National Cyber Security Policy - [UPSC Notes PDF]

In 2013 the Department of Electronics and Information Technology approved a policy document known by the name The National Cyber Security Policy and its framework, aiming to protect private configuration from cyber attacks. The principle is to pursue protecting information, such as personal information, financial/banking information, sovereign data etc.

In this article we will discuss the importance of cyber security and detailed information regarding the National Cyber Security Policy as cybersecurity is an important topic in the UPSC exam syllabus.

What is National Cyber Security Policy ?

National Cyber Security Policy is a policy structure formulated by The Department of Electronics and Information Technology (DeitY) and Its aim is to protect the public and private infrastructure from cyber attacks. This policy also proposes to safeguard information, such as personal information of web users , financial and banking information and sovereign data.

India had no Cyber security policy before 2013. This policy was brought up particularly in the wake of The US government was spying on India and there were no technical or legal safeguards against it. Under pressure, the government disclosed a National Cyber Security Policy on 2 July 2013.

The National Cyber Security Policy document blueprint is a guideline to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country.

National Cyber Security Policy Vision

The National Cyber Security Policy vision is to build a secure and irrepressible cyberspace for citizens, business, and government and also to protect anyone from conciliation in user's privacy.

National Cyber Security Policy Mission

- Mission is to protect information and information infrastructure in cyberspace.

- To build capabilities to prevent and respond to cyber threats.
- To reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.

National Cyber Security Policy Objectives

- Increase adoption of IT in all sectors of the economy by the creation of a secure cyber ecosystem.
- Achieving an adequate trust and confidence in IT systems and transactions in cyberspace by creating a secure cyber ecosystem in the country.
- Increase adoption of IT in all sectors of the economy by the creation of a secure cyber ecosystem.
- Creating a guaranteed framework for the design of security policies and promotion and enabling actions for concurrence to global security standards and best practices by way of conformity assessment (Product, process, technology & people).
- Developing a culture of cybersecurity and privacy.
- Developing effective public and private partnerships to cyberspace and also collaborative commitments by means of technical and operational cooperation.
- Strengthening the Regulatory Framework for ensuring a SECURE CYBERSPACE ECOSYSTEM.
- Expanding and enhancing National and Sectoral level 24x7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions.
- Improving the visibility of integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products.
- Creating a workforce for 500,000 professionals skilled in the next 5 years through capacity building skill development and training.
- By providing fiscal benefit to businesses for adoption of standard security practices and processes.
- By enabling Protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and reducing economic losses due to cyber crime or data theft.
- By developing effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.
- To Build up suitable indigenous security technologies to address requirements in this field.

National Cyber Security Policy Strategies

As per American cybersecurity firm Palo Alto Networks 2021 report, Maharashtra was the most targeted state in India according to the increasing number of cyber attacks — facing 42% of all ransomware attacks.

In that report stated that India is among the more economically profitable regions for hacker groups and in order to regain access to the data, these hackers were asking Indian firms to pay a ransom, usually using cryptocurrencies. Higher the the global average of 21%, one in four Indian organisations suffered a ransomware attack in 2021

Creating a secure cyber ecosystem

- To delegate a National nodal agency to coordinate all matters related to cyber security in the country, with clearly defined roles & responsibilities.
- To encourage all organizations to develop information security policies duly integrated with their business plans and implement such policies as per international best practices . Such policies should include establishing standards and mechanisms for secure information flow (while in process, handling, storage & transit), crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.
- To ensure that all organizations earmark a specific budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents.
- To prevent occurrence and recurrence of cyber incidents by way of incentives for technology development, cyber security compliance and proactive actions.
- To establish a mechanism for sharing information and for identifying and responding to cyber security incidents and for cooperation in restoration efforts.

Creating an assurance framework

- To enable implementation of global security best practices in formal risk assessment and risk management processes, business continuity management and cyber crisis management plan by all entities within Government and in critical sectors, to reduce the risk of disruption and improve the security posture.
- To identify and classify information infrastructure facilities and assets at entity level with respect to risk perception for undertaking commensurate security protection measures.
- To encourage secure application / software development processes based on global best practices.
- To promote adoption of global best practices in information security and compliance and thereby enhance cyber security posture.

