Hello everyone! In this video, you will learn about Cyber Security policies recommended for any organization and various regulatory bodies in India and International.

An Information Security Policy (ISP) is a set of rules, policies, and procedures designed to ensure all end users and networks within an organization meet minimum IT security and data protection security requirements. It should address all data, programs, systems, facilities, infrastructure, authorized users, third parties, and fourth parties of an organization.

Let's discuss the importance of information security: -
Information security policies can have many benefits for an organization such as **It Facilitates data integrity, availability, and confidentiality for ensuring data security in an enterprise network, Protects sensitive data, Minimizes the risk of security incidents by defining best practices to follow, Executes security programs across the organization, Provides a clear security statement to third parties** to avoid any possible conflict and **Helps comply with regulatory requirements** to identify security gaps related to regulatory requirements and address them.

**Now Lets us learn about the elements of an information security policy-**
**The first element of a security policy is its Purpose** which may be to create an overall approach to information security for detecting any information security breaches

such as misuse of networks, data, applications, and computer systems, maintaining the reputation of the organization, and upholding ethical and legal responsibilities, etc.

**The second element of the policy is its audience or users** to whom the information security policy applies. You may also specify which audiences are out of the scope of the policy (for example, staff in another business unit that manages security separately may not be in the scope of the policy).

**Information security objective is the third element that** Guides your management team to agree on well-defined objectives for strategy and security. Information security focuses on three main objectives **Confidentiality, Integrity,** and **Availability.**

**The fourth element is Authority and access control policy** which deals with the matters like a hierarchical authority in an organization.

The fifth element is **Data classification which** classifies data into categories, which may include “top secret”, “secret”, “confidential”, and “public”. The r objective of classifying data is to protect highly important data, and avoid needless security measures for unimportant data.

**6th element is Data support and operations** to store personal data or other sensitive data which must be protected. Most security standards require, at a minimum, encryption, a firewall, and anti-malware protection. The data in transit and at rest must be protected.

**7th element is Security awareness and behavior** which emphasizes continuous training of employees and IT professionals.

**The last element is the Responsibilities, rights, and duties of personnel** to carry out user access reviews,

education, change management, incident management, implementation, and periodic updates of the security policy. Responsibilities should be clearly defined as part of the security policy.

Here are the prominent Regulatory Bodies that regulate Information Security Policies in India- These bodies are

- Cert In
- CRAT
- Reserve Bank of India Act
- IRDA
- DOT
- NIST
- DSCI

CertIn is the national nodal agency responsible for prompt responses to cybersecurity incidents. It started its official operations in January 2004. It acts as the primary task force responsible for:

- Alerts and forecasts preventing cybersecurity incidents
- Defining emergency measures to tackle and mitigate the effects of cyber risks
- Collection, analysis, and responsible dissemination of data on cyber threats
- Constant coordination of cyber response activities
- Issuing best practices, guidelines, and precautions in the public interest for better reporting and management of cyber incidents

Cyber Regulations Appellate Tribunal (CRAT) covered under the IT Act, 2000, is the chief governing body established by the Central Government based on the provisions of Section 48(1) of IT Act. The Central Government notifies all the relevant cybersecurity breaches to them, which fall under the jurisdiction of the Tribunal.
The power of the Tribunal is same as of the Civil Court covered under the Code of Civil Procedure, 1908 and includes,

- Enforcing and summoning the attendance of people to be examined under oath
- Ensuring that all related electronic records and documents are available
- Demanding evidence on affidavits.

Reserve Bank of India(RBI) issued elaborate cybersecurity guidelines that restricted and tested the operations of all urban co-operative banks (UCBs), carefully assessing the evolving IT risk factors. The level of technology adoption and digitization varies across banks and sectors but the RBI aims to standardize the security frameworks for all of them.

The Insurance Regulatory Authority of India rolled out a comprehensive cybersecurity framework upholding the security of the insurers. The directives passed by IRDA focus on the mitigation of external as well as internal threats, preventing cyber frauds, establishing robust business continuity, and risk assessment plan to bolster the backbone of shaping a secured Fintech industry. The key focus areas for the insurance industry remain:

- Online transaction and messaging frauds

- Data leakage
- IPR violations risk and
- Ransomware attack

The Department of Telecommunication has also taken cybercrime, data privacy, and consumer security as important issues to handle.

- The designated officials of TRAI (Telecom Regulatory Authority of India) and DOT have amended the cyber laws, underlying their responsibility towards consumer data – as the most critical online transactions are conducted via mobile phones.
- TRAI, the telecom industry watchdog, is renamed as the Digital Communications Regulatory Authority of India – with modified and intensified powers.
- Data Security Council of India (DSCI), is a not-for-profit, industry body on data protection in India, set up by NASSCOM®, committed to making cyberspace safe, secure, and trusted by establishing best practices, standards, and initiatives in cyber security and privacy.
- To further its objectives, DSCI engages with governments and their agencies, regulators, industry sectors, industry associations, and think tanks for designing cyber security policies.



NIST, an International body of standards has released a Cybersecurity Framework, which encompasses all required guidelines, standards, and best practices to manage cyber-related risks responsibly. It promotes the resilience and protection of critical infrastructure by:

- Allowing better interpretation, management, and reduction of cybersecurity risks – to mitigate data loss, data misuse, and the subsequent restoration costs
- Determining the most important activities and critical operations - to focus on securing them and many more.

Thank You