New Telecom Cyber Security Rules in India

Published by: https://www.gktoday.in/ebooks/ | © 2025 GKToday | All Rights Reserved

The Government of India has implemented new telecom cyber security regulations, aimed to enhance the protection of communication networks and services. Telecom companies are now required to report security incidents to the government. They must also share specific data for cybersecurity purposes.

Reporting Security Incidents

Telecom companies must report any security incidents within six hours. Reports should include details about the affected systems. Within 24 hours, they must provide information on the number of users impacted and the geographic area affected.

Companies must share traffic data and other relevant information, which excludes message content. The government can request this data to boost cyber security efforts.

Cyber Security Policies

Each telecom entity must adopt a comprehensive cyber security policy. This policy should encompass security measures, risk management, and incident response strategies. Training and network testing are also essential components.

A Chief Telecommunication Security Officer must be appointed by each telecom company. This officer will oversee the implementation of security measures and compliance with regulations.

Infrastructure for Data Management

Telecom entities may be required to establish infrastructure for collecting and processing data. This infrastructure must ensure the secure storage of information. Adequate safeguards are necessary to protect data from unauthorised access.

Prohibited Activities

The rules explicitly prohibit actions that could undermine telecom security. Misuse of telecom equipment and fraudulent activities are strictly banned. Companies must implement measures to prevent security incidents and assess risks regularly.

Equipment Registration

Manufacturers of telecom equipment must register International Mobile Equipment Identity (IMEI) numbers with the government. This registration is mandatory before selling equipment in India.

Telecom entities encompass all organisations providing services or managing telecom networks. This includes those with proper authorisation from the government.

Important Facts for Exams:

1. **Chief Telecommunication Security Officer (CTSO):** The CTSO oversees cyber security measures in telecom companies. They ensure compliance with regulations and manage security incidents effectively to protect communication networks.
2. **International Mobile Equipment Identity (IMEI):** IMEI is a unique identifier for mobile devices. Manufacturers must register IMEI numbers with the government before selling equipment, enhancing tracking and security in telecommunications.

3. **Telecom Cyber Security Policy:** This policy includes risk management, incident response, and security measures. It is mandatory for telecom entities to adopt such policies to enhance network protection against vulnerabilities.
4. **Data Sharing Requirements:** Telecom companies must share traffic data with the government. This excludes message content, ensuring that sensitive information remains private while enhancing overall cyber security efforts.