicate the information to any person without prior written consent from CSRO. For the avoidance of doubt, CSRO can at any time determine that certain categories of information need no longer be treated as confidential.	~~4.2. The Licensee shall produce at its own expense any such information, records, documents, data or other materials relevant to any investigation under this paragraph 4 (referred to collectively in this paragraph as the "Relevant Information").~~ ~~4.3. The Licensee shall keep confidential any information relating to such investigations, including but not limited to the fact that investigations are being conducted, or details regarding any Relevant Information provided by the Licensee to CSRO. All reasonable care must be taken to safeguard the confidentiality of the information, and Licensees shall not communicate the information to any person without prior written consent from CSRO. For the avoidance of doubt, CSRO can at any time determine that certain categories of information need no longer be treated as confidential.~~
5	5. **Changes to Information** 5.1. The Licensee shall notify the Licensing Officer, in the manner described in CSRO's website at www.csro.gov.sg, of any change or inaccuracy in the information and particulars that the Licensee and/or its Officers submitted to the Licensing Officer in relation to this Licence, within fourteen (14) calendar days of such change or knowing of such inaccuracy (exclusive of the day such change or knowledge occurs). Such information and particulars include, but are not limited to: a. The appointment of any Officer; b. When an Officer ceases to hold such office;	5. **Changes to Information** 5.1. The Licensee shall notify the Licensing Officer, in the manner described in CSRO's website at www.csro.gov.sg, of any change or inaccuracy in the information and particulars that the Licensee and/or its Officers submitted to the Licensing Officer in relation to this Licence, within ~~fourteen (14) calendar days~~ ***thirty (30) calendar days*** of such change or knowing of such inaccuracy (exclusive of the day such change or knowledge occurs). Such information and particulars include, but are not limited to: a. The appointment of any Officer; b. When an Officer ceases to hold such office;

	c. Changes to or inaccuracies in the Licensee's and/or its Officers' names, designations, addresses and contact particulars; d. Criminal convictions or civil judgments entered against the Licensee and/or its Officers for offences or proceedings involving fraud, dishonesty, breach of fiduciary duty, or moral turpitude, or any offences under the Cybersecurity Act 2018; or e. Where the Licensee and/or its Officers have been declared bankrupt or have gone into compulsory or voluntary liquidation other than for the purpose of amalgamation or reconstruction.	c. Changes to or inaccuracies in the Licensee's and/or its Officers' names~~, designations, addresses and contact particulars;~~ d. Criminal convictions or civil judgments entered against the Licensee and/or its Officers for offences or proceedings involving fraud, dishonesty, breach of fiduciary duty, or moral turpitude, or any offences under the Cybersecurity Act 2018; or e. Where the Licensee and/or its Officers have been declared bankrupt or have gone into compulsory or voluntary liquidation other than for the purpose of amalgamation or reconstruction.
6	6. **Other Licences** 6.1. Nothing in this Licence affects the requirement to obtain any other licence that may be required under the Act or any other written law.	6. **Other Licences** 6.1. Nothing in this Licence affects the requirement to obtain any other licence that may be required under the Act or any other written law.
7	7. **Use of symbol or logo** 7.1. The Licensee shall not do any of the following in relation to any symbols or logos that CSA or CSRO uses in connection with its activities or affairs, except with prior written permission of the Licensing Officer: a. Use any symbol or logo that is identical with those used by CSA or CSRO; and b. Use any symbol or logo that is similar to those of CSA or CSRO in a manner that is likely to deceive or cause confusion.	~~7. **Use of symbol or logo**~~ ~~7.1. The Licensee shall not do any of the following in relation to any symbols or logos that CSA or CSRO uses in connection with its activities or affairs, except with prior written permission of the Licensing Officer:~~ ~~a. Use any symbol or logo that is identical with those used by CSA or CSRO; and~~ ~~b. Use any symbol or logo that is similar to those of CSA or CSRO in a manner that is likely to deceive or cause confusion.~~

8		***8. Duty to Maintain Active Certification*** ***8.1. The Licensees shall maintain an active or valid certificate for:*** ***a. Cyber Trust Mark (Level 3) or its equivalent, and*** ***b. Data Protection Trust mark or its equivalent*** ***for the duration of the Licence.***

Annex B – Proposed Changes to the Cybersecurity (Cybersecurity Service Providers) Regulations 2022

