ANNEXURE-I

Draft of proposed amendments in Part-I and Part-II of the IT Rules, 2021

Black Text – existing Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
Blue Text – Modification proposed

PART I

…..

2. Definitions. — (1) In these rules, unless the context otherwise requires-

……

(l) "Grievance Appellate Committee" means an appellate committee constituted to deal with appeals by users against the decision of the Grievance Officer;

……

PART II
DUE DILIGENCE BY INTERMEDIARIES AND GRIEVANCE REDRESSAL MECHANISM

3. (1) **Due diligence by an intermediary:** An intermediary, including social media intermediary and significant social media intermediary, shall observe the following due diligence while discharging its duties, namely:—

(a) the intermediary shall prominently publish on its website, mobile based application or both, as the case may be, the rules and regulations, privacy policy and user agreement for access or usage of its computer resource by any person and ensure compliance of the same.;

(b) the intermediary shall inform the rules and regulations, privacy policy or user agreement of the intermediary to the user and shall cause the user of its computer resource not to host, display, upload, modify, publish, transmit, store, update or share any information that,—

(i) belongs to another person and to which the user does not have any right;
(ii) is defamatory, obscene, pornographic, paedophilic, invasive of another's privacy, including bodily privacy, insulting or harassing on the basis of gender, libellous, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or otherwise inconsistent with or contrary to the laws in force;
(iii) is harmful to child;

(iv) infringes any patent, trademark, copyright or other proprietary rights;
(v) violates any law for the time being in force;
(vi) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact;
(vii) impersonates another person;
(viii) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting other nation;
(ix) contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;
(x) is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person;

(c) an intermediary shall periodically inform its users, at least once every year, that in case of non-compliance with rules and regulations, privacy policy or user agreement for access or usage of the computer resource of such intermediary, it has the right to terminate the access or usage rights of the users to the computer resource immediately or remove non-compliant information or both, as the case may be;

(d) an intermediary, on whose computer resource the information is stored, hosted or published, upon receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its agency under clause *(b)* of sub-section *(3)* of section 79 of the Act, shall not host, store or publish any unlawful information, which is prohibited under any law for the time being in force in relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force:

Provided that any notification made by the Appropriate Government or its agency in relation to any information which is prohibited under any law for the time being in force shall be issued by an authorised agency, as may be notified by the Appropriate Government:

Provided further that if any such information is hosted, stored or published, the intermediary shall remove or disable access to that

information, as early as possible, but in no case later than thirty-six hours from the receipt of the court order or on being notified by the Appropriate Government or its agency, as the case may be:

Provided also that the removal or disabling of access to any information, data or communication link within the categories of information specified under this clause, under clause (b) on a voluntary basis, or on the basis of grievances received under sub-rule (2) by such intermediary, shall not amount to a violation of the conditions of clauses (a) or (b) of sub-section (2) of section 79 of the Act;

(e) the temporary or transient or intermediate storage of information automatically by an intermediary in a computer resource within its control as an intrinsic feature of that computer resource, involving no exercise of any human, automated or algorithmic editorial control for onward transmission or communication to another computer resource shall not amount to hosting, storing or publishing any information referred to under clause *(d)*;

(f) the intermediary shall periodically, and at least once in a year, inform its users of its rules and regulations, privacy policy or user agreement or any change in the rules and regulations, privacy policy or user agreement, as the case may be;

(g) where upon receiving actual knowledge under clause (d), on a voluntary basis on violation of clause (b), or on the basis of grievances received under sub-rule (2), any information has been removed or access to which has been disabled, the intermediary shall, without vitiating the evidence in any manner, preserve such information and associated records for one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by Government agencies who are lawfully authorised;

(h) where an intermediary collects information from a user for registration on the computer resource, it shall retain his information for a period of one hundred and eighty days after any cancellation or withdrawal of his registration, as the case may be;

(i) the intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011;

(j) the intermediary shall, as soon as possible, but not later than seventy two hours of the receipt of an order, provide information under its control or possession, or assistance to the Government agency which is lawfully

authorised for investigative or protective or cyber security activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force, or for cyber security incidents:

Provided that any such order shall be in writing stating clearly the purpose of seeking information or assistance, as the case may be;

(k) the intermediary shall not knowingly deploy or install or modify technical configuration of computer resource or become party to any act that may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform thereby circumventing any law for the time being in force:

Provided that the intermediary may develop, produce, distribute or employ technological means for the purpose of performing the acts of securing the computer resource and information contained therein;

(l) the intermediary shall report cyber security incidents and share related information with the Indian Computer Emergency Response Team in accordance with the policies and procedures as mentioned in the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013;

(m) the intermediary shall take all reasonable measures to ensure accessibility of its services to users along with reasonable expectation of due diligence, privacy and transparency;

(n) the intermediary shall respect the rights accorded to the citizens under the Constitution of India.

(2) **Grievance redressal mechanism of intermediary:** (a) The intermediary shall prominently publish on its website, mobile based application or both, as the case may be, the name of the Grievance Officer and his contact details as well as mechanism by which a user or a victim may make complaint against violation of the provisions of this rule or any other matters pertaining to the computer resources made available by it, and the Grievance Officer shall –

(i) acknowledge the complaint, including suspension, removal or blocking of any user or user account or any complaint from its users in the nature of request for removal of information or communication link relating to sub-clauses (i) to (x) of the clause (b) under sub-rule (1) of rule 3, within twenty-four hours and dispose of such complaint within a period of fifteen days from the date of its receipt;

Provided that the complaint in the nature of request for removal of information or communication link relating to sub-clauses (i) to (x) of the clause (b) under sub-rule (1) of rule 3, shall be acted upon expeditiously and redressed within 72 hours of reporting:

Provided further that appropriate safeguards may be developed by the intermediary to avoid any misuse by users.

(ii) receive and acknowledge any order, notice or direction issued by the Appropriate Government, any competent authority or a court of competent jurisdiction.

(b) The intermediary shall, within twenty-four hours from the receipt of a complaint made by an individual or any person on his behalf under this sub-rule, in relation to any content which is *prima facie* in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual, take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it:

(c) The intermediary shall implement a mechanism for the receipt of complaints under clause (b) of this sub-rule which may enable the individual or person to provide details, as may be necessary, in relation to such content or communication link.

(3) **Appeal to Grievance Appellate Committee(s)**: – (a) The Central Government shall constitute one or more Grievance Appellate Committees, which shall consist of a Chairperson and such other Members, as the Central Government may, by notification in the Official Gazette, appoint;[1]

(b) Any person aggrieved by an order made by the Grievance Officer under clause (a) and clause (b) of sub-rule (2) of rule 3 may prefer an appeal to the Grievance Appellate Committee having jurisdiction in the matter within a period of 30 days of receipt of communication from the Grievance Officer;

[1] The Grievance Appellate Committee is set up to provide an alternative to a user to file an appeal against the decision of the Grievance Officer rather than directly going to the court of law. Hence, the user can appeal to the said Committee in case of his dissatisfaction with the order of the Grievance Officer and seek an alternative redressal mechanism. However, the user has the right to seek judicial remedy at any time.

(c) The Grievance Appellate Committee shall deal with such appeal expeditiously and shall make an endeavour to dispose of the appeal finally within 30 calendar days from the date of receipt of the appeal;

(d) Every order passed by the Grievance Appellate Committee shall be complied with by the concerned Intermediary.

