

DATA SECURITY COUNCIL OF INDIA

A Self Regulatory initiative in Data Security and Privacy Protection

1. Background

The phenomenon of globalization has led to creation of innovative business models and provided unprecedented benefits for the global economy. The Indian IT and ITeS/BPO sector had played a pivotal role in this irreversible trend and contributed to the national economy in no small measure. However, the unbundling of business processes has also brought in its wake some unforeseen challenges in the area of data security and privacy.

The Indian ITeS and BPO industry, which started with the advantage of low-cost human resources, has now moved on to add quality and diversity as its differentiators. With companies maturing and successfully coping with the issue of scaling up and expanding, will now need to tackle the problem of offering consistent data security to the customers at an affordable cost. The security landscape is constantly evolving, as the threats, consumer perceptions and legislative and regulatory strategies keep changing. These are the challenges that will need to be met with effective responses.

The Indian ITES/BPO companies are striving hard to ensure the security of data and privacy protection. They are following the stringent security controls specified by their customers through contracts. However, many a times, the problem can not be contained by an individual company, irrespective of the cost incurred, and requires industry-level solutions. Successful security solutions require a convergence of the three components, viz. technology, people and processes. Further, a single instance of information security breach can tarnish the entire industry's image and the country's reputation as a safe destination for data. Smaller companies lack dedicated resources for handling security and need cost-effective approaches for demonstrative security levels. There is an urgent need to provide a protected environment for data and privacy for IT and ITeS sector in India, through the establishment of rules and standards that promote ethics, quality and best practices.

NASSCOM has been proactive in pushing this cause for ensuring that the Indian Information Security environment benchmarks with the best across the globe. As a part of its Trusted Sourcing initiative, NASSCOM is in the process of setting up the Data Security Council of India (DSCI) as a Self Regulatory Organization (SRO) to establish, popularize, monitor and enforce privacy and data protection standards for India's ITeS-BPO industry.

2. Guiding Principles

DSCI is envisaged as a credible and committed body to uphold a high level of data privacy and security standards. DSCI shall be based on the following five guiding principles:

1. Self-Regulation: The structure and operating procedures of DSCI rely primarily upon self-regulation. Industry, rather than a governmental body, is best positioned to develop appropriate data privacy and security standards based upon its greater knowledge and understanding with the practical commercial issues involved. A self regulatory approach will allow DSCI to evolve and respond more effectively to developments in overseas and domestic markets.
2. Adoption of best global practices: DSCI shall adopt the best global practices, drawing upon U.S. laws, the European Union Directive and Safe Harbor Framework, OECD guidelines, and Asia Pacific Economic Cooperation (APEC) Framework in designing the Code of conduct, which in turn, will continue to evolve with time and experience.
3. Independent Oversight:

The composition of governing body of DSCI shall be balanced with adequate representation of independent directors and industry specialists.

4. Focused Mission:

Initial focus of DSCI shall be its core mission of establishing itself with significant membership with focus on evolving the Code of Conduct and promoting a culture of privacy and security through education and outreach.

5. Enforcement Mechanism:

DSCI shall promote and encourage voluntary compliance of the code, but, in due course, will seek to create a mechanism for enforcement of the code to enhance its credibility among a variety of stakeholders.

3. Structure

DSCI shall be a not-for-profit organization, registered under section 25 of the Companies Act. It would have a diversified membership associated with Data Security and Privacy Protection. This could include: companies in information technology (IT) and IT enabled services (ITeS) sector, companies other than in IT/ITeS sector, Academic or research Institutions and universities. DSCI will thus seek to develop a diverse membership, unified in its pursuit of its objectives. Activities of DSCI members could be in the fields of provision of IT/ITES services, consultancy, research and development and manufacturing. Irrespective of the field of specialization, all DSCI members will be expected to share and support the objectives of DSCI and to operate in a manner consistent therewith.

DSCI shall be headed by a Board of Directors with balanced representation from industry and independent individuals. In the technical aspects, it will be guided by a Steering Committee, which will have experts from the various domains of security.

4. Mission

The key objectives of DSCI will be:

- To enable Indian IT/ITeS organizations to provide high standard of security and data protection by adopting the best practices.
- To develop, monitor and enforce an appropriate security and data protection standard for the Indian IT/ITES industry that would be adequate, cost effective, adaptable and comparable with the global standards
- To build capacity to provide security certification for organizations.
- To create a common platform for promoting sharing of knowledge about information security and foster a community of security professionals and firms.
- To create awareness among industry professionals and other stakeholders about security and privacy issues.

5. Activities

DSCI shall function as an enabler to the IT and ITeS industry to grow at a rapid pace by facilitating the adoption and enforcement of the prescribed security standards and best practices. It plans to undertake the following activities.

1. Awareness through Security Forums: Creation and functioning of Security Forums throughout the country for creating awareness among the involved entities and individuals about the importance and measures for data protection.
2. GAP analysis: Analyzing the existing standards and best practices adopted by the industry in India and industry at the international level.

3. Devising standards and best practices: Consolidating, devising and enforcing ethical standards and best practices in line with international standards for creating a secured environment for data in India that would be cost effective and easily adoptable.
4. Research: Carrying out research in the field of data privacy and protection in the context of Indian situation.
5. Conferences: Organizing national and regional conferences on data security issues.
6. Certification: Certifying the companies who adopt the standard proposed by DSCI.

Keeping in view the broad objectives, DSCI, as a Self Regulatory Organization, would be a credible and committed body for upholding an effective data privacy and security standard in India, thereby enabling member companies with competitive edge to sustain their rate of rapid growth.