एनटीपीसी
NTPC
A Maharatna Company

Cyber Security Policy

NTPC LIMITED

**REG. OFFICE – NTPC BHAWAN, CORE-7, SCOPE COMPLEX
INSTITUTIONAL AREA, LODHI ROAD
NEW DELHI-110003**

Confidentiality Statement

This product or document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form, by any means electronic, mechanical, photographic, optic recording or otherwise without prior consent, in writing, of the information owner.

Document Control

Document Name	Cyber Security Policy
Document Reference Number	CCIT-IMS-PLCY-CSP
Classification	Public
Version Number	R1.0
Date	30-12-2022
Reviewed by	A K Patel
Approved by	M Bishoyee

Revision History

Date	Version	Description	Created by
30-12-2022	R1.0	Initial Draft	Kuldeep Singh

Distribution

- Intranet Portal
- E-mail

Documentation Status

This is a controlled document. This document may be printed; however, any printed copies of the document are not controlled. The electronic version maintained in the Intranet Portal is the controlled copy.

NTPC Cyber Security Policy Statement

NTPC aspires to be the world's leading power company, energizing India's growth by providing reliable power and related solutions in an economical, efficient and environment friendly manner, driven by innovation and agility.

Cyber Security Vision

"To become the most effective power generation and distribution company with the ability to make risk based informed decisions diminishing security risks to an acceptable level"

We, at NTPC recognize the importance of enabling cyber security and consider information and related assets as fundamental for the successful business operations. A cyber security framework compromising of the security policies and procedures has been adopted to effectively protect data/information and assets of the organization and its stakeholders from security threats, whether internal or external, deliberate, or accidental.

Cyber Security Mission

"Design, implement and maintain a security program that protects the NTPC's resources against unauthorized use, modification and loss. Establish a practical security program that enables NTPC to be the best power generating and distribution company".

NTPC acknowledges that cyber security is everyone's responsibility in the organization. NTPC employees are committed towards an effective cyber security in accordance with the strategic business objectives.

NTPC shall achieve cyber security vision and mission by ensuring that assets are:

- Not accessed by unauthorized person through deliberate or careless action
- Protected from unauthorized modification and
- Available to authorized users when needed.

Hence maintaining Confidentiality, Integrity and Availability (CIA).

NTPC shall ensure compliance with all applicable contractual, regulatory bodies & legislative requirements and cyber security framework designed as per the standards, guidelines and practices that can be used to prevent, detect, and respond cyber-attacks.

NTPC shall ensure communication and availability of policies to all personnel accessing NTPC's assets and violation of policies is dealt with appropriate disciplinary action.

NTPC shall ensure to maintain the cyber security during all crisis situations and disaster scenarios as far as practicable and cyber security awareness/ training are imparted to all the stakeholders.

NTPC shall ensure that the incident management process is established and implemented to adequately manage security breach, actual or suspected, and all security incidents are reported and investigated. Also, cyber security strategic decisions, future-plans, achievements and likewise are taken up as agenda in the board meetings regularly.

NTPC shall ensure that adequate measures are taken to protect security and privacy of citizen data at each stage of data life cycle

NTPC Cyber Security Objectives

NTPC shall enable cyber security framework consisting of structured and well-defined policies, procedures and guidelines while addressing the following objectives:

- Critical information, data and assets are protected from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional by implementing technical, process, people control.
- Business continuity and disaster recovery plans are established, maintained, and tested periodically to provide guidance for identifying, containing, eradicating, and recovering from cyber security incidents pertaining to phishing attack.
- Measures to be adopted and implemented to protect the industrial control systems with operational control information security, process Hazard Analysis, Health Safety and Environment (HSE) and Safety Instrumented Systems security requirements (SIS) to ensure delivery of critical infrastructure services by NTPC.
- Awareness programs on information/ cyber-security are imparted to all employees and wherever applicable to third parties.
- Ensuring continual improvement to the NTPC cyber security posture

Review and Compliance

Responsibility for compliance with the Policies lies with HEAD-IT and the nominated Representatives.

The Policy will be reviewed at least once annually or when necessitated by significant changes in business context.