4. Additional due diligence to be observed by significant social media intermediary.—(1) In addition to the due diligence observed under rule 3, a significant social media intermediary shall, within three months from the date of notification of the threshold under clause (v) of sub-rule (1) of rule 2, observe the following additional due diligence while discharging its duties, namely:—

(a) appoint a Chief Compliance Officer who shall be responsible for ensuring compliance with the Act and rules made thereunder and shall be liable in any proceedings relating to any relevant third-party information, data or communication link made available or hosted by that intermediary where he fails to ensure that such intermediary observes due diligence while discharging its duties under the Act and rules made thereunder:

Provided that no liability under the Act or rules made thereunder may be imposed on such significant social media intermediary without being given an opportunity of being heard.

Explanation.—For the purposes of this clause "*Chief Compliance Officer*" means a key managerial personnel or such other senior employee of a significant social media intermediary who is resident in India;

(b) appoint a nodal contact person for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders or requisitions made in accordance with the provisions of law or rules made thereunder.

Explanation.—For the purposes of this clause "*nodal contact person*" means the employee of a significant social media intermediary, other than the Chief Compliance Officer, who is resident in India;

(c) appoint a Resident Grievance Officer, who shall, subject to clause (b), be responsible for the functions referred to in sub-rule (2) of rule 3.

Explanation.—For the purposes of this clause, "*Resident Grievance Officer*" means the employee of a significant social media intermediary, who is resident in India;

(d) publish periodic compliance report every month mentioning the details of complaints received and action taken thereon, and the number of specific communication links or parts of information that the intermediary has removed or disabled access to in pursuance of any proactive monitoring conducted by using automated tools or any other relevant information as may be specified;

(2) A significant social media intermediary providing services primarily in the nature of messaging shall enable the identification of the first originator of the information on its computer resource as may be required by a judicial order passed by a court of competent jurisdiction or an order passed under section 69 by the Competent Authority as per the Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009, which shall be supported with a copy of such information in electronic form:

Provided that an order shall only be passed for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or of incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for a term of not less than five years:

Provided further that no order shall be passed in cases where other less intrusive means are effective in identifying the originator of the information:

Provided also that in complying with an order for identification of the first originator, no significant social media intermediary shall be required to disclose the contents of any electronic message, any other information related to the first originator, or any information related to its other users:

Provided also that where the first originator of any information on the computer resource of an intermediary is located outside the territory of India, the first originator of that information within the territory of India shall be deemed to be the first originator of the information for the purpose of this clause.

(3) A significant social media intermediary that provides any service with respect to an information or transmits that information on behalf of another person on its computer resource–

(a) for direct financial benefit in a manner that increases its visibility or prominence, or targets the receiver of that information; or

(b) to which it owns a copyright, or has an exclusive license, or in relation with which it has entered into any contract that directly or indirectly restricts the publication or transmission of that information through any means other than those provided through the computer resource of such social media intermediary,

shall make that information clearly identifiable to its users as being advertised, marketed, sponsored, owned, or exclusively controlled, as the case may be, or shall make it identifiable as such in an appropriate manner.

(4) A significant social media intermediary shall endeavour to deploy technology-based measures, including automated tools or other mechanisms to proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit, or any information which is exactly identical in content to information that has previously been removed or access to which has been disabled on the computer resource of such intermediary under clause (d) of sub-rule (1) of rule 3, and shall display a notice to any user attempting to access such information stating that such information has been identified by the intermediary under the categories referred to in this sub-rule:

Provided that the measures taken by the intermediary under this sub-rule shall be proportionate having regard to the interests of free speech and expression, privacy of users on the computer resource of such intermediary, including interests protected through the appropriate use of technical measures:

Provided further that such intermediary shall implement mechanisms for appropriate human oversight of measures deployed under this sub-rule, including a periodic review of any automated tools deployed by such intermediary:

Provided also that the review of automated tools under this sub-rule shall evaluate the automated tools having regard to the accuracy and fairness of such tools, the propensity of bias and discrimination in such tools and the impact on privacy and security of such tools.

(5) The significant social media intermediary shall have a physical contact address in India published on its website, mobile based application or both, as the case may be, for the purposes of receiving the communication addressed to it.