Encouraging Open Standards

- To encourage use of open standards to facilitate interoperability and data exchange among different products or services.
- To promote a consortium of Government and private sector to enhance the availability of tested and certified IT products based on open standards

Strengthening the Regulatory framework

- To mandate periodic audit and evaluation of the adequacy and effectiveness of security of information infrastructure as may be appropriate, with respect to regulatory framework.
- To enable, educate and facilitate awareness of the regulatory framework.
- To develop a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyberspace.
- Creating mechanisms for security threat early warning, vulnerability management and response to security threats
- To implement Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical national processes or endangering public safety and security of the Nation, by way of well coordinated, multi disciplinary approach at the National, Sectoral as well as entity levels.
- To create National level systems, processes, structures and mechanisms to generate necessary situational scenarios of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.
- To conduct and facilitate regular cyber security drills & exercises at National, sectoral and entity levels to enable assessment of the security posture and level of emergency preparedness in resisting and dealing with cyber security incidents.

Securing E - Governance services

- To mandate implementation of global security best practices, business continuity management and cyber crisis management plan for all e-Governance initiatives in the country, to reduce the risk of disruption and improve the security posture.
- To encourage wider usage of Public Key Infrastructure (PKI) within Government for trusted communication and transactions.
- To engage information security professionals / organisations to assist e - Governance initiatives and ensure conformance to security best practices.

Protection and resilience of Critical Information Infrastructure

- To encourage and mandate as appropriate, the use of validated and certified IT products.
- To mandate security audit of critical information infrastructure on a periodic basis.
- To mandate certification for all security roles right from CISO / CSO to those involved in operation of critical information infrastructure.
- To mandate implementation of global security best practices, business continuity management and cyber crisis management plan by all critical sector entities, to reduce the risk of disruption and improve the security posture.
- To mandate a secure application/software development process.

Promotion of Research & Development in cyber security

- To encourage Research & Development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of cyber security challenges and targets for export markets.
- To facilitate transition, diffusion and commercialization of the outputs of Research & Development into commercial products and services for use in public and private sectors.

Reducing supply chain risks

- To build trusted relationships with product / system vendors and service providers for improving end-to-end supply chain security visibility.
- To create awareness of the threats, vulnerabilities and consequences of breach o f security among entities for managing supply chain risks related to IT.
- To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices.

Human Resource Development

- To establish cyber security training infrastructure across the country by way of public private partnership arrangements.
- To establish cyber security concept labs for awareness and skill development in key areas.
- To establish institutional mechanisms for capacity building for Law Enforcement Agencies

Creating Cyber Security Awareness

- To promote and launch a comprehensive national awareness program on security of cyberspace.

- To conduct, support and enable cyber security workshops / seminars and certifications.
- To sustain security literacy awareness and publicity campaigns through electronic media to help citizens to be aware of the challenges of cyber security.

Developing effective Public Private Partnerships

- To facilitate collaboration and cooperation among stakeholder entities including private sector, in the area of cyber security in general and protection of critical information infrastructure in particular for actions related to cyber threats, vulnerabilities, breaches, potential protective measures, and adoption of best practices.

Information sharing and cooperation

- To enhance National and global cooperation among security agencies, CERTs, Defence agencies and forces, Law Enforcement Agencies and the judicial systems.
- To create mechanisms for dialogue related to technical and operational aspects with industry in order to facilitate efforts in recovery and resilience of systems including critical information infrastructure.

Prioritized approach for implementation

- To adopt a prioritized approach to implement the policy so as to address the most critical areas in the first instance.

Key features of the National Cyber Security Policy

- Increasing cooperation and coordination among all the stakeholder entities within the country.
- Objectives and strategies in assisting with the National Cybersecurity vision and mission.
- Framework and enterprises that can be pursued at the Govt. level, sectoral levels as well as in public-private partnership mode.
- Enabling goals aimed at minimising response & recovery time and effective cybercrime investigation and prosecution, reducing national vulnerability to cyber attacks, preventing cyber attacks & cyber crimes.
- Enabling goals aimed at reducing national vulnerability to cyber attacks, preventing cyber attacks & cyber crimes, minimising response & recovery time and effective cybercrime investigation and prosecution.

- National cyber security policy 2013 vision and mission is aimed at building a secure and give cyberspace for citizens, businesses and Government.