S/N	Current	Proposed (changes as highlighted)
1	**Applications for grant or renewal of licence** **2.**—(1) Subject to paragraph (4), every application for the grant or renewal of a cybersecurity service provider's licence under section 26 of the Act must be made electronically using the electronic application service provided by the licensing officer mentioned in section 25 of the Act at https://www.gobusiness.gov.sg/licences. (2) The application for the grant or renewal of a licence must include the following: (*a*) where the applicant is an individual — (i) the applicant's name; (ii) the applicant's identity card number, work pass number, passport number or foreign identification number; (iii) the applicant's nationality; (iv) the applicant's residential address and, if different, the applicant's correspondence address; (v) the applicant's contact telephone number and email address; (vi) information relating to —	**Applications for grant or renewal of licence** **2.**—(1) Subject to paragraph (4), every application for the grant or renewal of a cybersecurity service provider's licence under section 26 of the Act must be made electronically using the electronic application service provided by the licensing officer mentioned in section 25 of the Act at https://www.gobusiness.gov.sg/licences. ***(2) Every such application for the grant and renewal of a licence must include any information and declaration specified by the licensing officer in the electronic application service mentioned in paragraph (1).*** ~~(2) The application for the grant or renewal of a licence must include the following:~~ ~~(*a*) where the applicant is an individual —~~ ~~(i) the applicant's name;~~ ~~(ii) the applicant's identity card number, work pass number, passport number or foreign identification number;~~ ~~(iii) the applicant's nationality;~~

	(A) the applicant's qualification or experience (if any) relating to the licensable cybersecurity service for which a licence is sought; (B) where the applicant does not have any qualification or experience relating to the licensable cybersecurity service for which a licence is sought — the qualification or experience of the applicant's employees or proposed employees having supervisory responsibility relating to the licensable cybersecurity service; or (C) where sub-paragraphs (A) and (B) are not applicable — the business partnership, consortium or other legal arrangement (if any) through which the applicant proposes to provide the licensable cybersecurity service;	~~(iv) the applicant's residential address and, if different, the applicant's correspondence address;~~ ~~(v) the applicant's contact telephone number and email address;~~ ~~(vi) information relating to —~~ ~~(A) the applicant's qualification or experience (if any) relating to the licensable cybersecurity service for which a licence is sought;~~ ~~(B) where the applicant does not have any qualification or experience relating to the licensable cybersecurity service for which a licence is sought — the qualification or experience of the applicant's employees or proposed employees having supervisory responsibility relating to the licensable cybersecurity service; or~~ ~~(C) where sub-paragraphs (A) and (B) are not applicable — the business partnership, consortium or other legal arrangement (if any) through~~

	(vii) information as to whether the applicant has been convicted in Singapore or elsewhere of — (A) an offence involving fraud, dishonesty or moral turpitude; or (B) an offence the conviction for which involves a finding that the applicant had acted fraudulently or dishonestly; (viii) information as to whether the applicant has had a judgment entered against the applicant in civil proceedings that involves a finding of fraud, dishonesty or breach of fiduciary duty on the part of the applicant; (ix) information as to whether the applicant is or was suffering from a mental disorder; (x) information as to whether the applicant is an undischarged bankrupt or has entered into a composition with any creditor of the applicant; (xi) information as to whether the applicant has had a licence revoked by the licensing officer previously; and	~~which the applicant proposes to provide the licensable cybersecurity service;~~ ~~(vii) information as to whether the applicant has been convicted in Singapore or elsewhere of —~~ ~~(A) an offence involving fraud, dishonesty or moral turpitude; or~~ ~~(B) an offence the conviction for which involves a finding that the applicant had acted fraudulently or dishonestly;~~ ~~(viii) information as to whether the applicant has had a judgment entered against the applicant in civil proceedings that involves a finding of fraud, dishonesty or breach of fiduciary duty on the part of the applicant;~~ ~~(ix) information as to whether the applicant is or was suffering from a mental disorder;~~ ~~(x) information as to whether the applicant is an undischarged bankrupt or has entered into a composition with any creditor of the applicant;~~

	(xii) any other information that may be specified by the licensing officer in the electronic application service mentioned in paragraph (1); (*b*) where the applicant is a business entity — (i) the applicant's name; (ii) the applicant's — (A) Singapore unique entity number; or (B) business entity registration number in the foreign country or territory that the applicant is incorporated or registered in; (iii) the address of the applicant's registered office or principal place of business; (iv) if the address in sub-paragraph (iii) is outside Singapore, the address of the applicant's principal place of business or address for service in Singapore; (v) the applicant's contact telephone number and email address;	~~(xi) information as to whether the applicant has had a licence revoked by the licensing officer previously; and~~ ~~(xii) any other information that may be specified by the licensing officer in the electronic application service mentioned in paragraph (1);~~ ~~(*b*) where the applicant is a business entity —~~ ~~(i) the applicant's name;~~ ~~(ii) the applicant's —~~ ~~(A) Singapore unique entity number; or~~ ~~(B) business entity registration number in the foreign country or territory that the applicant is incorporated or registered in;~~ ~~(iii) the address of the applicant's registered office or principal place of business;~~ ~~(iv) if the address in sub-paragraph (iii) is outside Singapore, the address of the applicant's principal place of business or address for service in Singapore;~~

