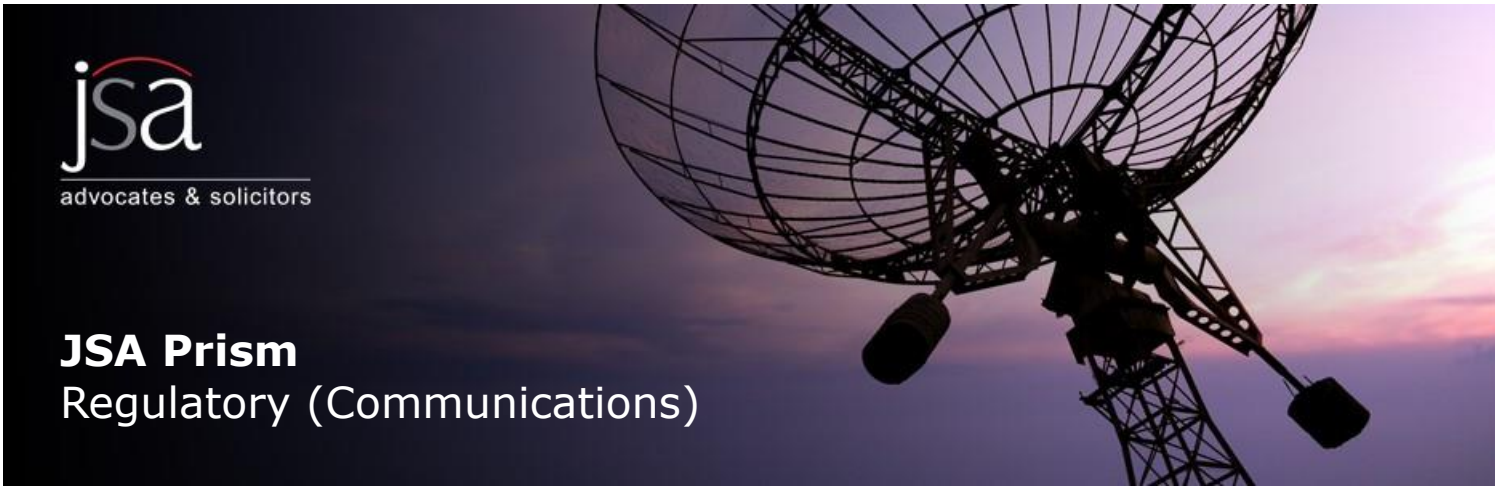

April 2022

MeitY issues directions relating to Cybersecurity

The Ministry of Electronics and Information Technology ("**MeitY**") released directions relating to information security practices, procedures, prevention, response and reporting of cyber incidents for safe and trusted internet on April 28, 2022 ("**Directions**"). The Directions will become effective after 60 days from its date of issue.

The Directions have been issued in light of the various instances of cyber security incidents that have been reported from time to time and to coordinate response activities as well as emergency measures to handle such cyber security incidents. Further, it has been issued to strengthen cyber security in India to protect the sovereignty and integrity of India, defence of India, security of the state, friendly relations with foreign states or public order and to prevent incitement to the commission of any cognizable offence using computer resource.

The key highlights of the Directions are as follows:

1. All service providers are required to ensure the synchronisation of all their information and communications technology ("**ICT**") systems clocks by connecting to the Network Time Protocol ("**NTP**") Server of National Informatics Centre ("**NIC**") or National Physical Laboratory ("**NPL**") or with NTP servers traceable to these NTP servers.
2. If the service providers have ICT system across different geographies, then accurate and standard time source other than NPL and NIC is to be used while ensuring that their time source does not deviate from NPL and NIC.
3. All service providers, intermediaries, data centers, body corporates and government organisations are mandated to:
    a) report relevant cyber security incidents to Indian computer emergency response team ("**CERT-In**") within 6 hours of noticing such incidents.
    b) take action or provide information or any such assistance to CERT-In when required by order/direction of CERT-In, for the purposes of cyber incident response, protective and preventive actions related to cyber incidents.
    c) designate a point of contact to interface with CERT-In and the information relating to the point of contact is to be sent to CERT-In and is to be updated from time to time.
    d) enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days and the same is to be maintained within the Indian jurisdiction.
4. Data centres, virtual private server providers, cloud service providers and virtual private network service providers are required to register certain information including validated names of subscribers/customers hiring the services; period of hire including dates; IPs allotted to / being used by the members; email address and IP address and time stamp used at the time of registration / on-boarding; validated address and contact numbers

etc. This information is to be maintained for a period of five years or longer as mandated by the law, after any cancellation or withdrawal of the registration.

5. The virtual asset service providers, virtual asset exchange providers and custodian wallet providers are to mandatorily maintain all information obtained as part of Know Your Customer (KYC) and records of financial transactions for a period of five years so as to ensure cyber security in the area of payments and financial markets for citizens while protecting their data, fundamental rights and economic freedom in view of the growth of virtual assets.

For more details, please contact km@jsalaw.com

Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi

