

# CYBER LAWS and GUIDELINES

By

Varun Kumar  
Deputy Director (T/F)  
National Power Training Institute

### Definition IT Act

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “electronic commerce”, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker’s Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

## Sec-2 of IT Act

(d) “affixing electronic signature”: adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.

(f) “asymmetric crypto system”: system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

(nb) “cyber security means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

(x) “key pair”, in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.

### Sec-3

(c) any alteration to the electronic signature made after affixing such signature is detectable.

(d) any alteration to the information made after its authentication by electronic signature is detectable.

Sec-4: Legal recognition of electronic records—Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference.

Sec-5 : Legal recognition of electronic signatures—Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.

## Notification of Forensic labs as 'Examiner of Electronic Evidence' under Section 79A of the Information Technology Act 2000

- ◆ Cyber Forensic Division, State Forensics Science Laboratory, Thiruvananthapuram, Kerala  1.28 MB
- ◆ Cyber Forensic Laboratory, Air Force Cyber Group, New Delhi  1.17 MB
- ◆ Notification of Cyber Forensic Lab, CERT-In as 'Examiner of Electronic Evidence' under section 79A of IT Act 2000  862.54 KB
- ◆ Notification of Regional Forensic Science laboratory, Northern Range, Dharamshala, Himanchal Pradesh as 'Examiner of Electronics Evidence' as per the provision of section 79 A of IT Act 2000  220.48 KB
- ◆ Cyber Forensic Laboratory, Army Cyber Group, DGMO, Signals Enclave, New Delhi  1.64 MB
- ◆ State Forensic Science Laboratory, Madiwala, Bangalore  1.62 MB
- ◆ Central Forensic Science Laboratory (CFSL), Hyderabad  1.65 MB
- ◆ Directorate of Forensic Science, Gandhi Nagar Gujarat  1.65 MB
- ◆ Computer Forensic and Data Mining Laboratory (CFDML), Serious Fraud Investigation Office (SFIO), Delhi  1.65 MB
- ◆ Notification of Forensic Science Laboratory Govt of NCT, Rohini New Delhi  1.67 MB

## NCIIPC (National Critical Information Infrastructure Protection Centre)

National Nodal Agency in respect of Critical Information Infrastructure Protection created under Sec 70A of the *Information Technology Act, 2000 (amended 2008)*.

Issue guidelines, advisories and vulnerability or audit notes etc. relating to protection of critical information infrastructure and practices, procedures, prevention and response in consultation with the stake holders, in close coordination with Indian Computer Emergency Response Team and other organisations working in the field or related fields.

Exchange cyber incidents and other information relating to attacks and vulnerabilities with Indian Computer Emergency Response Team and other concerned organisations in the field etc.

## NCIIPC has broadly identified the following as "Critical Sectors"

- Power & Energy
- Banking, Financial Services & Insurance
- Telecom
- Transport
- Government
- Strategic & Public Enterprises



## Role of CERT-In (Indian Computer Emergency Response Team)

National nodal agency for responding to computer security incidents as and when they occur.

As per *IT Amendment Act, 2008*, CERT-In has been designated to perform following functions

Collection, analysis and dissemination of information on cyber incidents.

Cyber incidents forecast and alerts.

Emergency measures for handling cyber incidents.

Issue guidelines, advisories, vulnerability notes and white papers on information security practices, procedures, prevention, response and reporting cyber incidents etc.

## Cyber Forensics (CERT-In)

Equipped with tools and equipment to carry out retrieval and analysis of data extracted from data storage devices using computer forensics and mobile device forensic techniques.

Facility for Digital Forensics data extraction and analysis is being utilized in investigation of cases of cyber security incidents, submitted by central and state government ministries, departments, public sector organizations, law enforcement agencies, etc.

Imparts training through workshops organized on computer forensics and mobile device forensics through lectures, demonstrations and hands on practical sessions, which covers seizing, preservation, imaging and analysis of the data retrieved from the digital data storage devices

Provides support to other training institutes in imparting training by delivering lectures with demonstrations on various aspects of cyber forensics.

## Power Sector – Information Sharing and Analysis Center (ISAC – Power)

### Six sectoral CERTs- MoP, GoI

S.No.	Sectoral CERT	Nodal Organization
1.	CERT – Thermal	NTPC
2.	CERT – Hydro	NHPC
3.	CERT – Transmission	POWERGRID
4.	CERT – Distribution	DP&T Division, CEA
5.	CERT – Grid Operation	NLDC
6.	CERT – Renewable Energy	MNRE/SECI

## **CEA (Cyber Security in Power Sector) Guidelines, 2021**

### **Objectives:**

- a) Creating cyber security awareness
- b) Creating a secure cyber ecosystem,
- c) Creating a cyber-assurance framework,
- d) Strengthening the regulatory framework,
- e) Creating mechanisms for security threat early warning, vulnerability management and response to security threats,
- f) Securing remote operations and services,
- g) Protection and resilience of critical information infrastructure,
- h) Reducing cyber supply chain risks,
- i) Encouraging use of open standards,
- j) Promotion of research and development in cyber security,
- k) Human resource development in the domain of Cyber Security,
- l) Developing effective public private partnerships,
- m) Information sharing and cooperation
- n) Operationalization of the National Cyber Security Policy

### **Responsible Entity:**

- a) Transmission Utilities as well as Transmission Licensees,
- b) Load despatch centres (State, Regional and National),
- c) Generation utilities (Hydro, Thermal, Nuclear, RE),
- d) Distribution Utilities
- e) Generation Aggregators,
- f) Trading Exchanges,
- g) Regional Power Committees, and
- h) Regulatory Commissions

<b>Chief Information Security Officer:</b> designated employee of Senior management level directly reporting to Managing Director/Chief Executive Officer/Secretary of the Responsible Entity, having knowledge of Information Security and related issues, responsible for cyber security efforts and initiatives including planning, developing, maintaining, reviewing and implementation of Information Security Policies.
<b>Appointment of CISO</b>
a) The Responsible Entity shall mandatorily appoint a CISO and shall confirm to qualification, if any, <b>laid</b> by Quality Council of India (QCI). In absence, the work of CISO shall be looked upon by Alternate CISO. In case qualification for appointment of Alternate CISO has been relaxed for reasons recorded thereof, Alternate CISO has to mandatorily acquire the minimum required cyber security skill sets within six months from the date of his appointment.
b) The Responsible Entity shall regularly update details of CISO and Alternate CISO, with the Sectoral CERT, as well as on ISAC-Power Portal.
c) Roles and Responsibility of CISOs shall be as laid by CERT-In and ring-fenced to ensure cyber security of the Cyber Assets of the Responsible Entity.

<b>Cyber Security Audit:</b>
a) The Responsible Entity shall implement Information Security Management System (ISMS) covering all its Critical Systems.
b) The Responsible Entity shall through a CERT-In Empanelled Cyber Security OT Auditor shall get their IT as well as OT System audited at least once in every 6 (six) months and shall close all critical and high vulnerabilities within a period of one month
and medium as well as low non-conformity before the next audit. Effective closure of all non-conformities shall be verified during the next audit.
c) The Cyber Security Audit shall be as per ISO/IEC 27001 along with sector specific standard ISO/IEC 27019, IS 16335 and other guidelines issued by appropriate Authority if any. These mentioned standards shall be current with all amendments if any and in case if any standard is superseded, the new standard shall be applicable. CISO shall ensure immediate closure of non-conformance, based on the criticality and by means all non-conformances are to be closed before the next audit.
d) The Responsible Entity shall ensure that CISO has all the required systems and documents in place, as mandated by NSCS for base line cyber security audit.



## References

[cert-in.org.in](http://cert-in.org.in)

[nciipc.gov.in](http://nciipc.gov.in)

[powermin.gov.in](http://powermin.gov.in)

[cea.nic.in](http://cea.nic.in)

[meity.gov.in](http://meity.gov.in)

[mha.gov.in](http://mha.gov.in) (NISPG)