	(vi) the particulars mentioned in sub-paragraph (*a*) (except sub-paragraph (*a*)(vi)(B) and (C)) in respect of every director or partner of the applicant or other person who is responsible for the management of the applicant, with each reference in sub-paragraph (*a*) to the applicant substituted with a reference to the director, partner or other person, as the case may be; (vii) where no director or partner of the applicant or other person who is responsible for the management of the applicant has any qualification or experience relating to the licensable cybersecurity service for which a licence is sought — information relating to the qualification or experience of the applicant's employees or proposed employees having supervisory responsibility relating to the licensable cybersecurity service for which a licence is sought; (viii) information as to whether the applicant has been convicted in Singapore or elsewhere of —	~~(v) the applicant's contact telephone number and email address;~~ ~~(vi) the particulars mentioned in sub-paragraph (*a*) (except sub-paragraph (*a*)(vi)(B) and (C)) in respect of every director or partner of the applicant or other person who is responsible for the management of the applicant, with each reference in sub-paragraph (*a*) to the applicant substituted with a reference to the director, partner or other person, as the case may be;~~ ~~(vii) where no director or partner of the applicant or other person who is responsible for the management of the applicant has any qualification or experience relating to the licensable cybersecurity service for which a licence is sought — information relating to the qualification or experience of the applicant's employees or proposed employees having supervisory responsibility relating to the licensable cybersecurity service for which a licence is sought;~~

	(A) an offence involving fraud, dishonesty or moral turpitude; or (B) an offence the conviction for which involves a finding that the applicant had acted fraudulently or dishonestly; (ix) information as to whether the applicant has had a judgment entered against the applicant in civil proceedings that involves a finding of fraud, dishonesty or breach of fiduciary duty on the part of the applicant; (x) information as to whether the applicant is in liquidation or is the subject of a winding up order, or there is a receiver appointed in relation to the applicant, or the applicant has entered into a composition or scheme of arrangement with any creditor of the applicant; (xi) information as to whether the applicant has had a licence revoked by the licensing officer previously; and (xii) any other information that may be specified by the licensing officer in the	~~(viii) information as to whether the applicant has been convicted in Singapore or elsewhere of —~~ ~~(A) an offence involving fraud, dishonesty or moral turpitude; or~~ ~~(B) an offence the conviction for which involves a finding that the applicant had acted fraudulently or dishonestly;~~ ~~(ix) information as to whether the applicant has had a judgment entered against the applicant in civil proceedings that involves a finding of fraud, dishonesty or breach of fiduciary duty on the part of the applicant;~~ ~~(x) information as to whether the applicant is in liquidation or is the subject of a winding up order, or there is a receiver appointed in relation to the applicant, or the applicant has entered into a composition or scheme of arrangement with any creditor of the applicant;~~ ~~(xi) information as to whether the applicant has had a licence revoked by the licensing officer previously; and~~

	electronic application service mentioned in paragraph (1). (3) An application for the renewal of a licence must be made no later than 2 months before the date of expiry of the licence. (4) If the electronic application service is not operating or available, an application for the grant or renewal of a licence must be made in such written form as the licensing officer may require. (5) If an application for the renewal of a licence cannot be submitted in accordance with paragraph (1) within the time specified in paragraph (3) due to the unavailability of the electronic application service, an application in such written form mentioned in paragraph (4) must be submitted on the next working day to the licensing officer. (6) In this regulation, "employee having supervisory responsibility relating to the licensable cybersecurity service", in relation to an applicant, means an employee of the applicant who is responsible for supervising or managing the provision of a licensable cybersecurity service or any part of a licensable cybersecurity service by any other employee of the applicant.	~~(xii) any other information that may be specified by the licensing officer in the electronic application service mentioned in paragraph (1).~~ (3) An application for the renewal of a licence must be made ~~no later than 2 months~~ before the date of expiry of the licence. (4) If the electronic application service is not operating or available, an application for the grant or renewal of a licence must be made in such written form as the licensing officer may require. ~~(5) If an application for the renewal of a licence cannot be submitted in accordance with paragraph (1) within the time specified in paragraph (3) due to the unavailability of the electronic application service, an application in such written form mentioned in paragraph (4) must be submitted on the next working day to the licensing officer.~~ (6) In this regulation, "employee having supervisory responsibility relating to the licensable cybersecurity service", in relation to an applicant, means an employee of the applicant who is responsible for supervising or managing the provision of a licensable cybersecurity service or any part of a licensable cybersecurity service by any other employee of the applicant.
2	**Licence fee**	**Licence fee**

