AI IMPACT SUMMIT
भारत 2026 INDIA

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

FREQUENTLY ASKED QUESTIONS

on

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026

[through amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021]

(10th February, 2026)

Government of India

Ministry of Electronics and Information Technology (MeitY)

Table of Contents

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026

Frequently Asked Questions (FAQs)

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026

Introduction

The Government of India is committed to ensuring an Open, Safe, Trusted, and Accountable Internet for its citizens availing Internet-enabled services. In order to ensure an Open, Safe & Trusted Internet and accountability of intermediaries including the social media intermediaries to users, the Ministry of Electronics and Information Technology (MeitY), in exercise of the powers given under the Information Technology Act, 2000 ("IT Act"), notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (hereinafter referred to as "**IT Rules, 2021**") on 25th February, 2021 and subsequently amended time-to-time on various dates viz. 28th October, 2022, 6th April, 2023 and 22nd October, 2025 respectively to address the emerging risks and issues in the cyberspace.

With the advances in artificial intelligence (AI) and machine learning technologies, online platforms are now capable of generating synthetic content that is highly realistic in nature. Synthetically generated information ("**SGI**"), when developed and used responsibly, offers significant benefits to users in India by enabling innovation, accessibility, and economic growth across sectors. Such technologies support the creation of multilingual and local-language content, improve access to education and skill development through personalised learning tools, and enhance public service delivery through simulations, virtual assistants, and data-driven decision-making. Synthetic information can also promote inclusion by enabling assistive technologies for persons with disabilities, supporting creative expression, and empowering small businesses, startups, and creators with affordable digital tools. If harnessed with robust safeguards, synthetically generated information can strengthen India's digital economy, foster trust in the online ecosystem, and advance the goal of inclusive, safe, and responsible digital transformation.

However, every new technology advancement comes with its own unique challenges and recognising the challenges posed by growing misuse of SGI, including deepfakes, misinformation, and other unlawful content capable of misleading users causing user harms, violating privacy, or threatening national integrity, the Ministry of Electronics and Information Technology (MeitY) has made amendments to the IT Rules, 2021 in relation to the SGI and other associated concerns by notifying **the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026**, *vide* Gazette notification number G.S.R. 120(E), dated 10th February, 2026, which shall come into force on **20 th February, 2026**.

The following FAQs have been prepared to bring clarity as well as to explain the nuances of the due diligence to be followed by intermediaries in relation to the SGI and other associated concerns. The FAQs are limited to the IT Rules, 2021 to be administered by MeitY.

Note: This document is in response to general queries received by MeitY. It is not a legal document and in no way whatsoever replaces, amends or alters any part of the IT Act/ IT Rules, 2021 (as amended). For legal compliance, the notified Rules may be referred to.

The FAQ is an evolving document and hence the versions of this document may undergo changes. It is requested that the concerned stakeholders verify the version of this document from MeitY.

Section I: Overview and Objectives

1. What are the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026?

Ans: The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 amend the IT Rules, 2021 to further strengthen the due diligence framework for intermediaries, particularly in relation to **synthetically generated information (SGI)** and associated online harms. The amendments, *inter alia*, cover the following broad areas:

- insertion of definitions relating to **"audio, visual or audio-visual information"** and **"synthetically generated information (SGI)"**, along with specific exclusions of certain categories information from the definition of SGI;
- clarification that, for purposes of these Rules, references to **"information"** in the context of unlawful acts shall include **SGI**;
- clarification that removal/disablement of information including SGI in compliance with the Rules (including through reasonable technical measures / automated tools) shall **not** amount to violation of section 79(2)(a) or 79(2)(b) conditions (safe harbour);
- strengthening of **user awareness obligations**, including periodic user information at least once every three months, and additional warnings for intermediaries facilitating SGI creation;
- strengthening of **timelines for compliance**, including reduced timelines for takedown upon actual knowledge and for grievance redressal (including special categories such as nudity/impersonation etc.);
- introduction of a dedicated SGI due diligence framework under **Rule 3(3)**, including:
    - measures to prevent unlawful/prohibited SGI; and
    - labelling/metadata/identifier obligations for permissible SGI;
- additional due diligence obligations for **Significant Social Media Intermediaries (SSMIs)**, including user declaration and technical verification before publishing SGI, and prominent labelling of SGI.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, *vide* Gazette notification number G.S.R. 120(E), dated 10th February, 2026 may be accessed at the following link:

https://egazette.gov.in/WriteReadData/2026/269993.pdf

https://www.meity.gov.in/static/uploads/2026/02/f55fe52418b03f58b0669f6a8bc03b6d.pdf