(6) The significant social media intermediary shall implement an appropriate mechanism for the receipt of complaints under sub-rule (2) of rule 3 and grievances in relation to the violation of provisions under this rule, which shall enable the complainant to track the status of such complaint or grievance by providing a unique ticket number for every complaint or grievance received by such intermediary:

Provided that such intermediary shall, to the extent reasonable, provide such complainant with reasons for any action taken or not taken by such intermediary in pursuance of the complaint or grievance received by it.

(7) The significant social media intermediary shall enable users who register for their services from India, or use their services in India, to voluntarily verify their accounts by using any appropriate mechanism, including the active Indian mobile number of such users, and where any user voluntarily verifies their account,

such user shall be provided with a demonstrable and visible mark of verification, which shall be visible to all users of the service:

Provided that the information received for the purpose of verification under this sub-rule shall not be used for any other purpose, unless the user expressly consents to such use.

(8) Where a significant social media intermediary removes or disables access to any information, data or communication link, under clause (b) of sub-rule (1) of rule 3 on its own accord, such intermediary shall,—

(a) ensure that prior to the time at which such intermediary removes or disables access, it has provided the user who has created, uploaded, shared, disseminated, or modified information, data or communication link using its services with a notification explaining the action being taken and the grounds or reasons for such action;

(b) ensure that the user who has created, uploaded, shared, disseminated, or modified information using its services is provided with an adequate and reasonable opportunity to dispute the action being taken by such intermediary and request for the reinstatement of access to such information, data or communication link, which may be decided by the Resident Grievance Officer ~~within a period of fifteen days~~/ as per sub-rule (2) of rule 3;

(c) ensure that the Resident Grievance Officer of such intermediary maintains appropriate oversight over the mechanism for resolution of any disputes raised by the user under clause (b).

(9) The Ministry may call for such additional information from any significant social media intermediary as it may consider necessary for the purposes of this part.

5. Additional due diligence to be observed by an intermediary in relation to news and current affairs content.—In addition to adherence to rules 3 and 4, as may be applicable, an intermediary shall publish, on an appropriate place on its website, mobile based application or both, as the case may be, a clear and concise statement informing publishers of news and current affairs content that in addition to the common terms of service for all users, such publishers shall furnish the details of their user accounts on the services of such intermediary to the Ministry as may be required under rule 18:

Provided that an intermediary may provide such publishers who have provided information under rule 18 with a demonstrable and visible mark of verification as being publishers, which shall be visible to all users of the service.

Explanation**.** —This rule relates only to news and current affairs content and shall be administered by the Ministry of Information and Broadcasting.

6. Notification of other intermediary.—(1)The Ministry may by order, for reasons to be recorded in writing, require any intermediary, which is not a significant social media intermediary, to comply with all or any of the obligations mentioned under rule 4, if the services of that intermediary permits the publication or transmission of information in a manner that may create a material risk of harm to the sovereignty and integrity of India, security of the State, friendly relations with foreign States or public order.

(2) The assessment of material risk of harm referred to in sub-rule (1) shall be made having regard to the nature of services of such intermediary, and if those services permit,—

(a) interaction between users, notwithstanding, whether it is the primary purpose of that intermediary; and

(b) the publication or transmission of information to a significant number of other users as would be likely to result in widespread dissemination of such information.

(3) An order under this rule may be issued in relation to a specific part of the computer resources of any website, mobile based application or both, as the case may be, if such specific part is in the nature of an intermediary:

Provided that where such order is issued, an entity may be required to comply with all or any of the obligations mentions under rule 4, in relation to the specific part of its computer resource which is in the nature of an intermediary.

7. Non-observance of Rules.—Where an intermediary fails to observe with these rules, the provisions of sub-section (1) of section 79 of the Act shall not be applicable to such intermediary and the intermediary shall be liable for punishment under any law for the time being in force including the provisions of the Act and the Indian Penal Code: