Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024

I, Julie Inman Grant, eSafety Commissioner, determine the following industry standard.

Dated 19 June 2024

Julie Inman Grant
eSafety Commissioner

Contents

Part 1—Preliminary

1 Name

This is the *Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024*.

2 Commencement

This industry standard commences on the day that is 6 months after the later of:

(a) the day after the day on which it is registered under the Act; and

(b) the day after the day on which it is registered under the *Legislation Act 2003*.

3 Authority

This industry standard is determined under section 145 of the *Online Safety Act 2021*.

4 Object of this industry standard

The object of this industry standard is to improve online safety for Australians in respect of class 1A material and class 1B material, including by ensuring that providers of designated internet services establish and implement systems, processes and technologies to manage effectively risks that Australians will solicit, generate, distribute, get access to or be exposed to class 1A material or class 1B material through the services.

5 Application of this industry standard

(1) This industry standard applies to a designated internet service, wherever it is provided from, but only so far as it is provided to end-users in Australia.

(2) If:

(a) this industry standard applies to a designated internet service; and

(b) another industry standard, or an industry code, applies to the service; and

(c) the service's predominant purpose is more closely aligned with the other industry standard or the industry code;

this industry standard does not apply to the service.

Part 2—Interpretation

Note: A number of expressions used in this industry standard are defined in the Act, including the following:

(a) child;
(b) class 1 material;
(c) class 2 material;
(d) Classification Board;
(e) Commissioner;
(f) computer game;
(g) consent;
(h) designated internet service;
(i) material;
(j) parent:
(k) posted;
(l) publication;
(m) removed;
(n) service.

6 General definitions

Definitions

(1) In this industry standard:

account holder, for a designated internet service, means the person who is the counterparty to the agreement with the provider of the service for the provision of the service.

Example: A designated internet service may be provided to a family, where a parent or carer has the agreement with the provider of the service. The parent or carer is the account holder. Family members (including the parent or carer who is the account holder) who use the service are end-users.

Act means the *Online Safety Act 2021*.

appropriate: see section 11.

Australian child means a child who is in Australia.

child sexual abuse material means class 1 material that:

(a) describes, depicts, promotes or provides instruction in child sexual abuse; or
(b) is known child sexual abuse material.

child sexual exploitation material means class 1 material that:

(a) is or includes material that promotes, or provides instruction in, paedophile activity; or
(b) is or includes:
    (i) child sexual abuse material; or
    (ii) exploitative or offensive descriptions or depictions involving a person who is, appears to be or is described as a child; or

(c) describes or depicts, in a way that is likely to cause offence to a reasonable adult, a person who is, appears to be or is described as a child (whether or not the person is engaged in sexual activity);

and, in the case of a publication, also includes class 1 material that is or includes gratuitous, exploitative or offensive descriptions or depictions of:

(d) sexualised nudity; or

(e) sexual activity;

involving a person who is, appears to be or is described as a child.

class 1A material means:

(a) child sexual exploitation material; or

(b) pro-terror material; or

(c) extreme crime and violence material.

class 1B material means:

(a) crime and violence material (but not extreme crime and violence material); or

(b) drug-related material.

classified means classified under the *Classification (Publications, Films and Computer Games) Act 1995*.

Note: RC is a classification.

classified DIS means a designated internet service that has the sole or predominant purpose of providing general entertainment, news or educational content, being:

(a) films or computer games that:

(i) have been classified R18+ Restricted or lower; or

(ii) are exempt from classification under the *Classification (Publications, Films and Computer Games) Act 1995*; or

(b) films or computer games that have not been classified but, if classified, would likely be classified R18+ Restricted or lower; or

(c) books, newspapers and magazines, whether in digital or audio form, podcasts or digital music that, if required to be classified, would likely be classified Unrestricted or Category 1 restricted;

and includes a service that is taken to be a classified DIS under subsection 12(2).

complainant: see subsection 27(2).

complaint means a complaint referred to in paragraph 27(2)(b).

compliance report means a report required by section 36.

crime and violence material, in relation to a computer game, means class 1 material that is a computer game and that, without justification:

(a) promotes, incites or instructs in matters of crime or violence, or is or includes detailed instruction in, or promotion of, matters of crime or violence; or

(b) is or includes depictions of bestiality or similar practices; or

(c) depicts, expresses or otherwise deals with matters of crime, cruelty or violence in such a way that it offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that it should be classified RC; or

(d) is or includes depictions of violence that:

(i) have a very high degree of impact; and

(ii) are excessively frequent, prolonged, detailed or repetitive; or

(e) is or includes depictions of cruelty or realistic violence that:

(i) have a very high degree of impact; and

(ii) are very detailed; or

(f) is or includes depictions of actual sexual violence; or

(g) is or includes depictions of implied sexual violence related to incentives or rewards.

crime and violence material, in relation to a publication, means class 1 material that is, or is included in, the publication and that, without justification:

(a) promotes, incites or instructs in matters of crime or violence, or is or includes detailed instruction in matters of crime or violence; or

(b) is or includes realistic depictions of bestiality; or

(c) depicts, expresses or otherwise deals with matters of crime, cruelty or violence in such a way that it offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that it should be classified RC; or

(d) is or includes gratuitous, exploitative or offensive descriptions or depictions of violence that:

(i) have a very high degree of impact; and

(ii) are excessively frequent, emphasised or detailed; or

(e) is or includes gratuitous, exploitative or offensive descriptions or depictions of cruelty or real violence that:

(i) have a very high degree of impact; and

(ii) are very detailed; or

(f) is or includes gratuitous, exploitative or offensive descriptions or depictions of sexual violence.

crime and violence material, in relation to material that is not a computer game or a publication, means class 1 material that, without justification:

(a) promotes, incites or instructs in matters of crime or violence, or is or includes detailed instruction in matters of crime or violence; or

(b) is or includes depictions of bestiality or similar practices; or

(c) depicts, expresses or otherwise deals with matters of crime, cruelty or violence in such a way that it offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that it should be classified RC; or

(d) is or includes gratuitous, exploitative or offensive depictions of violence that:
  (i) have a very high degree of impact; or
  (ii) are excessively frequent, prolonged or detailed; or
(e) is or includes gratuitous, exploitative or offensive depictions of cruelty or real violence that:
  (i) have a very high degree of impact; and
  (ii) are very detailed; or
(f) is or includes gratuitous, exploitative or offensive depictions of sexual violence.

designated internet service has the meaning given by section 14(1) of the Act.

development program means a program required by section 23.

DIS means a designated internet service.

drug means a chemical, compound or other substance or thing, that is included in Schedule 4 of the *Customs (Prohibited Imports) Regulations 1956*.

drug-related material, in relation to a computer game, means class 1 material that, without justification:
(a) depicts the unlawful use of drugs in connection with incentives or rewards; or
(b) depicts interactive, detailed and realistic use of drugs, being unlawful use; or
(c) depicts, expresses or otherwise deals with matters of drug misuse or addiction in such a way that the material offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that the material should be classified RC; or
(d) is or includes detailed instruction in the unlawful use of drugs.

drug-related material, in relation to a publication, means class 1 material that, without justification:
(a) depicts, expresses or otherwise deals with matters of drug misuse or addiction in such a way that the material offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that the material should be classified RC; or
(b) is or includes detailed instruction in the unlawful use of drugs.

drug-related material, in relation to material that is not a computer game or a publication, means class 1 material that, without justification:
(a) depicts, expresses or otherwise deals with matters of drug misuse or addiction in such a way that the material offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that the material should be classified RC; or
(b) is or includes detailed instruction in the unlawful use of drugs; or
(c) is or includes material promoting the unlawful use of drugs.

end-user, of a designated internet service, means a natural person who uses the service.

Example: A designated internet service may be provided to a family, where a parent or carer has the agreement with the provider of the service. The parent or carer is the account holder. Family members (including the parent or carer who is the account holder) who use the service are end-users.

end-user managed hosting service means:

(a) a designated internet service that is primarily designed or adapted to enable end-users to store or manage material; and

(b) includes a service that is taken to be an end-user managed hosting service under subsection 12(2).

Note 1: Examples of end-user managed hosting services include online file storage services, photo storage services, and other online media hosting services, including such services that include functionality to allow end-users to post or share content.

Note 2: For purposes of this industry standard, an enterprise DIS that meets this definition will be taken to be both an enterprise DIS and an end-user managed hosting service – see subsection 12(2)(c).

Note 3: An end-user managed hosting service differs from Third-Party Hosting Services (as defined in the Hosting Services Online Safety Code (Class 1A and Class 1B Material)) which have the sole or predominant purpose of supporting the delivery of another service online and which do not directly interact with end-users.

enforcement authority means a police force or other law enforcement authority.

enterprise customer means the account holder under the agreement for the provision of an enterprise DIS.

Note: The enterprise customer will often make the service available to a class of end-users, such as its staff.

enterprise DIS means a designated internet service:

(a) the account holder for which is an organisation (and not an individual); and

(b) the predominant purpose of which is to enable the account holder, in accordance with the terms of use for the service, to use the service for the organisation's activities, including integrating the service into the organisation's own services that are or may be made available by the organisation to the organisation's end-users; and

(c) that is of a kind that is usually acquired by account holders for the purpose mentioned in paragraph (b);

and includes a service that is taken to be an enterprise DIS under subsection 12(2).

Note 1: An enterprise DIS excludes Third-Party Hosting Services (as defined in the Hosting Services Online Safety Code (Class 1A and Class 1B Material) and which are dealt with by that Code).

Note 2: An enterprise DIS would, for example, include:

(a) websites designed for the ordering of commercial supplies by enterprise customers; and

(b) services which provide pre-trained artificial intelligence or machine learning models for integration into a service deployed or to be deployed by an enterprise customer.

exploitative, in relation to a description or depiction of an event, means that the description or depiction:

(a) appears intended to debase or abuse, for the enjoyment of readers or viewers, the person or entity described or depicted; and

(b) has no moral, artistic or other value.

extreme crime and violence material, in relation to a computer game, means material that is crime and violence material in relation to a computer game where, without justification, the impact of the material is extreme because:

(a) the material is more detailed; or

(b) the material is realistic rather than stylised; or

(c) the game is highly interactive; or

(d) the gameplay links incentives or rewards to high impact elements of the game; or

(e) for any other reason.

extreme crime and violence material, in relation to a publication, means material that is crime and violence material in relation to a publication where, without justification, the impact of the material is extreme because of the emphasis, tone, frequency, context and detail of the relevant elements of the publication and other factors that heighten impact.

extreme crime and violence material, in relation to material that is not a computer game or a publication, means crime and violence material where, without justification, the impact of the material is extreme because:

(a) the material is more detailed; or

(b) the material is highly interactive; or

(c) the relevant depictions in the material are realistic, prolonged or repeated; or

(d) for any other reason.

general purpose DIS means a designated internet service that:

(a) is a website or application that:

(i) primarily provides information for business, commerce, charitable, professional, health, reporting news, scientific, educational, academic research, government, public service, emergency, or counselling and support service purposes; or

(ii) enables transactions related to the matters in subparagraph (i); or

(b) is a web browser; and

(c) cannot be characterised as a different category of designated internet service under this industry standard.

high impact DIS means a designated internet service that:

(a) has the sole or predominant purpose of enabling end-users to access high impact materials; and

(b) makes available high impact material that has been posted by end-users;

and includes a service that is taken to be a high impact DIS because of subsection 12(2).

Note 1: This category would, for example, include websites or applications such as pornography websites and 'gore' or 'shock sites' that contain sexually explicit and/or graphically violent end-user generated content that qualifies as high impact material.

Note 2: Under paragraph 12(2)(a), a high impact DIS may also be taken to be a high impact generative AI DIS.

high impact generative AI DIS means a designated internet service that:

(a) uses machine learning models to enable an end-user to produce material; and

(b) is capable of being used to generate synthetic high impact material;

and includes a service that is taken to be a high impact generative AI DIS because of subsection 12(2), but a DIS is not a high impact generative AI DIS if it incorporates controls such that the risk of the service being used to generate synthetic high impact material is immaterial.

Note 1: This category would, for example, include services with generative artificial intelligence functionality to produce high impact material including completely new material and new material that has been created from editing existing material (for example – deepfake child sexual exploitation material).

Note 2: See note 3 to definition of ***model distribution platform*** for example of an exclusion from this category.

Note 3: A high impact generative AI DIS may also be taken to be:

(a) a high impact DIS—see paragraph 12(2)(a); or

(b) a classified DIS—see paragraph 12(2)(b).

high impact material, in relation to a DIS other than a high impact generative AI DIS, means material which is:

(a) a film or a computer game that has been, or would likely be, classified R18+ Restricted, X18+ Restricted or RC; or

(b) a publication that has been, or would likely be, classified Category 1 Restricted, Category 2 Restricted or RC.

high impact material, in relation to a high impact generative AI DIS is material which is:

(a) a film or computer game that has been or would likely be classified X18+ Restricted or RC; or

(b) a publication which has been or would likely be classified Category 2 Restricted or RC.

industry code has the meaning given in section 132 of the Act.

justification: see subsection (3).

known child sexual abuse material means material that:

(a) is or includes images (either still images or video images); and

(b) has been verified as child sexual abuse material by a governmental (including multi-lateral) or non-governmental organisation:

(i) the functions of which are or include combating child sexual abuse or child sexual exploitation; and

(ii) in the case of a non-governmental organisation—that is generally recognised as expert or authoritative in that context; and

(c) is recorded on a database that:

(i) is managed by an organisation of a kind described in paragraph (b); and

(ii) is made available to government agencies, enforcement authorities and providers of designated internet services for the purpose of their using technological means to detect or manage child sexual abuse material on designated internet services.

Example: An example of a database referred to in paragraph (c) is the database managed by the National Center for Missing & Exploited Children.

known pro-terror material means material that has been verified as pro-terror material.

Note 1: ***Known pro-terror material*** may include material that can be detected via hashes, text signals, searches of key words terms, URLs or behavioural signals or patterns that signal or are associated with online materials produced by terrorist entities that are on the United Nations Security Council Consolidated List.

That List was accessible, on the registration of this industry standard, at https://www.un.org/securitycouncil/content/un-sc-consolidated-list.

Note 2: Material may, for example, be verified as a result of a decision of the Classification Board. Material may also be verified by using tools provided by independent organisations that are recognised as having expertise in counter-terrorism. Examples of these organisations include Tech Against Terrorism and the Global Internet Forum to Counter Terrorism.

model distribution platform means a designated internet service which:

(a) has a purpose which includes making available machine learning models; and

(b) allows end-users to upload machine learning models to the service.

Note 1: Models made available on the service (including models uploaded to the service) and their associated content and materials hosted on the service, are components of the service.

Note 2: Except to the extent specified in section 27(2), material that is generated by or using models made available on the service, but that is not stored on or accessible using the service, is not a component of the service.

Note 3: A model distribution platform which includes functionality to enable end-users to use a hosted model to generate synthetic high impact material is not considered a high impact generative AI DIS.

offensive: see subsection (4).

pre-assessed classified DIS means a classified DIS that meets the requirements of subsection (2).

pre-assessed tier 3 designated internet service means each of the following:

(a) a pre-assessed classified DIS; and

(b) a pre-assessed general purpose DIS.

pre-assessed general purpose DIS means a general purpose DIS that meets the requirements of subsection (2).

pro-terror material means:

(a) class 1 material that:

(i) directly or indirectly counsels, promotes, encourages or urges the doing of a terrorist act; or

(ii) directly or indirectly provides instruction on the doing of a terrorist act; or

(iii) directly praises the doing of a terrorist act in circumstances where there is a substantial risk that the praise might have the effect of leading a person (regardless of the person's age or any mental impairment that the person might suffer) to engage in a terrorist act; or

(b) material that is known pro-terror material.

However, material accessible using a designated internet service is not pro-terror material if its availability on the service can reasonably be taken to be part of public discussion, public debate, entertainment or satire.

provide a designated internet service includes make the service available.

RC or ***RC Refused Classification*** means the "Refused Classification" classification under the *Classification (Publications, Films and Computer Games) Act 1995*.

risk assessment means an assessment of a kind required by subsection 7(1).

risk profile, for a designated internet service, means the risk profile of the service worked out under subsection 7(8).

sexual activity is not limited to sexual intercourse.

store: material is ***stored on a designated internet service*** if it is:

(a) in storage used for the service; or

(b) accessible through or using the service.

terms of use, for a designated internet service, means the provisions of the agreement under which the service is provided and includes anything that may reasonably be regarded as the equivalent of terms of use.

Note: For what must be included in terms of use for a designated internet service see section 13.

terrorist act has the meaning given by section 100.1(1) of the *Criminal Code* (no matter where the action occurs, the threat of action is made or the action, if carried out, would occur).

Tier 1 designated internet service means:

(a) a designated internet service that is determined in accordance with section 7(8) to have a Tier 1 risk profile;

(b) a high impact DIS; and

(c) a designated internet service that is determined in accordance with section 7(9) to have a Tier 1 risk profile.

Tier 2 designated internet service means a designated internet service that is determined in accordance with section 7 to have a Tier 2 risk profile.

Tier 3 designated internet service means:

(a) a designated internet service that is determined in accordance with section 7 to have a Tier 3 risk profile;

(b) a pre-assessed Tier 3 designated internet service; and

(c) an enterprise DIS.

violence means an act of violence or an obvious threat of an act of violence.

Requirements for pre-assessment

(2) The requirements for a classified DIS or a general purpose DIS to be pre-assessed are that:

(a) in respect of posting or sharing of material—the relevant service:

(i) does not enable end-users in Australia to post material to the service; or

(ii) enables end-users in Australia to post material only for the purposes of enabling such end-users to review or provide information on products, services, or physical points of interest or locations made available on the service; or

(iii) enables end-users in Australia to post or share material only for the purpose of sharing that material with other end-users for a business, informational or government service or support purpose; and

(b) in respect of chat or messaging functionality—the relevant service:

(i) does not offer a chat or messaging function; or

(ii) offers a chat or messaging function but the chat or messaging function is limited to private messages or chats between the service and end-users in Australia for a business, informational or government service or support purpose.

Justification

(3) For this industry standard, in determining whether material is without justification, the matters to be taken into account include:

(a) the standards of morality, decency and propriety generally accepted by reasonable adults; and

(b) the literary, artistic or educational merit (if any) of the material; and

(c) the general character of the material, including whether it is of a medical, legal or scientific character; and

(d) the persons or class of persons to or amongst whom it is published or is intended or likely to be published.

Offensive material

(4) The question whether material is offensive for the purposes of this industry standard is to be determined in accordance with the Act, including section 8 of the Act.

Part 3—Risk assessments and risk profiles

7 Requirement to carry out risk assessments and determine risk profiles of designated internet services

Risk assessments to be carried out

(1) The provider of a designated internet service must, at the times required by and in accordance with this Part, carry out an assessment of the risk that class 1A material or class 1B material:
  (a) will be generated or accessed by, or distributed by or to, end-users in Australia using the service; and
  (b) will be stored on the service.

Timing of risk assessments

(2) If the provider of the service was providing the service before the commencement of this industry standard, the risk assessment must be carried out as soon as practicable after, but no later than 6 months after, the commencement of this industry standard.

(3) Subsection (2) does not apply if a risk assessment that met the requirements of this Part had been carried out in respect of the service within 6 months before the commencement of this industry standard.

(4) A person must not start to provide a designated internet service to an end-user in Australia unless a risk assessment of the service has been carried out in accordance with this Part within 6 months before the person started to provide the service.

(5) The provider of a designated internet service must not make a material change to the service unless:
  (a) a risk assessment of the service, as proposed to be changed, has been carried out in accordance with this Part; or
  (b) the change will not increase the risk of class 1A material or class 1B material being accessed or generated by, or distributed to, end-users in Australia using the service, or being stored on the service.

Note: See also sections 33 and 34.

Certain services exempt from risk assessment requirements

(6) Subsections (1) and (4) do not apply to any of the following:
  (a) a pre-assessed general purpose DIS;
  (b) a pre-assessed classified DIS;
  (c) an end-user managed hosting service;
  (d) an enterprise DIS;
  (e) a high impact DIS;
  (f) a high impact generative AI DIS;

(g) a model distribution platform;

(h) a designated internet service that is determined under subsection (9) to be a Tier 1 designated internet service.

Note: However, subsection (1) applies to a designated internet service mentioned in this subsection (6) if the service is materially changed.

Risk profiles of designated internet services

(7) The provider of a designated internet service that conducts a risk assessment of the service must, on completion of the assessment, determine, in accordance with subsection (8), what the risk profile of the service is.

(8) The risk profile of a designated internet service is worked out as follows:

Item	If the risk that class 1A material or class 1B material will be accessed or generated by, or distributed to, end-users in Australia using the service, or will be stored on the service, is…	the risk profile of the service is …
1	High	Tier 1
2	Moderate	Tier 2
3	Low	Tier 3

Note: Some designated internet services have a pre-assessed risk profile for purposes of this industry standard. For example, a high impact DIS is pre-assessed as having a Tier 1 risk profile, and a pre-assessed classified DIS, pre-assessed general purpose DIS and an enterprise DIS are each pre-assessed as having a Tier 3 risk profile.

(9) However, the provider of a designated internet service may, at any time, without having conducted a risk assessment, determine that the risk profile of the service is Tier 1.

8 Methodology, risk factors and indicators to be used for risk assessments and risk profile determinations

Requirement for plan and methodology

(1) If the provider is required by this Part to carry out a risk assessment for a service, the provider must formulate in writing a plan, and a methodology, for carrying out the assessment that ensure that the risks mentioned in subsection 7(1) in relation to the service are accurately assessed.

(2) The provider must ensure that the risk assessment is carried out in accordance with the plan and methodology.

(3) The provider must ensure that a risk assessment is carried out by persons with the relevant skills, experience and expertise.

Forward-looking analyses of likely changes

(4) As part of a risk assessment carried out as required by this Part, the provider must undertake a forward-looking analysis of:

(a) likely changes to the internal and external environment in which the service operates or will operate, including likely changes in the functionality or purpose of, or the scale of, the service; and

(b) the impact of those changes on the ability of the service to meet the object of this industry standard.

Note: For the object of this industry standard see section 4.

Matters to be taken into account

(5) Without limiting subsection (1), the methodology for the conduct of a risk assessment must specify the principal matters to be taken into account in assessing relevant risks, which must include the following, so far as they are relevant to the service:

(a) the predominant purpose of the service;

(b) the functionality of the service, including whether the service enables end-users in Australia to post or share material;

(c) the manner in which material is created or contributed to in connection with the service;

(d) whether the service includes chat, messaging or other communications functionality;

(e) the extent to which material posted on, generated by or distributed using the service will be available to end-users of the service in Australia;

(f) the terms of use for the service;

(g) the terms of arrangements under which the provider acquires content to be made available on the service;

(h) the ages of end-users and likely end-users of the service;

(i) the outcomes of the analysis conducted as required by subsection (4);

(j) safety by design guidance and tools published or made available by a government agency or a foreign or international body;

(k) the risk to the online safety of end-users in Australia in relation to material generated by artificial intelligence;

(l) without limiting paragraph (k), the risk that any generative AI features of the service will be used to generate high impact materials;

(m) where applicable, design features and controls deployed to mitigate the risks referred to in paragraphs (k) and (l).

Note 1: Arrangements referred to in paragraph (g) may include provisions that, if complied with, will reduce the risk that class 1A material and class 1B material will be made available through the service.

Note 2: Examples of agencies mentioned in paragraph (j) are the Commissioner and the Digital Trust & Safety Partnership.

9 Documenting risk assessments and risk profiles

(1) As soon as practicable after determining the risk profile of a designated internet service, the provider of the service must record in writing:

(a) details of the determination; and

(b) details of the conduct of any related risk assessment;

sufficient to demonstrate that they were made or carried out in accordance with this Part.

(2) The record must include the reasons for the results of the assessment and the determination of the risk profile.

Part 4—Online safety compliance measures

Division 1—Preliminary

10 This Part not exhaustive

This Part does not prevent the provider of a designated internet service from taking measures, in addition to and not inconsistent with those required by this Part, to improve and promote online safety for Australians.

11 Determining what is appropriate

(1) In determining whether something (including action) in relation to a designated internet service is appropriate, the matters to be taken into account include:

(a) the extent to which the thing achieves or would achieve the object of this industry standard in relation to the service; and

(b) in relation to a breach of applicable terms of use of a designated internet service in relation to class 1A material or class 1B material:

(i) the nature of the material and the extent to which the breach is inconsistent with online safety for end-users in Australia; and

(ii) the extent to which the thing will or may reasonably be expected to reduce or manage the risk that the service will be used to solicit, generate, access, distribute or store class 1A material or class 1B material;

(c) whether the thing is or would be proportionate to the level of risk to the online safety of end-users in Australia from the material being accessible through the service.

Note 1: For the object of this industry standard see section 4.

Note 2: For paragraph (b), appropriate action may include exercising any of the provider's rights under the terms of use for the service in relation to the breach.

(2) For paragraph (1)(c), in deciding whether a thing is or would be proportionate to the level of risk to online safety of end-users in Australia, take into account the scale and reach of the service.

12 Index of requirements for designated internet services

(1) The following table sets out the provisions of this Part applicable to providers of designated internet services.

Item	For this kind of designated internet service …	the applicable provisions of this Part are…
1	all designated internet services	sections 31, 33 and 37
2	Tier 1 designated internet service	(a) the provisions listed in item 1

Item	For this kind of designated internet service …	the applicable provisions of this Part are…
		(b) sections 17, 18, 19, 20, 24, 25, 26, 27, 28, 29, 30, 32, 34 and 35 (c) subsections 13(2), and 13(4) to (8) (d) subsections 14(2) and (3) (e) subsections 15(2) and (3) (f) subsections 16(2) and (3) (g) subsections 21(2) to (8), and 21(11) (h) subsection 22(2) (i) subsections 23(1) to (3), subparagraphs 23(4)(a)(i) and (ii), and subsections 23(5) to 23(8) (j) subsections 36(2) to (6), and 36(8)
3	Tier 2 designated internet service	(a) the provisions listed in item 1 (b) sections 17, 19, 26, 27, 28, and 34 (c) subsections 13(2), and 13(4) to (8) (d) subsections 14(2) and (3) (e) subsections 15(2) and (3) (f) subsections 16(2) and (3) (g) subsection 24(2) (h) subsections 36(2) to (6)
4	Tier 3 designated internet service	the provisions listed in item 1
5	end-user managed hosting service	(a) the provisions listed in item 1 (b) sections 17, 18, 19, 25, 26, 27, 28, 30, 32, 34 and 35 (c) subsections 13(2), and 13(4) to (8) (d) subsections 14(2), (4) and (5) (e) subsections 15(2) and (3) (f) subsections 16(2) and (4) (g) subsections 20(2) to (6) (h) subsections 21(3) to (7), and 21(9) to (11) (i) subsection 22(2) (j) subsections 23(1) to (3), subparagraphs 23(4)(a)(i) and (ii), paragraph 23(4)(b), and subsections 23(5) to 23(8) (k) subsection 24(2) (l) subsections 36(2) to (6), and 36(8) and (9)
7	high impact generative AI DIS	(a) the provisions listed in item 1 (b) sections 17, 18, 19, 22, 23, 25, 26, 27, 28, 30, 32 and 35 (c) subsections 13(2), and 13(4) to (8) (d) subsections 14(2), (4) and (5)

Item	For this kind of designated internet service …	the applicable provisions of this Part are…
		(e) subsections 15(2) and (3) (f) subsections 16(2) and (4) (g) subsections 20(2) to (6) (h) subsections 21(3) to (8), and 21(11) (i) subsection 24(2) (j) subsections 36(2) to (6), and 36(8) and (9)
8	model distribution platform	(a) the provisions listed in item 1 (b) sections 13, 15, 18, 27 and 28 (c) subsection 14(2) (d) subsection 22(2) (e) subsections 36(2) to (7)

Note 1: Paragraph 23(4)(a)(iii) does not apply to a Tier 1 designated internet service or an end-user managed hosting service.

Note 2: Subsection 23(4)(b) does not apply to a Tier 1 designated internet service.

(2) Where a designated internet service meets the definition of more than one kind of designated internet service under this industry standard, then, for the purposes of this industry standard:

(a) if the service meets the definition of a high impact DIS and a high impact generative AI DIS—the service is taken to be a service of each of those kinds; and

(b) if the service meets the definition of a classified DIS and a high impact generative AI DIS—the service is taken to be a service of each of those kinds; and

(c) if the service meets the definition of an enterprise DIS and an end-user managed hosting service—the service:

(i) when and to the extent made available to enterprise customers—is taken to be an enterprise DIS; and

(ii) when and to the extent made available by the provider directly to end-users in Australia—is taken to be an end-user managed hosting service; and

(d) if the service meets the definitions of 2 or more other kinds of designated internet services—the service will be taken to be the kind of designated internet service that is most closely aligned with the service's predominant purpose.

Note 1: For paragraphs (a) and (b), this means the provider of the service must ensure the service meets the compliance measures that are applicable to each kind of service.

Note 2: For paragraph (c), this means that the provider of the service must ensure the service meets the compliance measures applicable to:

(a) an enterprise DIS (when the service is being provided to enterprise customers); and

(b) an end-user managed hosting service (when the service is being provided directly to end-users).

Division 2—Compliance measures

13 Terms of use

(1) This section applies to the following:
  (a) a Tier 1 designated internet service;
  (b) a Tier 2 designated internet service;
  (c) an end-user managed hosting service;
  (d) a high impact generative AI DIS;
  (e) a model distribution platform.

Provisions to be included in terms of use—generally

(2) The provider of a service must include in the terms of use for the service provisions:
  (a) requiring the account holder of the service to ensure that the service is not used in breach of community standards set out or described in the terms of use; and
  (b) requiring the account holder of the service to ensure that the service is not used, whether by the account holder or by an end-user in Australia, to solicit, access, generate, distribute or store (as applicable, having regard to the purpose and functionality of the service) class 1A material or class 1B material; and
  (c) regulating the use of the service by end-users and requiring the account holder of the service to ensure that end-users of the service comply with those provisions; and
  (d) giving rights for the provider to do any of the following if the service is used to solicit, access, generate, distribute or store (as applicable) child sexual exploitation material or pro-terror material:
    (i) suspend the provision of the service to a specified end-user of the service for a specified period;
    (ii) impose specified restrictions on the use of the service by a specified end-user of the service for a specified period;
    (iii) terminate the agreement for the provision of the service;
    (iv) remove or delete the relevant child exploitation material or pro-terror material from the service, or limit access to it through the service.

Further minimum requirements—model distribution platforms

(3) Without limiting subsection (2), the provider of a model distribution platform must include provisions in the terms of use for the service that:
  (a) require that, for each model uploaded to the service, whether by the account holder or an end-user in Australia, the account holder has taken appropriate steps to minimise the risk of the model being used to generate child sexual exploitation material or pro-terror material; and

(b) give rights for the provider to do any of the following if a model uploaded to the service is used to generate child sexual exploitation material or pro-terror material:

(i) suspend the provision of the service, or the relevant model, to a specified end-user of the service for a specified period;

(ii) impose specified restrictions on the use of the service, or the relevant model, by a specified end-user of the service for a specified period;

(iii) remove or delete the relevant model from the service, or suspend or otherwise limit access to the relevant model by a specified end-user of the service for a specified period;

(iv) terminate the agreement for the provision of the service.

Note: For appropriate see section 11.

(4) It is not necessary that a particular form of words be used in the terms of use so long as the contractual effect of the terms of use are as required by subsections (2) and (3).

Enforcement of terms of use

(5) If the provider of a service becomes aware of a breach of the obligation mentioned in paragraphs (2)(a) or (3)(a), the provider must enforce its contractual rights in respect of the breach in an appropriate way.

Note: For appropriate see section 11.

(6) In proceedings in respect of a contravention of subsection (5), the provider bears the evidential burden of establishing:

(a) the action it took to enforce the rights; and

(b) that the action that it took conformed to the requirements of subsection (5).

Publication of terms of use

(7) The provider of a service must publish its terms of use for the service.

(8) The publication must:

(a) be in plain language; and

(b) be accessible on the website and application (if any) for the service; and

(c) make it clear that class 1A material is not permitted on the service and describe the broad categories of material within class 1A material; and

(d) describe the broad categories of material within class 1B material and specify the extent to which that material is not permitted on the service or is subject to specified restrictions.

Note: For paragraphs (c) and (d) for a high impact generative AI DIS, material includes material that is not permitted to be generated by the service.

14 Systems and processes for responding to class 1A material

Note: For responding to class 1B material see section 16.

(1) This section applies to the following:

(a) a Tier 1 designated internet service;
(b) a Tier 2 designated internet service;
(c) an end-user managed hosting service;
(d) a high impact generative AI DIS;
(e) a model distribution platform.

Minimum requirements—generally

(2) The provider of a service must implement systems and processes that ensure that, if the provider becomes aware that there is or has been a breach of an obligation under the terms of use for the service in respect of class 1A material, the provider takes appropriate action to ensure that:
(a) the breach, if it is continuing, ceases; and
(b) the risk of further such breaches is minimised.

Further minimum requirements—Tier 1 or Tier 2 designated internet services

(3) Without limiting subsection (2), the systems and processes implemented by a provider of a Tier 1 or Tier 2 designated internet service must include ones under which the provider:
(a) reviews reports by end-users of the service in Australia that class 1A material is accessible using the service; and
(b) appropriately prioritises those reports and, if necessary, escalates them to senior management personnel of the provider for action.

Note: For paragraph (a), report includes the reports referred to in section 27.

Further minimum requirements—end-user managed hosting services and high impact generative AI DIS

(4) Without limiting subsection (2), a provider of an end-user managed hosting service or high impact generative AI DIS must establish standard operating procedures that:
(a) require the provider to investigate reports of class 1A material received from end-users to help determine whether the terms of use for the service prohibiting class 1A material on the service have been breached; and
(b) enable the provider to take appropriate action to assess and respond to those breaches.

(5) A provider of an end-user managed hosting service or high impact generative AI DIS must implement the standard operating procedures established as required by subsection (4).

15 Responding to child sexual exploitation material and pro-terror material

Note: For responses in respect of extreme crime and violence material see section 17.

(1) This section applies to the following:
(a) a Tier 1 designated internet service;

(b) a Tier 2 designated internet service;
(c) an end-user managed hosting service;
(d) a high impact generative AI DIS;
(e) a model distribution platform.

Minimum requirements—generally

(2) If the provider of a service becomes aware that the service is being or has been used, whether by the account holder, or by an end-user in Australia, to solicit, access, generate, distribute or store child sexual exploitation material or pro-terror material (whether or not this amounts to a breach of the terms of use for the service), the provider must:
(a) as soon as practicable, remove the material, or cause the material to be removed, from the service unless the provider has been required by an enforcement authority to deal with the material in a manner that requires the material to be retained; and
(b) take appropriate action to ensure that:
(i) the service no longer permits access to or distribution or generation of the material; and
(ii) any related breach of the terms of use for the service, if it is continuing, ceases; and
(iii) the risk of further such breaches of the terms of use for the service is minimised.

(3) Without limiting subsection (2), the provider must:
(a) terminate an end-user's account as soon as reasonably practicable if the end-user:
(i) is distributing child sexual exploitation material or pro-terror materials to end-users with the intention to cause harm; or
(ii) has repeatedly breached terms of use prohibiting child sexual exploitation material and pro-terror materials on the service; and
(b) ensure that end-users and account holders who breach terms of use prohibiting child sexual exploitation material or pro-terror material and who have had their user accounts terminated, do not acquire new accounts.

Further minimum requirements—model distribution platform

(4) Without limiting subsections (2) and (3), if the provider of a model distribution platform becomes aware that a model made available on the service is being or has been used, whether by the account holder, or by an end-user in Australia, to solicit, access, generate, distribute or store child sexual exploitation material or pro-terror material (whether or not this amounts to a breach of the terms of use for the service), the provider must take appropriate action.

Note: For subsection (4), appropriate action includes, but is not limited to, limiting access to the relevant model or models.

16 Systems and processes for responding to breaches of terms of use—class 1B material

(1) This section applies to the following:
  (a) a Tier 1 designated internet service;
  (b) a Tier 2 designated internet service;
  (c) an end-user managed hosting service;
  (d) a high impact generative AI DIS.

Minimum requirements—generally

(2) The provider of a service must implement systems and processes that ensure that, if the provider becomes aware that there is or has been a breach, in Australia, of an obligation under the terms of use for the service in respect of class 1B material, the provider takes appropriate action to ensure that:
  (a) the breach, if it is continuing, ceases; and
  (b) the risk of further such breaches is minimised.

Note: For appropriate see section 11.

Further minimum requirements —Tier 1 or Tier 2 designated internet services

(3) Without limiting subsection (2), the systems and processes implemented by a provider of a Tier 1 or Tier 2 designated internet service must:
  (a) include ones under which the provider:
    (i) reviews reports by end-users of the service in Australia that class 1B materials are accessible using the service; and
    (ii) appropriately prioritises those reports and, if necessary, escalates them to senior management personnel of the provider for action; and
  (b) include operational guidance to provider personnel, including actions to be taken and time limits to be observed, in performing the provider's duties under this section.

Note: For paragraph (a), ***report*** include the reports referred to in section 27.

Further minimum requirements for end-user managed hosting services and high impact generative AI DIS

(4) Without limiting subsection (2), the provider of an end-user managed hosting service or high impact generative AI DIS must implement standard operating procedures that:
  (a) require the provider to engage with reports of class 1B material received from end-users to help determine whether the provider's terms of use relating to class 1B materials on the service have potentially been breached; and
  (b) enable the provider to take appropriate action to assess and respond to potential breaches of terms of use prohibiting class 1B material.

Note: For paragraph (a), ***reports*** include the reports referred to in section 27.

17 Responding to breaches of terms of use in respect of extreme crime and violence material and class 1B material

(1) This section applies to the following:
  (a) a Tier 1 designated internet service;
  (b) a Tier 2 designated internet service;
  (c) an end-user managed hosting service;
  (d) a high impact generative AI DIS.

(2) If the provider of a service becomes aware that there is or has been a breach, in Australia, of an obligation under the terms of use for the service in respect of extreme crime and violence material or class 1B material, the provider must take appropriate action to respond to the breach.

18 Notification of child sexual exploitation material and pro-terror material

(1) This section applies to the following:
  (a) a Tier 1 designated internet service;
  (b) an end-user managed hosting service;
  (c) a high impact generative AI DIS;
  (d) a model distribution platform.

(2) If the provider of a service:
  (a) becomes aware of child sexual exploitation material, or pro-terror material, on the service; and
  (b) believes in good faith that the material affords evidence of a serious and immediate threat to the life or physical safety of a person in Australia;

the provider must, as soon as practicable, report the matter to an enforcement authority, or otherwise as required by law.

(3) If the provider of a service:
  (a) becomes aware of child sexual exploitation material on the service; and
  (b) believes in good faith that the material is not known child sexual abuse material;

the provider must, as soon as practicable, notify an organisation of a kind referred to in paragraph (b) of the definition of ***known child sexual abuse material*** in subsection 6(1).

(4) If the provider of a service:
  (a) identifies pro-terror material on the service; and
  (b) believes in good faith that the material is not known pro-terror material;

the provider must, as soon as practicable, notify an appropriate non-governmental organisation that:
  (c) verifies material as pro-terror material; or
  (d) is generally recognised as having expertise in counter-terrorism.

(5) Subsections (2), (3) and (4) are in addition to any other applicable law.

19 Resourcing trust and safety functions

(1) This section applies to the following:
  (a) a Tier 1 designated internet service;
  (b) a Tier 2 designated internet service;
  (c) an end-user managed hosting service;
  (d) a high impact generative AI DIS.

(2) The provider of a service must have and implement, in respect of the service, management, supervision and internal reporting arrangements to ensure that at all times the provider:
  (a) complies with the requirements of this industry standard; and
  (b) can otherwise effectively supervise the online safety of the service.

Note: These arrangements may include duties and responsibilities for personnel, and systems, processes and technologies.

(3) The provider of a service must have, or have access to, sufficient personnel who have the skills, experience and qualifications needed to ensure that the provider complies with the requirements of this industry standard at all times.

20 Detecting and removing known child sexual abuse material

(1) This section applies to the following:
  (a) a Tier 1 designated internet service;
  (b) an end-user managed hosting service;
  (c) a high impact generative AI DIS.

Minimum requirements—generally

(2) The provider of a service must implement appropriate systems, appropriate processes and appropriate technologies to:
  (a) detect and identify known child sexual abuse material that:
    (i) is stored on the service; or
    (ii) is accessible by an end-user in Australia using the service; or
    (iii) is being or has been accessed or distributed in Australia using the service; and
  (b) remove known child sexual abuse material from the service as soon as practicable after the provider becomes aware of it.

Note 1: The technologies that the provider may use include hashing technologies and machine learning.

Note 2: For a high impact generative AI DIS, compliance with this subsection may require the provider to assess whether inputs into the service contain child sexual abuse material.

(3) Subsection (2) does not require a provider to use a system or technology if:
  (a) it is not technically feasible or reasonably practicable for the provider to do so; or
  (b) to do so would require the provider to:

(i) implement or build a systemic weakness, or a systemic vulnerability, into the service;

(ii) in relation to an end-to-end encrypted service—implement or build a new decryption capability into the service, or render methods of encryption used in the service less effective.

(4) If, because of subsection (3), a provider does not implement any systems as described in subsection (2) the provider must take appropriate alternative action.

(5) If, because of subsection (3), a provider does not implement any technologies as described in subsection (2) the provider must take appropriate alternative action.

Note: For appropriate see section 11.

(6) This section does not affect the operation of section 22.

Note: This section does not prevent a provider from complying with legal obligations to preserve evidence of offences.

Further minimum requirements —Tier 1 designated internet services

(7) Without limiting subsection (2) to (6), the provider of a Tier 1 designated internet service must ensure that the service uses systems, processes and technologies that:

(a) prevent end-users from distributing known child sexual abuse material through the service; and

(b) identify phrases or words commonly linked to child sexual abuse material and linked activity to enable the provider to deter and reduce the incidence of such material and linked activity on the service.

21 Detecting and removing known pro-terror material

(1) This section applies to the following:

(a) a Tier 1 designated internet service;

(b) an end-user managed hosting service;

(c) a high impact generative AI DIS.

(2) However, this section does not apply to a Tier 1 designated internet service predominantly used for making pornography available.

Minimum requirements—generally

(3) The provider of a service must have and maintain appropriate systems, appropriate processes and appropriate technologies that detect and identify known pro-terror material that:

(a) is being distributed by or to an end-user in Australia using the service;

(b) is stored on the service; or

(c) is being accessed by an end-user in Australia using the service.

Note 1: The technologies that the provider may use include hashing technologies and machine learning.

Note 2: For a high impact generative AI DIS, compliance with this subsection may require the provider to assess whether inputs into the service contain pro-terror material.

Note 3: See subsections (8) to (11) for the requirement to implement such systems, processes and technologies.

(4) The provider of a service must remove known pro-terror material from the service as soon as practicable after the provider detects or identifies the material through a system or technology described in subsection (3).

(5) Subsection (3) does not require a provider to have or implement a system or technology if:

(a) it is not technically feasible or reasonably practicable for the provider to do so; or

(b) to do so would require the provider to:

(i) implement or build a systemic weakness, or a systemic vulnerability, into the service; or

(ii) in relation to an end-to-end encrypted service—implement or build a new decryption capability into the service, or render methods of encryption used in the service less effective.

(6) If, because of subsection (5), a provider does not have or implement any systems as described in subsection (3), the provider must take appropriate alternative action.

(7) If, because of subsection (5), a provider does not have or implement any technologies as described in subsection (3) the provider must take appropriate alternative action.

Note: For appropriate see section 11.

Implementation of systems and technologies—Tier 1 designated internet services and high impact generative AI DIS

(8) The provider of a Tier 1 designated internet service or high impact generative AI DIS must implement the systems, processes and technologies described in subsection (3) at all times.

Implementation of systems and technologies—end-user managed hosting service

(9) The provider of an end-user managed hosting service must implement the systems, processes and technologies described in paragraph (3)(a) at all times.

(10) The provider of an end-user managed hosting service must implement the systems, processes and technologies described in paragraphs (3)(b) and (c) in respect of material stored on the service, or being accessed using the service, as soon as practicable after the provider suspects or has reason to suspect that the material:

(a) is known pro-terror material; and

(b) is being stored on the service by an end-user in Australia; and

(c) has been accessed by more than 1 end-user.

(11) This section does not affect the operation of section 22.

Note: This section does not prevent a provider from complying with legal obligations to preserve evidence of offences.

22 Disrupting and deterring child sexual exploitation material and pro-terror material

(1) This section applies to the following:
(a) a Tier 1 designated internet service;
(b) an end-user managed hosting service;
(c) a high impact generative AI DIS;
(d) a model distribution platform.

Minimum requirements—generally

(2) The provider of a service must implement systems and processes and, if it is appropriate to do so, technologies that:
(a) effectively deter end-users of the service from using the service; and
(b) effectively disrupt attempts by end-users of the service to use the service;
to solicit, generate, access, distribute or otherwise make available, or store, child sexual exploitation material or pro-terror material (including known child sexual abuse material and known pro-terror material).

Note 1: Examples of systems, processes and technologies include hashing, machine learning and artificial intelligence systems that scan for known child sexual abuse material and those that are designed to detect key words, behavioural signals and patterns associated with child sexual abuse material.

Note 2: For appropriate see section 11.

Further minimum requirements —high impact generative AI DIS

(3) Without limiting subsection (2), the provider of a high impact generative AI DIS must, at a minimum:
(a) implement systems, processes and technologies that prevent generative AI features from being used to generate outputs that contain child sexual exploitation material or pro-terror material; and
(b) regularly review and test models on the potential risk that a model is used to generate child sexual exploitation material or pro-terror material; and
(c) promptly following review and/or testing, adjust models and deploy mitigations with the aim of reducing the misuse and unintentional use of models to generate child sexual exploitation material or pro-terror material; and
(d) implement systems, processes and technologies that differentiate AI outputs generated by the model; and
(e) ensure that end-users in Australia specifically seeking images of child sexual abuse material are presented with prominent messaging that outlines the potential risk and criminality of accessing child sexual abuse material; and

(f) ensure that material generated for end-users in Australia using terms that have known associations to child sexual exploitation material are accompanied by information or links to services that assist end-users in Australia to report child sexual exploitation material to enforcement agencies, to seek support or both; and

(g) ensure that the systems, processes and technologies implemented by the provider under subsection (2) are able to detect automatically and take appropriate action in respect of child sexual abuse material in training data, user prompts, and outputs.

Note 1: A requirement to put in place systems, processes, and technologies to disrupt and deter the production of child sexual exploitation material should take account of the fact that not all high impact generative AI DIS providers will always have sufficient visibility and control of their models—if a provider lacks that visibility or control of certain aspects so that it cannot deploy all mitigations, it will have to rely on other systems, processes and technologies that are available.

Note 2: For paragraph (d), systems, processes and technologies may include by embedding indicators of provenance into material generated by a model to enable differentiation.

Note 3: For paragraph (g), systems, processes and technologies may include using hashing, key word lists, classifiers or other safety technologies designed or used to prevent child sexual exploitation material from being generated using services of the relevant kind.

23 Development programs

(1) This section applies:

(a) to the following:

(i) a Tier 1 designated internet service;

(ii) a high impact generative AI DIS;

but only where the average monthly number of active end-users of the service, in Australia, over the immediate previous calendar year was 1,000,000 or more; and

(b) to an end-user managed hosting service but only where the average monthly number of active end-users of the service, in Australia, over the immediate previous calendar year was 500,000 or more.

(2) However:

(a) this section, so far as it relates to pro-terror material, does not apply to a Tier 1 designated internet service predominantly used for making pornography available; and

(b) subparagraph (4)(a)(iii) does not apply to a Tier 1 designated internet service or an end-user managed hosting service; and

(c) paragraph (4)(b) does not apply to a Tier 1 designated internet service.

(3) The provider of the service must establish and implement, for the calendar year, a program of investment and development activities (***development program***) in respect of systems, processes and technologies.

Note: See also section 35.

(4) A development program must include:

(a) investments and activities designed to develop systems, processes and technologies that enhance the ability of the provider, or of other providers of designated internet services:
  (i) to detect and identify child sexual abuse material or pro-terror material (including known child sexual abuse material and known pro-terror material) on the service; and
  (ii) to deter end-users of the service from using the service, and to disrupt attempts by end-users of the service to use the service, to generate, access, distribute or store child sexual exploitation material or pro-terror material (including known child sexual abuse material and known pro-terror material); and
  (iii) to reduce the risk to the online safety of end-users in Australia in relation to class 1A material or class 1B material generated by artificial intelligence; and
(b) arrangements for cooperating and collaborating with other organisations in activities of the kind referred to in paragraph (a) and to enhance online safety for Australians.

