INFORMATION AND COMMUNICATION TECHNOLOGIES AUTHORITY

9th Floor, The Celicourt, Sir Celicourt Antelme Street, Port Louis, MAURITIUS

Ref. ICTA/TD/2/2025 24 March 2025

THE TELECOMMUNICATION DIRECTIVE 2 OF 2025

The Information and Communication Technologies Authority, in the discharge of its statutory functions under the Information and Communication Technologies Act 2001 (the Act), hereby issues the following directive, pursuant to section 17(3) of the Act regarding the deployment of a decentralised Child Sexual Abuse (CSA) Filtering system

1. Short title

These directives may be cited as the Telecommunication Directive 2 of 2025 (TD 2 of 2025).

2. Application of directives

These directives shall apply to holders of Internet Services Licence offering services to the general public, namely Cellplus Mobile Communications Ltd, Mauritius Telecom, Emtel Ltd and Mahanagar Telephone (Mauritius) Ltd.

3. Explanatory Note

3.1. The ICT Authority in the exercise of its statutory functions under the ICT Act issues the following Directive pursuant to section 18 (1) (m) combined with Section 32 (5) (a), (b) of the ICT Act and Sections 14 and 21 of the Internet Service Provider (ISP) licence conditions.

3.2. This Directive sets out obligations on Licensed ISPs with a view to curtailing access to online child sexual abuse (CSA) materials for Internet users from the Republic of Mauritius.

3.3. Under section 18 (1) (m) of the ICT Act, one of the functions of the ICT Authority is mandated to "take steps to regulate or curtail harmful and illegal content on Internet and other information and communication services".

3.4. Equipped with the above legal mandate, since February 2011, the ICT Authority has set up a centralised online content filtering service that enables Internet service providers in Mauritius to filter out online CSA contents, which are considered as illegal in Mauritius.

3.5. However, as online CSA contents can be hosted at IP (Internet Protocol) addresses that also host other non-CSA content, it has been noted that with the deployment of this centralised filtering set up, traffic to a non-CSA website may also travel through the centralised filtering up. If or when this occurs, it can cause an end user's IP address to incorrectly appear to be from an unexpected location.

4. Obligations of Licensed ISPs

4.1. In order to solve the issue in section 3.5 above, the proposed solution is to move away from the centralised configuration to an on-premises filtering set up configuration within each ISP's local network. This new filtering setup configuration will have the added benefit of mitigating the risk of a single point of failure of the CSA filtering system.

4.2. This on-premises filtering set up is to be deployed by each ISP's within its local network in conformity with the Data Protection Act, consisting of the necessary non-intrusive (no deep packet inspection) technical filtering infrastructure required to block access to online CSA contents for Internet users from the Republic of Mauritius to cater for the following scenarios:

4.2.1. For https traffic, blocking is to be done only at the website level considering the fact that a non-intrusive filtering solution will be able to block only at the web domain level and acknowledging the fact that in some cases, even at the domain level, blocking will not be possible.

4.3. Furthermore, the CSA filtering set up to be deployed by each licensed ISP will need to make use of the Project Arachnid blacklist (https://www.projectarachnid.ca/en/). Each ISP will need to make an online request for an Application Programming Interface (API)key

(https://www.projectarachnid.ca/en/contact/) to get access to the Arachnid blacklist which is free of charge.

4.4. Each ISP will need to submit to the ICT Authority a monthly statistics in terms of the following:

4.4.1. Number of attempts (hits) to access CSA websites by Mauritian Internet users irrespective of whether the number of hits is for the same CSA website and same user IP address;
4.4.2. Number of Mauritian IP addresses to which access to CSA websites was blocked;
4.4.3. Number of CSA domains being blocked.

4.5. Each ISP shall submit to the ICT Authority, by the end of each calendar year, an IT Security Audit Report on the functioning of the of CSA filtering system. The audit exercise shall be conducted by an external certified IT Auditor, detailing out:

4.5.1. Filtering technology used
4.5.2. Agreement in use with the CSA blacklist providers
4.5.3. How the data requested in section 4.4 above is being retrieved and compiled.

4.6. The ICT Authority may, at any time, request an IT Security Audit to be conducted outside of the annual cycle. This may be required in response to any security concerns, incidents, or following major changes to the CSA system, including but not limited to significant upgrades, modifications, or integrations with new technologies.

4.7. The CSA filtering set up of each ISP should become operational at latest on 1 May 2025.