Best Practices: Indian Information Act (Amendment) 2008/2011

Author: Rohit Kr. Sharma | CISM # 1322171 | ISO 27001 L.A | ISO 22301 L.A

Abstract:

The Information Technology (Amendment) Bill, 2008 (Bill No.96-F of 2008) was passed by the both houses of parliament on December, 2008 and received the accent of the president on 5th February, 2009 and became operational as the Information Technology (Amendment) Act, 2008 (ITAA, 2008) notified with effect from 27/10/2009 and is now become operational. Many significant changes have been introduced in the IT Amendment Act, 2008. Post this there were two more amendments were issues in 2011, a) The Intermediary responsibility and b) Cyber Café Guidelines as Amendments in ITAA (amendments) 2011.

Introduction:

With the enforcement of ITAA (amendment) 2008, Govt. Of India has shown its concern and focus on protection of the SPDI (Sensitive and Personal Data Information), Cyber terrorism, Cyber Crime, electronic transactions, identity theft, Child pornography and digital signatures; and moreover the Information technology (Intermediaries Guidelines) Rules, 2011 have introduced the concept of cyber law due diligence in India which naturally, cyber due diligence for Indian companies, cyber due diligence for PayPal and online payment transferors in India, cyber due diligence for foreign websites in India, etc. have now been officially introduced in India.

Thus, it has become essential and even to some extend mandatory for the Corporates, Private, Public and Govt organizations to be complaint with ITAA-2008 and 2011 amendments and non-compliance to the IT Acts may cause heavy penalty , imprisonment and in some serious non-compliances, both Penalty and imprisonment are provisioned.

This Document prepares in with the intention to aware the management who drives implement and maintain Information Security and Compliance within an enterprise or Organization to implement and stay complaint to the ITAA 2008 & 2011 amendments requirements presented in a shape of checklist.

Author: Rohit Kr. Sharma | CISM # 1322171| ISO 27001 L.A | ISO 22301 L.A

Keywords: ITAA 2008 Amendments, ITAA 2011 Amendments, Protection of Sensitive and Personal Data Information (SPDI), Indian Cyber Law.

Definitions:

Intermediary means "Intermediary" under Section 2(1) (w). It reads as – "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, webhosting service providers, search engines, online payment sites, online-auction sites, online-market places, social media, blog webistes and cyber cafes

"**Indian Computer Emergency Response Team**" means the Indian Computer Emergency Response Team appointed under sub section(1) of Section 70(B) of the The Indian Information Technology Act.

Author: Rohit Kr. Sharma | CISM # 1322171| ISO 27001 L.A | ISO 22301 L.A

Best Practices - ITAA 2008 & 2011 amendments requirements.			
Area	**Section/Rule/Sub Rule**	**Requirement**	**Penalties Imprisonment /Fine/Both**
Sensitive Personal Data or Information (SPDI)	Sec 43 A Sec 43/ Rule 3	An Organization shall be aware of the privacy role based on its functions, activities & business. An Organization Provides services to its end customers (individuals – 'providers of information' under the ITAA 2008) under a direct relationship shall inform the means and purpose of data collection and its processing to its customers. The organization deal (collect, process, store, transfer, access) with for "sensitive personal data or information" (SPDI) as defined under sec43A of the ITAA, 2008 shall identified functions, operations and activities that deal with SPDI.	Negligence in implementing and maintaining reasonable Security practices and procedures and causes wrongful loss or wrongful gain to any person , such body corporate shall be liable to pay damages by the way of compensation , not exceeding Five crore rupees**. (Covers up overall Section 43 and also to some extend Section 79 as both Section 43 and Section 79 are more or less similar in liabilities of Organization or body corporates and Intermediaries or Service providers respectively).**
Privacy Policy	Sec 43 /Rule 4	The organization shall have a privacy policy and shall also meet following parameters: a) Shall be published on the website of the organization? b) Shall be easily accessible? c) Shall be simple & easy to understand d) Shall provide links to organization's practices and policies e) Shall state Type of SPDI being collected f) Shall provide Reason for collecting such information g) The intended usage of the provided information h) Disclosure policy and practices of the organization.	

		i). Shall have Reasonable security practices and procedures adopted by the organization for securing SPDI
	Sec 79 /Rule 3/ Sub Rule (1)	The intermediary shall publish the rules and regulations, privacy policy and user agreement for access-or usage of the intermediary's computer resource by any person.
	Sec 79 /Rule 3/ Sub Rule (1)	The Intermediary shall inform its users that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the Intermediary has the right to immediately terminate the access or usage lights of the users to the computer resource of Intermediary and remove non-compliant information.
	Sec 79 /Rule 3/ Sub Rule (2)	The Intermediary shall ensure that its published/ Provided rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that :- (a) belongs to another person and to which the user does not have any right to; (b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, pedophilic, libelous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever; (c) harm minors in any way; (d) infringes any patent, trademark, copyright or other proprietary rights; (e) violates any law for the time being in force; (f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature; (g) impersonate another person; (h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource; (i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation .

Collection Limitation	Sec 43/ Rule 5/ 2(a)	The organization shall follow any due diligence to ensure SPDI is collected for a lawful purpose which is associated with the function or activity of the organization.
Due Diligence	Sec 43/Rule 5/ 2(b)	The organization shall follow any due diligence to ensure SPDI which is necessary for the above purpose is only collected.
Informing the Providers of Information	Sec 43/ Rule 5 / 3	The Organization shall ensure that when directly collecting SPDI from the provider of information, the organization shall take reasonable steps to ensure that the provider of information is having knowledge of following: i. the fact that the SPDI is being collected ii. the purpose for which SPDI is collected iii. the intended recipients of SPDI iv. the name & address of the agency which is collecting the SPDI v. the agency that will retain the SPDI
Consent	Rule 5(1) and Clarification Issued u/s 43A	The organization shall take written consent from the provider of information regarding purpose of usage before collecting their SPDI:
Modes for Obtaining Consent		a. Letter b. Fax c. Email d. Click in an online environment e. Instant messaging f. IVR g. Any other mode of electronic communication
Choice	Sec 43/ Rule 5 /Sub rule (7)	The organization shall provide an option to the provider of information to decline providing data or information sought to be collected for availing service.
Consent Withdrawal		The organization shall also provide option to the provider of information to withdraw his / her consent given earlier.

Purpose Limitation	Sec 43/Rule 5 / Sub Rule (5)	The organization shall perform any due diligence to ensure that the usage of SPDI is consistent with the purpose for which has been collected.
Access & Correction Mechanisms	Sec 43/Rule 5/ Sub Rule (6)	The organization shall allow providers of information, as & when requested by them, the facility to review the SPDI they have provided. The organization shall have mechanisms in place that allow providers of information to modify / update / correct their SPDI, if found to be outdated and / or incorrect.
Information Retention	Sec 43/ Rule 5 / Sub Rule (4)	The organization shall ensure that the SPDI is not retained for a period longer than required for its lawful use or is otherwise required by any other law for the time being in force.
Grievance Officer Publication on website Resolution	Sec 43/ Rule 5 / Sub Rule (9) & Sec 79 /Rule 3/ Sub Rule (11)	The organization shall designate a grievance officer to address any discrepancies & grievances raised by the providers of information. The organization published the name and contact details of the grievance officer on its website. The grievance officer mandated to redress the grievances of the providers of information within one month (maximum) from the date of the receipt of grievance.
Disclosure of Information Prior Permission Exceptions Publishing in Public Domain	Sec 43/ Rule 6/ Sub Rule (1) Sec 43/ Rule 6 / Sub Rule (3)	The contract shall be signed between the organization and providers of information mention the disclosure of SPDI to third parties. If not, The organization Shall take prior permission of the providers of information before disclosing their SPDI to third parties or publishing it. Any legal obligations shall be identified and documented under which the organization needs to disclose the SPDI without informing or taking permission of the providers of information. The organization shall take due diligence to ensure that the SPDI is not published intentionally or unintentionally in public domain, i.e., made available to unauthorized persons or public.

Controls	Sec 43/ Rule 6 / Sub Rule (4)	The organization shall put in place the mechanisms / controls to ensure that the third party with which SPDI is shared do not disclose it further.
Transfer of Information	Sec 43/ Rule 7	The organization shall follow due diligence to ensure that the same level of data protection is adhered to by third parties (which may be located in India or abroad) to whom the organization transfers SPDI for performance of a lawful contract between the organization and providers of information or where the providers of information have given their consent for such transfers.
	Sec 79 /Rule 3/ Sub Rule (3)	The intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in Section 79 /Rule3/ sub-rule (2).
Security Practices a. Agreement through contractual instruments	Sec 43A & Sec 79 /Rule 3/ Sub Rule (8)	The organization shall have implemented 'Reasonable Security Practices' for protecting SPDI. The contract signed between organization & provider of information or between organization & third party shall contains provisions that specify security practices and procedures designed to protect SPDI from unauthorized access, damage, use, modification, disclosure or impairment and shall also include following: i. Comprehensive documented information security policies & programs ii. Managerial, technical, operational & physical security controls that are commensurate with the value of information assets being protected and the risk exposure iii. Audit / assessment mechanisms for testing implementation of controls

b. In absence of any Contract	Sec 43/ Rule 8 Sub Rule (1 ,2 ,3)	The organization shall have implemented documented information security policies & programs that contain managerial, technical, operational & physical security controls that are commensurate with the value of information assets being protected and the risk exposure? Such security practices & procedures could be: a. IS/ISO/IEC 27001 b. Codes of best practices of an industry association (where the organization is a member) that are duly approved & notified by the central government	
	Sec 43/ Rule 8 Sub Rule (4)	The security practices & procedures shall get certified or audited by a government approved independent auditor, on a regular basis (at least once a year or as & when the organization undertakes significant up gradation of its processes & computer resources).	
c. Demonstration of Security Practices in case of security incident / data breach	Sec 43A	The organization shall maintain the requisite records, logs, trails, etc. for demonstrating compliance.	
	Sec 79 /Rule 3/ Sub Rule (4)	The intermediary, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes.	
Due Diligence over Internet and Email Services		If any Body corporate or Company maintains an Internet interface and allows its employees to access Internet and email. In such cases, it is necessary for the company shall have adequate access control , over Internet Access transmission and e-mail services as the organizations shall have obligations Section:	
	Sec 43	Damages to Computer systems through Hacking and Cracking	Up to 1 Crore INR
	Sec 65	Tempering with Computer Source documents	3 years/ 2 Lacks/ both

	Sec 66	Computer Related offences	3 years/ 5 lacks/ both
	Section 66A	Sending offensive messages through a computer or mobile phone ,	3 years with fine
	Sec 66B	Receiving stolen computer resource or communication device	3 years/ 1 lacks/ both
	Sec 66C	Identity theft	3 years with 1 Lac Fine
	Sec 66D	Cheating by personation using computer resource	
	Sec 66E	Publishing or transits the image/videotype of Private area of any person with his/her consent.	3 years/ 2 lacks/ both
	Sec 66F	Cyber Terrorism	Imprisonment for Life
	Sec 67	Publishing of obscene information in electronic form	3 years/5 lacks
	Sec 67A	Publishing or transmitting material in electronic form containing sexually explicit act	5 years/10 lacks
	Sec 67B	Child pornography	5 years/10 lacks
	Sec 79 /Rule 3/ Sub Rule (10)	The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to "perform thereby circumventing any law for the time being in force: --- Provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein.	
Preservation and Retention of information by intermediaries	67 C	Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.	3 years and fine
Power of interception of electronic communication to		Any Body Corporate, company or intermediary shall consider, adhere and follow the direction of Central Govt or State Govt or any of its authorized officer as prescribed under Section 69, 69A and 69 B .	7 Years and fine

the Government	Sec 69 & 69 A	Sections 69 and 69A of the amended Act empower the state to issue directions for interception, monitoring, decryption of any information through any computer resource; and for blocking websites in the interest of national security, and friendly relations with foreign states.	
	Sec 69 B	Section 69B empowers the government to authorize to monitor, collect traffic data or information through any computer resource for cyber security.	3 Years and fine
	Sec 79 /Rule 3/ Sub Rule (7)	When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing staling clearly the purpose of seeking such information or any such assistance.	
Disclosure of information in breach of lawful contract	72 A	Any Body Corporate, company or intermediary shall have adequate protection to the Data or Information which it accessed while providing services under a contract. Disclosure of such information with an intention to cause wrongful loss or wrongful gain or breach of contract without consent of person concerned may cause penalties as defined under Section 72 A .	3 years/1 lac / Both
Incident Reporting / Cyber Security Incident Handling	Sec 79 /Rule 3/ Sub Rule (9)	The intermediary shall report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team.	

References:

- THE INFORMATION TECHNOLOGY ACT, 2000
- THE INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008
- THE INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION) RULES, 2011.
- INFORMATION TECHNOLOGY (INTERMEDIARIES GUIDELINES) RULES, 2011
- SEC-43A-ITAA CHECKLIST, DATA SECURITY COUNCIL OF INDIA

Author: Rohit Kr. Sharma | CISM # 1322171| ISO 27001 L.A | ISO 22301 L.A