

Demystifying IT Rules 2011: What it means for you

The Government of India's recent notification of the Information Technology (IT) Rules 2011, under the aegis of the Information Technology Act 2000 (IT Act), has far-reaching implications for organizations and service providers as well as for end users. Consequent to the [amendment to the IT Act \(ITAA 2008\)](#), organizations began to consider ISO 27001 audits to conform to tightening IT security norms in the country. Now, the notifications under IT Rules 2011 appear to be more comprehensive, stringent, and in some aspects, possibly even stifling.

Although the true effectiveness of the IT rules and the constraints or benefits accruing to end users remain to be seen, it is certain that the new stipulations will pose a challenge to organizations in terms of costs of operation, compliance and implementation. "It is too early to predict the impact, and just how seriously the government is looking to implement these rules," says Gowree Gokhale, partner at Nishith Desai Associates.

According to Vicky Shah, author and founder of legal consultancy Eagle Eye, "The IT Act is applicable to every industry and domain, and the new IT rules are extremely exhaustive." For the first time, legal definitions of concepts such as 'blog', 'blogger', 'user' and 'cyber security incidents' have been included in the IT Rules 2011. Here's a more detailed look at some of the stipulations and implications of the IT Rules 2011.

Intermediary rules and liabilities

The IT Rules 2011 stipulate that due diligence be observed by intermediaries, which will absolve them of liability in case of legal action. Website owners are now required to appoint grievance officers, translating into added overheads and increased manpower requirements for monitoring user-generated content. Objectionable content must be removed from the website within 36 hours of a complaint being registered, to be absolved of liability. As a result, websites will be compelled to monitor user-generated content to maintain due diligence.

It is now mandatory for service providers to frame terms of service based on best practices recommended by the government under the IT Rules 2011. This is more of a one-size-fits-all measure, even though different services have different requirements and liabilities accruing to those requirements.

As with previous editions, the definition of what constitutes objectionable content is broad, and could be subjectively and/or arbitrarily interpreted under the IT Rules 2011. Lack of clarity is likely to suppress expression for fear of prosecution. Several experts contend that laws stifling freedom of speech guaranteed by the Constitution of India are invalid.

Reasonable security and sensitive information

For the first time under Indian law, sensitive personal data and information have been explicitly and exhaustively defined, including details from passwords up to sexual orientation and bio-metric data. IT Rules 2011 also specifies that any information available in the public domain not be regarded as sensitive personal data.

Under the IT Rules 2011, there are two separate definitions of personal information — sensitive personal information; and, personal information that is more general in nature. Gokhale believes that this can pose an interpretation problem. "Applicability of the IT Rules 2011 to personal information or sensitive personal information is currently a gray area, as to what is appropriate where," she says.

Organizations must now have a privacy policy, and need to obtain written consent through letter, fax or e-mail from the provider of sensitive information. Entities are required to "reasonably ensure" that users are aware that information is being collected, its purpose, intended recipients and particulars of the collecting agency. Disclosure of sensitive personal data will require prior permission from the information provider, unless it's necessary for compliance and legal obligations. An entity is considered to have complied with reasonable security, if they have implemented a documented information security program that is commensurate with international standards such as ISO, depending upon the business' nature.

IT Rules 2011 notifications

1. [IT \(Intermediaries guidelines\) Rules, 2011](#), (under sections 87 and 79(2))
2. [IT \(Reasonable Security Practices and Sensitive Personal Data\) Rules, 2011](#), (under sections 87 and 43A)
3. [IT \(Electronic Service Delivery\) Rules, 2011](#), (under sections 87 and 6A(2))
4. [IT \(Guidelines for Cyber-cafe\) Rules, 2011](#), (under sections 87 and 79(2))

More on the IT (Amendment) Act, 2008

- [Information Technology Amendment Act 2008 \(IT Act 2008\)](#)
- [IT \(Amendment\) Act 2008 and its effect on the Indian enterprise](#)
- [IT Amendment Act 2008 compliance guidelines for India.org](#)
- [Has IT Amendment Act 2008 created a new audit domain?](#)

Guidelines for cyber-cafes

IT Rules 2011 has introduced government-approved licensing agencies for cyber-cafes. The IT rules have further elaborated on identification of users, and minors will now have to be accompanied by adults. Cyber-cafes must securely maintain user identification records for a period of one year, in addition to maintaining photographs to establish identity. A log register of session details must be maintained for one year, with monthly reports submitted to the registration agency. Backups of history records for each computer must be maintained for a year.

Reasonable preventive measures to disallow users from tampering with computer settings must be incorporated. An officer designated by the registering authority is authorized to inspect a cyber-cafe at any time.

Rules for delivery of electronic services

Electronic service providers must now maintain transaction records up to five years under the IT Rules 2011. This move translates to a direct increase in costs with regards to maintaining these records in the prescribed format. "While organizations were earlier required to maintain logs and records, there was no stipulated time frame. The IT Rules 2011 remedies that oversight," says Shah.

India has a user base of over 100 million users. Just how the government proposes to implement these IT Rules 2011 is anybody's guess. Shah expects the country's IT security scenario to change for the better. While these rules are intended to safeguard the end user and curb cyber-crime, its effectiveness might require several rounds of modifications, before this becomes a reality.

All Rights Reserved, [Copyright 2009 - 2011](#), TechTarget | [Read our Privacy Statement](#)