The consolidated IT Rules, 2021 (as updated), as they would stand after incorporating the afore-said new amendments may be accessed at the following link:

https://www.meity.gov.in/static/uploads/2026/02/550681ab908f8afb135b0ad42816a1c9.pdf

2. Why were these amendments introduced?

Ans: The amendments were introduced in view of rapid advances in artificial intelligence (AI) and machine learning technologies, which have made it significantly easier to create, generate, modify or alter highly realistic synthetic audio, visual and audio-visual content, including deepfakes, that can appear real, authentic or true and may mislead or deceive users. While synthetically generated information (SGI) can deliver significant benefits such as innovation, accessibility and inclusive digital growth, its increasing misuse has emerged as a serious and evolving challenge.

Such misuse can lead to serious harms, including, *inter alia*:

- spread of misinformation/disinformation and erosion of public trust;
- impersonation, identity fraud and deception;
- non-consensual intimate imagery, obscenity and child sexual exploitative and abuse material;
- reputational harm, coercion, extortion and severe psychological impact on victims;

Accordingly, to ensure an Open, Safe, Trusted and Accountable Internet, and to address the unique risks posed by SGI in a clear and enforceable manner, the amendments seek to strengthen the IT Rules, 2021 by:

- introducing clear definitions of SGI and related audio/visual information along with specific exclusions;
- clarifying that references to "information" used for unlawful acts shall include **SGI**;
- strengthening user awareness and accountability obligations (including periodic user advisories and additional warnings for SGI-enabling intermediaries);
- prescribing a dedicated due diligence framework under Rule 3(3) requiring intermediaries to deploy reasonable and appropriate technical measures to prevent unlawful SGI, and to ensure labelling/provenance/identifier requirements for permissible SGI;
- introducing enhanced obligations for Significant Social Media Intermediaries (SSMIs), including user declaration and technical verification prior to publication/display of SGI and ensuring prominent labelling;
- tightening by reducing the removal/disabling access/grievance timelines to enable faster response and victim protection; and
- clarifying that removal/disablement of information (including SGI) in compliance with these Rules (including through automated tools) shall not by itself impact intermediaries' eligibility for exemption under section 79(2) of the IT Act.

In brief, these amendments aim to establish a regulatory framework that protects users while encouraging responsible innovation. The amendments prescribe clear obligations for the handling of synthetically generated information. They require intermediaries to deploy technical measures to prevent unlawful synthetic content, require labelling and provenance metadata for synthetic content, tighten timelines and reporting obligations, and clarify that lawful removal of such content by intermediaries does not remove their exemption from liability.

3. From when do the Amendment Rules, 2026 take effect?

Ans: The Amendment Rules, 2026 come into force on the date specified in the notification *vide* Gazette notification number **G.S.R. 120(E), dated 10th February, 2026**. As per this, the Amendment Rules, 2026 shall come into force on 20th February, 2026.

Section II: Key Definitions and Scope

4. What is meant by "audio, visual or audio-visual information"?

Ans: A new definition "audio, visual or audio-visual information" has been inserted under Rule 2(1)(ca) of the IT Rules, 2021 (as amended). It means any audio, image, photograph, graphic, video, moving visual recording, sound recording or any other audio/visual/audio-visual content, with or without accompanying audio, whether created/generated/modified/altered through a computer resource.

5. What is "synthetically generated information" (SGI)?

Ans: As per Rule 2(1)(wa) of the IT Rules, 2021 (as amended), **"**synthetically generated information" (SGI) means audio, visual or audio-visual information which is artificially or algorithmically created, generated, modified or altered using a computer resource, in a manner that such information appears to be real, authentic or true, and depicts or portrays any individual or event in a manner that is, or is likely to be perceived as indistinguishable from a natural person or a real-world event.

In simple terms, SGI refers to synthetic media that can realistically appear like a real person (including their appearance or voice) or a real-world event, in a way that may deceive viewers into believing that it is genuine.

This may include, for example, what is commonly referred to as **deepfakes**, **AI-generated/AI-altered images and videos**, **voice cloning**, and other forms of realistic synthetic audio-visual content, provided such content meets the above legal threshold of appearing real/authentic/true and being indistinguishable from real persons/events.

6. What types of content are not considered 'synthetically generated information' (SGI) (i.e., not treated as SGI)?

Ans: Considering that the synthetically generated information (SGI) can deliver significant benefits such as innovation, accessibility and inclusive digital growth, the definition of "synthetically generated information" (SGI) under Rule 2(1)(wa) of the IT Rules, 2021 (as amended) also provides specific exclusions of certain categories information from the definition, to ensure that routine, good-faith uses of AI or other technologies for editing, formatting, or improving content are not unnecessarily regulated as SGI.

Accordingly, the following types of content are **not treated as SGI**:

(a) Routine or good-faith editing / enhancement (without misrepresentation): Routine or good-faith actions such as editing, formatting, enhancement, technical correction, colour adjustment, noise reduction, transcription, or compression shall not be treated as SGI, provided such actions do not materially alter, distort, or misrepresent the substance, context or meaning of the underlying content.

Examples (not SGI): (for clarity)

- increasing brightness/contrast or sharpening a photo without changing what it depicts;
- compressing a video for faster upload/streaming;
- removing background noise in an audio recording;
- transcribing an audio/video interview into text;
- stabilising a shaky video or correcting colour balance.

(b) Routine good-faith creation/preparation of documents/materials (without false documents/records): Routine or good-faith creation/preparation/formatting/design of documents, presentations, PDF files, educational/training materials, or research outputs (including use of illustrative, hypothetical, draft, template-based or conceptual content) shall not be treated as SGI, so long as it does not result in creation of false documents or false electronic records.

Examples (not SGI): (for clarity)

- preparing a PowerPoint slide deck using templates/AI design tools;
- generating illustrative diagrams/flowcharts for training or awareness;
- creating hypothetical scenarios/case studies for classroom/research use;
- drafting a sample notice/order for internal training;
- formatting a PDF report using AI tools.

However (important clarification):

If AI tools are used to generate fake certificates, fake official letters, forged IDs or fabricated electronic records, such content will not fall under these exclusions and may be treated as unlawful SGI / false record.

(c) Use of tools only for accessibility/clarity/translation/searchability (without manipulating material part): Use of computer resources solely for improving accessibility, clarity, quality, translation, description, searchability, or discoverability shall not be treated as SGI, provided the process does not generate/alter/manipulate any material part of the underlying content.

Examples (not SGI): (for clarity)

- adding subtitles/closed captions to videos;
- translation of a speech/video into another language (where underlying meaning is not manipulated);
- auto-generated summaries/tags for improving search/discoverability;
- audio description for visually impaired users;
- improving clarity by reducing echo/distortion.

In summary, not every AI-assisted creation/editing qualifies as SGI. Content is treated as SGI only when it is artificially/algorithmically created or altered in a way that it appears real/authentic/true and is likely to be indistinguishable from a real person or real-world event. Routine, good-faith edits and accessibility/document preparation improvements are expressly excluded under Rule 2(1)(wa).

7. Will these amended rules affect lawful creative uses of synthetic media (e.g., satire, art, accessibility tools)?

Ans: The amendments recognise routine, good-faith editing, illustrative/educational content and accessibility improvements as exclusions to the definition of synthetic content where such activity does not materially alter substance or create false documents/records. Lawful uses such as labelled satire or creative synthetic works that do not violate law including Rule 3(3)(a)(i) of the IT Rules, 2021 (as amended) may be permitted so long as synthetic content is appropriately declared/labelled and does not contravene provisions of any law.

8. Do the amendments apply to text (written) information or only images/audio/video?

Ans: The 2026 amendments primarily focus on synthetically generated information (SGI) as defined under **Rule 2(1)(wa)** of the IT Rules, 2021 (as amended). This definition is specifically limited to "audio, visual or audio-visual information" (i.e., content such as images, videos and audio), which is artificially or algorithmically created/generated/modified/altered using a computer resource and made to appear real/authentic/true in a manner likely to be perceived as indistinguishable from a natural person or real-world event.

Accordingly:

- Pure text / written outputs, by themselves, are not SGI under Rule 2(1)(wa), since SGI is limited to audio/visual/audiovisual information.
- However, the amendments also insert **Rule 2(1A)** clarifying that, for specific provisions of the Rules, any reference to **"information"** used to commit an unlawful act shall include **SGI**. This ensures that unlawful acts involving synthetic audio/visual/audiovisual content are clearly covered, even where such SGI is accompanied by text (caption, description, message, post, etc.).

Further, intermediaries' general due diligence obligations under Rules 3 and 4 of the IT Rules, 2021 (as amended) relating to unlawful information (including content that violates applicable law) continue to apply irrespective of whether the content is in text form, visual form, or a combination.

