Govt notifies telecom cyber security rules; sets timelines for telcos to report security incidents

The rules also empower the central government/ its authorised agency to seek traffic data and any other data (other than the content of messages) from a telecom entity for the purpose of ensuring cyber security

Updated - November 22, 2024 07:02 pm IST - New Delhi

PTI

The government has notified the telecom cyber security rules, that aim to safeguard India's communication networks. File | Photo Credit: The Hindu

The government has notified the telecom cyber security rules, that aim to safeguard India's communication networks and services, through a host of measures including specified timelines for telcos to report security incidents and make disclosures.

The rules also empower the central government/ its authorised agency to seek traffic data and any other data (other than the content of messages) from a telecom entity for the purpose of ensuring cyber security.

Also Read: **Centre to train 5,000 cybercommandos in next five years: Shah**

Telecom entities would also be required to adopt telecom cyber security policy, that would include security safeguards, risk management approaches, actions, training, network testing, and risk assessment.

"The central government, or any agency authorised by the central government, may, for the purposes of protecting and ensuring telecom cyber security, seek from a telecommunication entity, traffic data and any other data, other than the content of messages, in the form and manner as may be specified by the central government on the portal; and direct a telecommunication entity to establish necessary infrastructure and equipment for collection and provision of such data from designated points to enable its processing and storage," according to the rules framed under the new Telecom Act.

The government and any agency authorised by it to collect data under these rules, as well as persons with whom such data is shared, will place adequate safeguards to ensure that such data is stored and maintained in strict confidentiality and prevent any unauthorised access, it said.

The rules clearly outline telecom cyber security obligations.

"...no person shall endanger telecom cyber security by misuse of telecommunication equipment or telecommunication identifier or telecommunication network or telecommunication services or by fraud, cheating or personation; transmitting any message which is fraudulent; committing or intending to commit any security incident; engaging in any other use which is contrary to the provision, of any other law for the time being in force; or any other means which may have security risk on telecom cyber security," according to the rules," it said.

Under the rules, every telecom entity will be required to implement specified measures to ensure cyber security, including adopting a telecom cyber security policy (security safeguards, risk management approaches, actions, training, best practices and technologies, to enhance telecom cyber security).

The policy, it said, should also encompass telecom network testing including hardening, vulnerability assessment and risk assessment, identification and prevention of security incidents among other aspects.

The policy should entail a rapid action system to deal with security incidents including mitigation measures to limit the impact of such incidents, and forensic analysis of security incidents to ensure learnings from such incidents and further strengthening telecom cyber security.

Telecom entities would be required to appoint a Chief Telecommunication Security Officer, and report security incidents within six hours to the Centre along with "relevant details of the affected system including the description of such incident."

In 24 hours of becoming aware of the security incident, telecom entities would be required to furnish information on a number of users affected, duration, geographical area, the extent to which the functioning of the network or service is affected; and the remedial measures taken or proposed to be taken.

As per the rules, a manufacturer of equipment that has an International Mobile Equipment Identity (IMEI) number, will register the number of such equipment manufactured in India with the government, before the first sale of such equipment.

A telecommunication entity has been defined as any person providing telecommunication services, or establishing, operating, maintaining, or expanding a telecommunication network, including an authorised entity holding an authorisation.

Published – November 22, 2024 05:49 pm IST