(5) A development program may include arrangements for the provider to make available to other providers of designated internet services, or organisations engaged in promoting online safety for Australians, systems, processes and technologies of a kind referred to in paragraph (4)(a) (including making them available without charge).

(6) The value and scale of the investment and development activities implemented in a calendar year must effectively address the need to enhance the ability of the provider to do the things mentioned in subsection (4), having regard to the nature and functionalities of the service concerned and the average monthly number of active end-users of the service, in Australia, over the immediate previous calendar year.

(7) Examples of activities that may be part of a provider's development program include:
(a) joining industry organisations intended to address serious online harms; and
(b) sharing information on best practice approaches relevant to the service; and
(c) working with the Commissioner to share information, intelligence, best practice and other information relevant to addressing categories of class 1A material or class 1B material that are relevant to the service; and
(d) collaborating with non-government or other organisations that facilitate the sharing of information, intelligence, best practices and other information relevant to addressing categories of class 1A or class 1B material that are relevant to the service.

(8) Examples of investments that may be part of a provider's development program include:

(a) procuring online safety systems and technologies for use in connection with the service, or enhancing online safety systems and technologies used in connection with the service; and
(b) conducting research into and development of online safety systems and technologies; and
(c) providing support, either financial or in kind, to organisations the functions of which are or include working to combat child sexual abuse, child sexual exploitation or terrorism.

24 Safety features and settings

(1) This section applies to the following:
(a) a Tier 1 designated internet service;
(b) a Tier 2 designated internet service;
(c) an end-user managed hosting service; and
(d) a high impact generative AI DIS.

Minimum requirements—generally

(2) Before the provider of the service makes a material change to the service, the provider must:
(a) carry out an assessment of the kinds of features and settings that could be incorporated into the service to minimise the risk that class 1A material or class 1B material:
(i) will be generated by, accessed by, or distributed to, end-users in Australia using the service; or
(ii) will be stored on the service; and
(b) determine, on the basis of the assessment, the most appropriate and effective features and settings for the service; and
(c) ensure that the service as so changed incorporates at all times the features and settings so determined.

(3) Subsections (4) and (5) do not limit subsection (2) and apply whether or not a material change is made or proposed to the service.

Further minimum requirements for a provider of a Tier 1 designated internet service

(4) The provider of a Tier 1 designated internet service must:
(a) implement measures that ensure that material can only be posted to or distributed on the service by a registered account holder; and
(b) make clear in terms of use that an Australian child is not permitted to hold an account on the service.

(5) The provider of the service must take appropriate action to:
(a) ensure that a child in Australia who is known by the provider to be under the age of 18 does not become an end-user of the service; and

(b) stop access to the service by a child in Australia who is known by the provider to be under the age of 18.

25 Responding to and referring unresolved complaints to the Commissioner

(1) This section applies to the following:
   (a) a Tier 1 designated internet service;
   (b) an end-user managed hosting service;
   (c) a high impact generative AI DIS.

(2) The provider of a service must implement policies and procedures that ensure that:
   (a) it responds in a timely and appropriate manner to communications from the Commissioner about compliance with this industry standard; and
   (b) if the provider becomes aware that a complainant is dissatisfied with the way in which the report or complaint was dealt with or with the outcome of a complaint—the provider refers the complaint to the Commissioner in accordance with section 30.

26 Giving information about the Commissioner to end-users in Australia

(1) This section applies to the following:
   (a) a Tier 1 designated internet service;
   (b) a Tier 2 designated internet service;
   (c) an end-user managed hosting service;
   (d) a high impact generative AI DIS.

(2) The provider of a service must ensure that information:
   (a) describing the role and functions of the Commissioner; and
   (b) describing how to refer a matter about the service or the provider to the Commissioner; and
   (c) describing the mechanisms and processes required by section 27 for the service;

   is accessible to end-users of the service in Australia at all times through a dedicated location on the service. The location must be "in service", that is, not on a separate website or application to the website or application for the service.

Division 3—Reports and complaints from end-users

27 Mechanisms for end-users and account holders to report, and make complaints, to providers

(1) This section applies to the following:
  (a) a Tier 1 designated internet service;
  (b) a Tier 2 designated internet service;
  (c) an end-user managed hosting service;
  (d) a high impact generative AI DIS;
  (e) a model distribution platform.

(2) The provider of a service must provide 1 or more tools that enable end-users and account holders of the service in Australia to do the following:
  (a) make a report to the provider, identifying or flagging class 1A material or class 1B material accessible on or through the service;
  (b) make a complaint to the provider about:
    (i) material referred to in paragraph (a); or
    (ii) the provider's non-compliance with this industry standard.

An end-user or account holder who makes a report or complaint under this section is a ***complainant***.

Note 1: For paragraph (a) for a high impact generative AI DIS, material includes material generated (or capable of being generated) by the service.

Note 2: For paragraph (a) for a model distribution platform, material ***accessible on or through the service*** includes material generated by models made available on the service.

(3) The tools required by subsection (2) must:
  (a) be easily accessible on or through the service and easy to use; and
  (b) include or be accompanied by clear instructions on how to use them; and
  (c) enable the complainant to specify the harm associated with the material, or the non-compliance, to which the report or complaint relates.

(4) The provider must ensure that the identity of a complainant is not accessible, directly or indirectly, by any other end-user or account holder of the service without the express consent of the complainant.

28 Dealing with reports and complaints from end-users–general rules

(1) This section applies to the following:
  (a) a Tier 1 designated internet service;
  (b) a Tier 2 designated internet service;
  (c) an end-user managed hosting service;
  (d) a high impact generative AI DIS;
  (e) a model distribution platform.

(2) If a person makes a report or complaint to the provider of the service under subsection 27(2), the provider must:
  (a) respond promptly to the complainant acknowledging the report or complaint; and
  (b) take appropriate and timely action to investigate the report or complaint.

Note: For appropriate see section 11.

(3) Paragraph (2)(b) does not apply if:
  (a) the provider believes on reasonable grounds that the report is frivolous, vexatious or otherwise not made in good faith; or
  (b) the matter the subject of the report is being investigated, or has been investigated, by the Commissioner under Division 5 of Part 3 of the Act.

(4) The provider of the service must:
  (a) notify the complainant of the outcome of any investigation into the report or complaint and the action proposed by the provider in consequence of the investigation; or
  (b) if the provider did not investigate the report or complaint because of subsection (3)—notify the complainant of that fact and of any action proposed by the provider in consequence of the complaint.

(5) The provider of a service must:
  (a) record in writing its systems, processes and technologies used to conduct investigations and reviews under this Division; and
  (b) ensure that its personnel who investigate reports and complaints, and conduct reviews, as required by this Division, have appropriate training and experience, including training in and experience of the provider's applicable policies and procedures.

29 Review of reports and complaints—additional rules for Tier 1 designated internet services

(1) This section applies to a Tier 1 designated internet service where a complainant makes a report or complaint to the provider about class 1A material or class 1B material accessible on or through the service.

Note: See paragraphs 27(2)(a) and subparagraph 27(2)(b)(ii).

(2) The provider of a service must:
  (a) ensure that the complainant can, within 1 month after being notified under subsection 28(4), require the provider to conduct a review of the outcome of the investigation into the report or complaint; and
  (b) if the complainant requires such a review—ensure that:
    (i) the outcome is reviewed in accordance with subsection (3); and
    (ii) the complainant is notified promptly of the outcome of the review.

(3) For a review under subsection (2):

(a) the review must be conducted by a person other than the person who conducted the investigation into the report or complaint concerned; and
(b) the provider must take appropriate action to facilitate the review.

30 Unresolved complaints about non-compliance to be referred to the Commissioner

(1) This section applies to the following:
(a) a Tier 1 designated internet service;
(b) an end-user managed hosting service;
(c) a high impact generative AI DIS.

(2) If:
(a) a complainant makes a report or complaint to the provider about the provider's non-compliance with this industry standard; and
(b) the provider becomes aware that the complainant is dissatisfied with:
(i) the way in which the report or complaint was dealt with; or
(ii) the outcome of the report or complaint;
the provider must refer the complaint to the Commissioner.

Note: For paragraph (a), see subparagraph 27(2)(b)(ii).

(3) The Commissioner may, by written notice to the provider, require the provider to give the Commissioner, within a specified period, specified information or documents that it holds that are relevant to the complaint. The provider must comply with the requirement.

Division 4—Reporting requirements

31 Commissioner may require documents about risk assessments and other information

(1) The Commissioner may, by written notice to the provider of a designated internet service, require the provider to give the Commissioner any of the following documents:

(a) the most recent risk profile determination for the service;

(b) the record, as required by section 9, of the most recent risk assessment for the service;

(c) the most recent assessment under paragraph 24(2)(a) for the service;

(d) the applicable risk methodology for the most recent risk assessment for the service;

(e) the provider's development program for a specified calendar year.

Note: For development programs see section 23.

(2) The provider must give the documents to the Commissioner within the period specified in the notice.

Note: See also section 37.

32 Reports relating to technical feasibility and practicability of compliance with provisions of Division 2

(1) The Commissioner may, by written notice to the provider of a designated internet service, require the provider to give the Commissioner a report:

(a) that describes:

(i) the cases in which it was not, or would not, be technically feasible; or

(ii) the cases in which it was not, or would not, be reasonably practicable;

for the provider to comply with an obligation under Division 2 to implement systems or technologies of a particular kind; and

(b) in the case of obligations under subsection 20(2)—that describes the systems and technologies that were or are available but were not, or would not be, implemented because of paragraph 20(3)(b); and

(c) in the case of obligations under subsection 21(3)—that describes the systems and technologies that were or are available but were not, or would not be, implemented because of paragraph 21(5)(b); and

(d) in each case—that describes the alternative action taken or that would be taken as required by subsections 20(4) or (5), or 21(6) or (7).

Note 1: Section 20 is about known child sexual abuse material.

Note 2: Section 21 is about known pro-terror material.

(2) The report must provide justification for the actions described, and the conclusions, in the report.

(3) The Commissioner may, by written notice to the provider, require the report to be in a specified form. The provider must comply with the requirement.

(4) A report may relate to 2 or more services.

(5) The provider must give the report to the Commissioner within the period specified in the notice.

Note: See also section 37.

33 Notifying changes to features and functions of designated internet services – generating high impact material

Note: A provider is also required to carry out an assessment under subsection 24(2) before the provider makes a material change to the service.

(1) This section applies to all designated internet services.

(2) If the provider of a service decides to:

(a) add a new feature or function to the service; or

(b) remove a feature or function from a service or make a feature or function inoperable for a service;

the provider must notify the Commissioner of the proposed change as soon as practicable after making the decision unless the provider believes, on reasonable grounds, that the proposed change will not significantly increase the risk that the service will be used to generate high impact material.

(3) If:

(a) a new feature or function is added to a service; or

(b) a feature is removed from a service or made inoperable for a service;

the provider of the service must notify the Commissioner of the change as soon as practicable after it is implemented unless the provider believes, on reasonable grounds, that the change has not significantly increased the risk that the service will be used to generate high impact material.

34 Notifying changes to features and functions of designated internet services—general

Note: A provider is also required to carry out an assessment under subsection 24(2) before the provider makes a material change to the service.

(1) This section applies to the following:

(a) a Tier 1 designated internet service;

(b) a Tier 2 designated internet service;

(c) an end-user managed hosting service.

(2) If the provider of a service decides to:

(a) add a new feature or function to the service; or

(b) remove a feature or function from a service or make a feature or function inoperable for a service;

the provider must notify the Commissioner of the proposed change as soon as practicable after making the decision unless the provider believes, on reasonable grounds, that the proposed change will not significantly increase the risk that the service will be used to solicit, access distribute or store class 1A material or class 1B material.

Note: For notification of changes relating to generation of high impact material see section 33.

(3) If:

(a) a new feature or function is added to a service; or

(b) a feature or function is removed from a service or made inoperable for a service;

the provider of the service must notify the Commissioner of the change as soon as practicable after it is implemented unless the provider believes, on reasonable grounds, that the change has not significantly increased the risk that the service will be used to solicit, access distribute or store class 1A material or class 1B material.

Note: For notification of changes relating to generation of high impact material see section 33.

35 Reports on outcomes of development programs

(1) The Commissioner may, by written notice to the provider of a designated internet service to which section 23 applied in respect of a particular calendar year, require the provider to give the Commissioner, within a specified period, a report that specifies:

(a) the activities and investments undertaken by the provider in respect of the calendar year to implement its development program; and

(b) the outcomes of those activities and investments in terms of enhancing online safety for end-users in Australia.

(2) The Commissioner may, by written notice to the provider, require the report to be in a specified form. The provider must comply with the requirement.

(3) The provider must give the report to the Commissioner within the period specified in the notice.

Note: See also section 37.

36 Commissioner may require compliance reports

(1) This section applies to the following:

(a) a Tier 1 designated internet service;

(b) a Tier 2 designated internet service;

(c) an end-user managed hosting service;

(d) a high impact generative AI DIS;

(e) a model distribution platform.

Minimum requirements—generally

(2) The Commissioner may, by written notice given to the provider of a service, require the provider to give the Commissioner a report (a ***compliance report***) for the most recent calendar year before the date of the notice (the ***reporting period***) that:

(a) specifies the steps that the provider has taken, including measures and controls the provider has implemented, to comply with applicable compliance measures in this Part;

(b) includes confirmation from the provider that the steps, measures and controls are appropriate, including reasonable supporting details and evidence;

(c) specifies the number of complaints made to the provider about the provider's compliance with this industry standard during the period specified in the notice; and

(d) where applicable for the relevant designated internet service, such other details as specified in subsections (7) and (8).

(3) However, the Commissioner may not request a report under this section in respect of a designated internet service:

(a) at any time prior to the first anniversary of the commencement of this industry standard; and

(b) without limiting paragraph (a), more than once in any 12 month period.

(4) The notice under subsection (2) may require the report to be in a specified form.

(5) The provider must comply with a notice under this section within 2 months after the notice under subsection (2) is given.

Note: See also section 37.

(6) A compliance report may relate to 2 or more services.

Further minimum requirements —model distribution platform

(7) Without limiting subsection (2), the provider of a model distribution platform must ensure that any report required by this section for a reporting period:

(a) specifies:

(i) the volume of child sexual exploitation material and pro-terror material identified by the provider in relation to the service in the reporting period, where it is technically feasible for the provider to identify such material; and

(ii) the number of models identified by the provider to be in breach of the provider's terms of use relating to child sexual exploitation material or pro-terror material;

(b) specifies the way in which the details and materials under paragraph (a) (if any) were identified; and

(c) includes details of the action taken by the provider in the reporting period in respect of the details and materials identified in paragraph (a).

Example: For paragraph (b): identification through reports made to the provider, hashing or through other measures and controls implemented by the provider.

Further minimum requirements—Tier 1 designated internet service, end-user managed hosting service, high impact generative AI DIS

(8) Without limiting subsection (2), the provider of a Tier 1 designated internet service, end-user managed hosting service or high impact generative AI DIS must ensure that the compliance report:

(a) specifies the volume of child sexual exploitation material and pro-terror material identified by the provider in relation to the service;

(b) specifies the manner in which the materials under paragraph (a) (if any) were identified;

(c) includes details of the action taken by the provider in respect of materials identified under paragraph (a); and

(d) specifies the average monthly number of active end-users of the service, in Australia, in the reporting period, and how that number was worked out.

Example: For paragraph (b): identification through reports made to the provider, hashing or through other measures and controls implemented by the provider.

Further minimum requirements—end-user managed hosting service and high impact generative AI DIS

(9) Without limiting subsections (2) and (8), the provider of an end-user managed hosting service or a high impact generative AI DIS must ensure that the compliance report sets out:

(a) details of any limitations on the service or the provider to identify, assess or take action in respect of class 1A material and class 1B material; and

(b) where relevant, a description of the design and technology features of the service giving rise to the limitations under (a); and

(c) the impact of such limitations on the matters specified in paragraphs (8)(a), (b) and (c).

37 Extension of reporting deadlines

The Commissioner may, on application, grant a provider an extension of time, for a specified period or to a specified date, for giving the Commissioner a document, report or notification under this Division, and may do so before or after the time for giving the document, report, certificate or notification has passed.

Part 5—Miscellaneous

38 Record-keeping

(1) This section applies to all designated internet services.

(2) The provider of a service must keep records that set out the actions that the provider has taken to comply with this industry standard.

(3) The provider must keep the records for at least 2 years after the end of the calendar year during which the action was taken.