Examples (for clarity):

- **Example 1 (SGI covered):** A deepfake video of a person saying something never said, posted with a misleading text caption like "breaking news".
  The video is SGI (audio-visual synthetic). The accompanying text does not change the fact that it is SGI.
- **Example 2 (SGI covered):** A cloned voice call recording (audio) falsely portraying a senior officer issuing illegal instructions, shared with a text transcript.
  Audio is SGI; transcript/text is supporting context.
- **Example 3 (text-only not SGI):** A chatbot-generated article spreading false rumours, without any synthetic audio/video/image.
  This is not SGI, but may still be "unlawful information" depending on the context/law violated.
- **Example 4 (mixed content):** An AI-generated fake photograph of a riot, circulated with text "This happened today in X city".
  The image is SGI and is covered; the text supports deception.

In summary, the SGI-specific framework introduced in the amendments is aimed at synthetic audio/visual/audiovisual content (deepfakes etc.). Text-only AI outputs are not SGI, but intermediaries' general obligations regarding unlawful information continue to apply, and SGI may also be used along with text to commit unlawful acts.

9. Do the Rules clarify how "information" should be interpreted in relation to SGI?

Ans: Yes. A clarification has been inserted that references to "information" in contexts of unlawful acts (including Rule 3(1)(b) and 3(1)(d), and Rule 4(2) and 4(4)) shall include SGI unless context otherwise requires.

10. If an intermediary removes/blocks SGI, does it risk losing exemption provided under section 79 of the IT Act?

Ans: The Rules clarify that removal or disabling of access to any information including SGI by an intermediary in compliance with the Rules (including via reasonable technical measures such as automated tools) shall **not** amount to a violation of the conditions under section 79(2)(a) or 79(2)(b) of the IT Act.

Section III: Due Diligence and User Obligations (Rule 3 Amendments)

11. What are the major changes in Rule 3(1)(c) (periodic user information)?

Ans: Under the amended **Rule 3(1)(c)** of the IT Rules, 2021 (as amended), intermediaries are required to inform users **at least once every three months (instead of erstwhile requirement of at least once every year)**, in a simple and effective manner, about important obligations and consequences relating to their use of the intermediary's platform/services.

The periodic user information includes, *inter alia*:

- the intermediary's right to terminate or suspend user access, or remove information / disable access to information, or both, for non-compliance with the Rules/terms;
- user liability for unlawful acts and for violating applicable law;
- where applicable, the intermediary's obligation to report information/violations involving offences that are mandatorily reportable under law.

Example (for clarity):

A platform must periodically display/send an advisory (every 3 months) stating that any unlawful information including deepfake/NCII/CSAM content is prohibited; violations may lead to removal/disablement of access and account suspension/termination; and certain offences may be reported to authorities.

12. Are there special user warnings required for intermediaries that facilitate SGI creation?

Ans: Yes. The amendments through introduction of new **Rule 3(1)(ca)** of the IT Rules, 2021 (as amended) provides for an additional user information (warning) requirement for intermediaries that offer a computer resource which enables or facilitates creation/ generation/ modification/ alteration/ sharing of synthetically generated information (SGI).

Such intermediaries must inform/warn users that violations relating to unlawful SGI may attract penalties/punishment under the IT Act and other applicable laws.

This warning under Rule 3(1)(ca) read with Rule 3(1)(c) should be issued in a simple and effective manner, and should be prominently communicated (including at onboarding and periodically).

Examples (for clarity):

- an AI image generation platform must show a warning such as: "Do not create deepfakes, impersonation content or non-consensual intimate imagery. Violations may result in removal/disablement of access, account action and legal consequences."
- a voice cloning tool must warn users that misuse for deception/impersonation may attract legal action.

13. What actions may be taken against users who violate synthetically generated information (SGI)-related obligations?

Ans: Where a user creates, uploads, publishes, transmits, shares or disseminates unlawful synthetically generated information (SGI) or otherwise violates the Rules/terms, the intermediary is required to take expeditious and appropriate action as per Rule 3(1)(cb) of the IT Rules, 2021 (as amended), read with Rule 3(1)(ca).

Such action may include, *inter alia*:

- **immediate removal of, or disabling access to**, such SGI/information;
- **suspension or termination** of the user account responsible for the violation (including prevention of further uploads), **while preserving evidence (E.g., logs and relevant information) and ensuring that evidence is not vitiated**, for purposes of investigation/legal proceedings; and
- where required under applicable law, **identification and disclosure** of information relating to the violating user to the complainant / competent authority, as applicable, in accordance with due process and legal requirements.

Example (for clarity):
If a user uploads an AI-generated morphed intimate image (NCII), the intermediary must **disable access/remove** such content immediately, **suspend/terminate** the user account (without vitiating evidence e.g., **preserve upload logs, etc.)**, and undertake reporting/assistance actions wherever the offence is mandatorily reportable or otherwise required under law.

14. What is the new timeline for removal/disablement upon "actual knowledge" under Rule 3(1)(d)?

Ans: Under the amended **Rule 3(1)(d)** of the IT Rules, 2021 (as amended), where an intermediary receives actual knowledge, either through a court order or a reasoned intimation from an authorised officer in the Appropriate Government or its authorised agency (in the manner prescribed), the intermediary must remove or disable access to the specified unlawful information **within 3 hours** of receipt of such order/notice. Please note that this timeline has been reduced from **36 hours to 3 hours** from receipt of such actual knowledge.

Example:

If an intermediary receives a reasoned intimation from an authorised officer in the Appropriate Government or its authorised agency at 11:00 AM to disable access to a deceptive SGI video, the intermediary must comply by 2:00 PM at the latest.

15. Are there changes in the authorised officer requirements for government intimation under Rule 3(1)(d)(ii)? Are there changes in officer authorisation requirements where the reasoned intimation under Rule 3(1)(d)(ii) is issued by police administration?

Ans: Yes. The amended provision under Rule 3(1)(d)(ii) of the IT Rules, 2021 (as amended), requires that the reasoned intimation must be issued by an officer authorised **by order in writing** for issuing such intimation.

The amendments also clarify that where the **reasoned intimation** under **Rule 3(1)(d)(ii)** is to be issued by the **police administration**, **there may be one or more authorised officers**, **each not below the rank of Deputy Inspector General of Police (DIG)**, who are **especially authorised by the Appropriate Government** in this behalf.

This is intended to ensure that such reasoned intimations for **removal of or disabling access to information** are issued only by duly authorised senior-level officers within the police administration, in accordance with the amended proviso to Rule 3(1)(d)(ii), thereby strengthening procedural clarity and accountability while retaining the requirement of reasoned intimation.

The change from providing for "one authorised officer" to "one or more authorised officers" (each not below the rank of DIG and especially authorised by the Appropriate Government) is intended to ensure **continuous, timely and effective issuance of reasoned intimations**, particularly in view of the **increased scale, speed and severity of harms** arising from unlawful online content, including synthetically generated information (SGI) such as deepfakes.

Given that such harmful content can spread virally within minutes and cause irreversible damage (e.g., reputational harm, extortion, non-consensual intimate imagery, public order issues, misinformation and fraud), reliance on a single authorised officer could lead to operational delays due to unavailability or workload constraints. Allowing more than one specifically authorised senior-level officer (not below the rank of DIG) ensures 24×7 readiness, avoids bottlenecks, and supports the stricter compliance timelines under Rule 3(1)(d), while retaining safeguards through rank and special authorisation.

Section IV: Grievance Redressal Timelines (Rule 3(2) Amendments)

16. What are the revised timelines in grievance redressal under Rule 3(2)(a)(i)?

Ans: Under amended **Rule 3(2)(a)(i)** of the IT Rules, 2021 (as amended), intermediaries must resolve grievances received from users **within 7 days** from the date of receipt of the grievance.

This timeline was earlier 15 days and has been reduced to ensure faster grievance resolution.

Example:

If a user submits a grievance about unlawful SGI content, the intermediary must take action and dispose of the grievance within 7 days (subject to faster timelines where applicable under proviso to Rule 3(2)(a)(i)).

17. What is the revised special timeline for grievances related to requests for removal/disablement of access?

Ans: The proviso to **Rule 3(2)(a)(i)** of the IT Rules, 2021 (as amended) provides a special expedited timeline. Under the amendments, the earlier **72-hour timeline has been reduced to 36 hours**, for certain grievances relating to requests for **removal of or disabling access to information** connected with Rule 3(1)(b).

Example:

If a grievance relates to deceptive or impersonation content falling under Rule 3(1)(b) that requires urgent action, the intermediary must take an appropriate decision and ensure removal/disablement of access within 36 hours.

18. What is the revised timeline for removing content against receipt of complaint relating to nudity/sexual act/impersonation etc. under Rule 3(2)(b)?

Ans: Under amended **Rule 3(2)(b)**, intermediaries are required to remove or disable access (as the case may be) to specified categories of content against receipt of complaint (including content relating to nudity/sexual content/morphed content/impersonation etc., as enumerated in the Rule) **within 2 hours** of receipt of a complaint. Please note that this timeline has been reduced from the **earlier 24-hours timeline to 2 hours** to enable rapid victim protection.

Example:

If an individual or any person on his behalf complains that an unlawful morphed intimate image is circulating, the intermediary must disable access to the content within 2 hours of receiving the complaint.

Section V: New Due Diligence for SGI (New Rule 3(3))

19. What is the new Rule 3(3) introduced in the IT Rules, 2021?

Ans: The amendments insert a new **Rule 3(3)** titled **"Due diligence in relation to synthetically generated information"**, which constitutes the **core operative due diligence framework** for addressing synthetically generated information (SGI).

Rule 3(3) prescribes specific due diligence obligations to be complied with by intermediaries in respect of SGI, including:

- deployment of technical measures to **prevent unlawful SGI**;
- explicit prohibition of certain **high-risk SGI categories**;
- **mandatory labelling and provenance embedding** for SGI which is not prohibited; and
- safeguards to prevent **tampering/removal** of such labels/metadata/identifiers.

20. Which intermediaries are covered under Rule 3(3)?

Ans: Rule 3(3) of the IT Rules, 2021 (as amended) applies where an intermediary offers a computer resource enabling or facilitating the creation, generation, modification, alteration, publication, transmission, sharing or dissemination of SGI.

This includes, *inter alia*, intermediaries offering (but not limited to):

- AI image/video generation or editing tools;
- voice synthesis / voice cloning tools;
- platforms/tools enabling manipulation of audio, visual or audio-visual information into realistic synthetic media; and
- platforms/services that facilitate publication or dissemination of SGI.

Example:

An intermediary offering a tool that can generate realistic AI videos or cloned voice notes is covered under Rule 3(3).

21. What categories of unlawful SGI must be prevented under Rule 3(3)(a)(i)? Please elaborate with some examples.

Ans: Under **Rule 3(3)(a)(i)** of the IT Rules, 2021 (as amended), intermediaries covered under Rule 3(3) must deploy reasonable and appropriate technical measures, including automated tools or other suitable mechanisms, to not allow users to create/ generate/ modify /alter / publish /transmit /share /disseminate SGI that violates any law for the time being in force.

In particular, the Rule expressly requires prevention of high-risk unlawful SGI, including SGI that comprises, *inter alia*:

- **child sexual exploitative and abuse material (CSEAM)**, **non-consensual intimate imagery (NCII)**, or **obscene/pornographic/ paedophilic/ sexually explicit content**, including content invasive of bodily privacy;

- SGI resulting in creation/generation/modification/alteration of any **false document** or **false electronic record**;
- SGI relating to preparation/development/procurement of **explosive material, arms or ammunition**; and
- SGI that falsely depicts/portrays a **natural person** or a **real-world event** by misrepresentation likely to deceive, including misrepresentation of **identity, voice, conduct, action or statement**, or the event itself.

Examples of unlawful/prohibited SGI that must be prevented under Rule 3(3)(a)(i) include, *inter alia*:

(A) CSEAM / sexually explicit content / content invasive of bodily privacy

- AI-generated or AI-altered image/video that depicts a child in sexually explicit manner (CSEAM).
- AI-generated sexually explicit deepfake content depicting any identifiable person without consent.
- AI-generated synthetic imagery/video intended to violate bodily privacy (e.g., synthetic "undressing" content or morphed nudity involving a real person).

(B) Non-consensual intimate imagery (NCII)

- AI-generated intimate photo/video of a person created using their real photographs (face swap/morphing), circulated without consent.
- Voice-cloned audio of a person used to fabricate "sexual conversation" clips for harassment/extortion.

(C) False documents / false electronic records

- AI-generated forged government identity documents (e.g., PAN/Aadhaar/passport-like document templates) presented as genuine.
- AI-generated appointment letters, service certificates, marksheets, salary slips or bank statements created in a manner that appears authentic.
- AI-generated fake emails/letters/records purportedly issued by ministries / PSUs /courts /authorities.

(D) Explosives / arms / ammunition related SGI

- AI-generated instructional video (made to appear like a real tutorial) showing steps/materials to prepare explosive substances.
- AI-generated realistic diagrams/video guidance for assembling firearms or procuring ammunition unlawfully.

(E) Deceptive impersonation / false depiction of person or event

- AI-generated video showing an election candidate making inflammatory remarks that were never made, circulated as genuine.