	3.—(1) The fee payable for the grant or renewal of a licence is the following: (*a*) where the applicant is an individual — (i) $125 per year or part of a year, where the application is made to the licensing officer during the initial period; or (ii) $250 per year or part of a year, where the application is made to the licensing officer after the expiry of the initial period; (*b*) where the applicant is a business entity — (i) $250 per year or part of a year, where the application is made to the licensing officer during the initial period; or (ii) $500 per year or part of a year, where the application is made to the licensing officer after the expiry of the initial period. (2) The licensing officer may, where the licensing officer considers appropriate, refund or remit the whole or part of any fee paid or payable under paragraph (1). (3) In this regulation, "initial period" means the period from 11 April 2022 to 10 April 2023 (both dates inclusive).	**3.**—(1) The fee payable for the grant or renewal of a licence is the following: (*a*) where the applicant is an individual — (i) $125 per year or part of a year, where the application is made to the licensing officer during the initial period; or (ii) $250 per year or part of a year, where the application is made to the licensing officer after the expiry of the initial period; (*b*) where the applicant is a business entity — (i) $250 per year or part of a year, where the application is made to the licensing officer during the initial period; or (ii) $500 per year or part of a year, where the application is made to the licensing officer after the expiry of the initial period. (2) The licensing officer may, where the licensing officer considers appropriate, refund or remit the whole or part of any fee paid or payable under paragraph (1). (3) In this regulation, "initial period" means the period from 11 April 2022 to 10 April 2023 (both dates inclusive).
3	**Keeping of records**	**Keeping of records**

	4.—(1) For the purposes of section 29(1)(*a*)(v) of the Act, a licensee must, in relation to each occasion on which the licensee is engaged to provide its cybersecurity service, keep records of the information specified in paragraph (2) in respect of every person who delivers the cybersecurity service on behalf of the licensee. (2) For the purposes of paragraph (1) — (*a*) the information for which records must be kept in respect of every individual who delivers any part of the cybersecurity service on behalf of the licensee, whether or not the individual is an employee of the licensee, is the following: (i) the individual's name; (ii) the individual's identity card number, work pass number, passport number or foreign identification number; and (*b*) the information for which records must be kept in respect of every business entity which delivers any part of the cybersecurity service on behalf of the licensee is the following: (i) the business entity's name; (ii) the business entity's — (A) Singapore unique entity number; or	**4.**—(1) For the purposes of section 29(1)(*a*)(v) of the Act, a licensee must, in relation to each occasion on which the licensee is engaged to provide its cybersecurity service, keep records of the information specified in paragraph (2) in respect of every person who delivers the cybersecurity service on behalf of the licensee. (2) For the purposes of paragraph (1) — (*a*) the information for which records must be kept in respect of every individual who delivers any part of the cybersecurity service on behalf of the licensee, whether or not the individual is an employee of the licensee, is the following: (i) the individual's name; (ii) the individual's identity card number, work pass number, passport number or foreign identification number; and (*b*) the information for which records must be kept in respect of every business entity which delivers any part of the cybersecurity service on behalf of the licensee is the following: (i) the business entity's name; (ii) the business entity's — (A) Singapore unique entity number; or

	(B) business entity registration number in the foreign country or territory that the business entity is incorporated or registered in.	(B) business entity registration number in the foreign country or territory that the business entity is incorporated or registered in.
4	**Appeals** **5.** An appeal made under section 35(1), (2), (3) or (4) of the Act must — (*a*) be made in the form set out at https://www.mci.gov.sg; (*b*) specify the name and particulars of the person bringing the appeal (called in this regulation the appellant); (*c*) identify the decision or order appealed against; (*d*) state the reasons for the appeal and the issues arising from the appeal; (*e*) be accompanied by any document mentioned in, or relied on in support of, the appeal; and (*f*) be signed and dated — (i) where the appellant is an individual — by that individual or a duly authorised representative of the individual; or	**Appeals** **5.** An appeal made under section 35(1), (2), (3) or (4) of the Act must — (*a*) be made in the form set out at ~~https://www.mci.gov.sg;~~ ***https://www.mddi.gov.sg;*** (*b*) specify the name and particulars of the person bringing the appeal (called in this regulation the appellant); (*c*) identify the decision or order appealed against; (*d*) state the reasons for the appeal and the issues arising from the appeal; (*e*) be accompanied by any document mentioned in, or relied on in support of, the appeal; and (*f*) be signed and dated — (i) where the appellant is an individual — by that individual or a duly authorised representative of the individual; or

	(ii) where the appellant is a business entity — by a duly authorised representative of the business entity.	(ii) where the appellant is a business entity — by a duly authorised representative of the business entity.