- A deepfake video/audio falsely showing a celebrity endorsing a product/service or investment scheme, presented as genuine in order to mislead users.
- Synthetic "interview footage" showing an actor/sportsperson making controversial remarks that were never made, circulated in a manner likely to deceive viewers.
- A deepfake video showing a celebrity engaging in unlawful/immoral conduct (that did not occur), circulated as real content causing reputational harm.
- Deepfake video of a senior government functionary/CEO giving false instructions (e.g., directing transfer of funds, issuing orders, approving contracts).
- Voice cloning of a family member or senior officer used to demand money urgently ("emergency scam call") in a manner likely to deceive.
- A deepfake video showing an ordinary individual (e.g., a teacher, student, private employee) making inflammatory/objectionable statements which they never made, circulated as genuine.
- An AI-generated audio clip cloning the voice of an individual and falsely portraying them as confessing to wrongdoing or making threats, with intent to deceive or harass.
- A synthetic video showing a person participating in an incident (e.g., assault, misconduct, vandalism) that never occurred, created to defame or intimidate the individual.
- Synthetic "news footage" showing riots, attack, stampede, or accident that never occurred, presented as real.

(F) Combined multi-modal deception (SGI + text)

- Synthetic video/audio made to appear real, paired with misleading text captions such as "official statement", "leaked recording", etc., to create deception and mislead users.

22. What are the labelling requirements for permitted SGI under Rule 3(3)(a)(ii)?

Ans: Under **Rule 3(3)(a)(ii)** of the IT Rules, 2021 (as amended), where SGI is **not covered under the prohibited categories under Rule 3(3)(a)(i)**, the intermediary must ensure that such SGI is:

- **clearly and prominently labelled** / displayed with a label or notice identifying it as SGI;
    - for visual/audiovisual content: label must ensure **prominent visibility** in the visual display;
    - for audio content: there must be a **prominently prefixed audio disclosure**; and
- embedded with **permanent metadata or technical provenance mechanisms**, to the extent technically feasible, including a **unique identifier**, to enable identification of such information as SGI and identification of the computer resource used to create/modify/alter it.

Example (for clarity):

(i) A lawful SGI/AI-generated video not covered under the prohibited categories under Rule 3(3)(a)(i) should carry a visible "synthetically generated" notice and include embedded permanent metadata / provenance mechanism, including a unique identifier, to enable identification of the audio as SGI and the computer resource used to generate/alter it.

(ii) A lawful SGI AI-generated audio message (e.g., a synthetic voice narration for an awareness campaign or an audio announcement generated using text-to-speech), not covered under the prohibited categories under Rule 3(3)(a)(i), should include a prominently prefixed audio disclosure such as "This audio is synthetically generated" at the beginning, and should also carry embedded permanent metadata / provenance mechanism, including a unique identifier, to enable identification of the audio as SGI and the computer resource used to generate/alter it.

23. Can the SGI label/metadata/unique identifier be modified, suppressed, or removed?

Ans: No. Under the anti-tampering safeguard in **Rule 3(3)(b)** of the IT Rules, 2021 (as amended), an intermediary must **not enable** the modification, suppression or removal of

- the SGI label and
- permanent metadata/provenance mechanisms and unique identifiers embedded for SGI identification.

This ensures SGI transparency and traceability and prevents circumvention of labelling/provenance obligations.

Example:
The intermediary should not offer "remove watermark", "export without metadata", or similar functionalities that undermine SGI identification.

Section VI: Additional Due Diligence for Significant Social Media Intermediaries (SSMIs) (Rule 4 Amendments)

24. What is new Rule 4(1A) related to SGI?

Ans: The amendments introduce new **Rule 4(1A)** introducing **enhanced *ex-ante* obligations** for **Significant Social Media Intermediaries (SSMIs)** in relation to SGI.

Rule 4(1A) requires an SSMI, **before allowing users to display, upload or publish information**, to:

- obtain a **user declaration** as to whether the content is SGI;
- deploy **reasonable and appropriate technical measures** (including automated tools) to **verify the correctness** of such declaration prior to publication, having regard to the nature/format/source of information; and
- where confirmed as SGI (by declaration and/or technical verification), ensure it is displayed with a **clear and prominent label/notice** indicating that the content is synthetically generated.

Example:
Before publication, an SSMI may require the uploader to declare "AI-generated: Yes/No", verify using metadata/detection signals, and apply a prominent label if confirmed SGI.

25. What happens if SSMI knowingly permits or promotes SGI in contravention of Rules?

Ans: The proviso to newly introduced **Rule 4(1A)** clarifies that where an SSMI **knowingly permits, promotes or fails to act upon** SGI in contravention of the Rules, it shall be **deemed to have failed to exercise due diligence** under the IT Rules, 2021. This strengthens platform accountability of SSMI in relation to unlawful SGI.

26. Does Rule 4(1A) change responsibility of SSMIs vis-à-vis verification, that is under Rule 4(1A), do SSMIs have to verify whether uploaded content is SGI, or is user declaration sufficient?

Ans: Yes. Rule 4(1A) makes verification obligations explicit. SSMIs are required to deploy **reasonable and appropriate technical measures** to verify user declarations regarding SGI **prior to publication**, rather than relying only on user self-declaration.

This ensures stronger prevention of deception, impersonation and misuse of deepfakes on large platforms.

27. What change has been made in Rule 4(4) regarding technology-based measures?

Ans: The amendments strengthen and harmonise the earlier existing **Rule 4(4)** with the SGI-related obligations introduced through new **Rule 4(1A)**. The revised framework:

- moves away from an **"endeavour"-based** formulation; and
- provides for a clearer, mandatory and proportionate obligation for SSMIs to deploy **reasonable and appropriate technical measures**, including automated tools or other suitable mechanisms, to ensure effective due diligence.

In effect, Rule 4(4) is aligned with the overall approach of strengthened technological due diligence in relation to unlawful content, including SGI.

Section VII: Practical Illustrations (Reference)

28. Can you give examples of content that qualifies as SGI?

Ans: Yes. SGI as per the definition under Rule 2(1)(wa) of the IT Rules, 2021 (as amended) refers to audio, visual or audio-visual information which is artificially or algorithmically created/generated/modified/altered using a computer resource, in a manner that it **appears real/authentic/true** and depicts/portrays any individual or event in a manner that is, or is likely to be perceived as **indistinguishable from a natural person or a real-world event, but with some exceptions as indicated thereunder**.

Examples of SGI (generic scenarios):

- an AI-generated realistic video clip of a person (virtual human) speaking in a manner that appears to be a real person speaking on camera;
- synthetic voice (text-to-speech / voice cloning) that reproduces a natural person's voice with realistic intonation and tone;
- synthetic/AI-generated reconstruction of an event (e.g., simulated disaster scene, accident scene, crowd incident) that is made to appear as real footage;
- AI-generated realistic image of a person participating in an event, despite the event/person depiction being artificially created or altered.

Examples of *unlawful/prohibited SGI* (covered under Rule 3(3)(a)(i)):

- **Deceptive impersonation SGI:** deepfake video/audio showing a public figure or any natural person making statements/actions which were never made/done, with the intent/effect of deception;
- **Sexual / NCII SGI:** AI-generated non-consensual intimate imagery / sexually explicit deepfake content depicting a person;
- **False document / false electronic record SGI:** synthetic generation/modification of documents or records (e.g., fabricated ID cards, certificates, official letters, electronic records) resulting in false documents/false electronic records;
- **Explosives/arms related SGI:** synthetic content providing or enabling preparation/procurement of explosive material, arms or ammunition;
- **False event depiction SGI:** fabricated but realistic recording depicting a real-world event as having occurred (e.g., riots, attacks, election violence, bribe-taking incident), when it did not occur, in a manner likely to deceive users.

29. Can you give examples of content that does not qualify as SGI?

Ans: Yes. As per the proviso to the definition of SGI under Rule 2(1)(wa) of the IT Rules, 2021 (as amended) that provides for specific exclusions of certain categories information from the definition of SGI, an audio/visual/audio-visual information shall **not** be deemed to be SGI where it arises from routine or good-faith actions that do **not materially alter, distort or misrepresent** the underlying content, or from routine good-faith creation of documents/materials (without generating false documents/records), or from use of computer resources solely for improving accessibility/translation/searchability without manipulating any material part of the underlying content.

Examples include:

- cropping, compression, noise reduction, transcription, brightness/contrast correction, or other routine good-faith edits which do not materially alter or misrepresent the underlying content;
- blur/masking of faces/vehicle number plates or other sensitive parts for privacy protection, without depicting a false identity or false event;

- translation/subtitles/closed captioning/audio descriptions to improve accessibility or clarity, without generating or manipulating any material part of the underlying audio/visual information;
- preparation of educational/ training/ research/ presentation materials using illustrative/ hypothetical/ template-based or conceptual content, where such preparation does not result in the creation of any false document or false electronic record.

Section VIII: Summary Table of Key Timelines (as amended)

30. What are the important timelines under the amended Rules?

Ans:

- **Rule 3(1)(d):** information removal/disablement upon actual knowledge received through (i) by an order of a court of competent jurisdiction; or (ii) a reasoned intimation from the authorised officer of the Appropriate Government or its agency - **within 3 hours**
- **Rule 3(2)(a)(i):** grievance disposal - **within 7 days**
- **Proviso to Rule 3(2)(a)(i):** certain grievances for removal or disabling access to information or communication link relating to rule 3(1)(b)- **within 36 hours**
- **Rule 3(2)(b):** removal or disabling access to information relating to nudity/sexual act/impersonation/morphed content against grievances - **within 2 hours**

*****