Cyber Security Policy

NTPC GREEN ENERGY LIMITED (NGEL)

REG. OFFICE –

NTPC BHAWAN, CORE -7, SCOPE COMPLEX 7 INSTITUTIONAL AREA,
LODI ROAD, NEW DELHI -110003

Document	Cyber Security Policy
Reference Number	NGEL-IT-CSP-01
Classification	Public
Version	V1.0
Date	02.01.2026
Reviewed by	Shri Rajeev Verma, AGM(IT), NGEL
Approved by	Shri Sarit Maheshwari, CEO (NGEL and NTPC REL)

Revision History

Date	Version	Description	Created by (Shri)	Reviewed by (Shri)	Approved by (Shri)
02.01.2026	1.0	Cyber Security Policy	Lokesh K Parekar	Rajeev Verma	Sarit Maheshwari

Distribution

- Internet website
- Intranet Portal
- E-mail

Confidentiality Statement

NGEL Cyber Security Policy Statement

NGEL is an umbrella company for the green business initiatives of NTPC (India's largest integrated power company). NGEL aspires to become World's leading Green Energy Solutions Company, Driving India's Energy Transition by providing reliable, affordable and Sustainable Green Energy Solutions to Achieve India's Energy Transition Objectives by Leveraging Innovation and Technology.

I. Purpose

This Cyber Security Policy establishes a framework to protect the confidentiality, integrity, and availability of information technology (IT) and operational technology (OT) assets critical to the safe and reliable operation of NGEL.

II. Scope

This policy applies to all employees, contractors, vendors, and third parties who access or manage the utility's IT and OT systems, including:

- Generation, transmission, and distribution infrastructure
- SCADA, EMS, DMS, and other control systems
- Corporate IT systems and data centres

III. Cyber Security Vision

"To safeguard our green energy future by embedding robust, adaptive, and sustainable cybersecurity practices across all digital and operational layers"

IV. Cyber Security Mission

"To safeguard the organization's digital resources through a risk-based, resilient security program that prevents unauthorized use, modification, and loss; ensures compliance with all applicable standards and regulations; and enables NGEL to be the world's leading Green Energy Solutions provider".

V. Strategies

NGEL acknowledges that cybersecurity is a shared responsibility across all levels of the organization. Every employee is expected to contribute to the protection of digital assets in alignment with the company's strategic business objectives.

To achieve its cybersecurity vision and mission, NGEL shall ensure that all information assets are:

- Not accessed by unauthorized individuals, whether through deliberate or careless actions
- Protected from unauthorized modification or tampering
- Available to authorized users when needed

This approach upholds the core principles of Confidentiality, Integrity, and Availability (CIA).

Compliance and Governance: NGEL shall comply with all applicable contractual obligations, regulatory requirements, and legislative mandates. A cybersecurity framework shall be designed and maintained in accordance with recognized standards, guidelines, and best practices to prevent, detect, and respond to cyber threats.

Policy Communication and Enforcement: All cybersecurity policies shall be communicated clearly and made accessible to personnel who interact with company assets. Violations of these policies shall be subject to appropriate disciplinary action, in accordance with HR and legal protocols.

Incident Management: An incident management process shall be established and implemented to effectively handle actual or suspected security breaches. All security incidents must be reported, investigated, and documented.

Data Lifecycle Protection: Adequate measures shall be taken to protect the security and privacy of citizen and client data at every stage of its lifecycle—from creation and storage to transmission and disposal.

VI. Objectives

NGEL shall establish and maintain a comprehensive cybersecurity framework consisting of structured and well-defined policies, procedures, and guidelines. This framework is designed to ensure the protection of digital assets, operational resilience, and regulatory compliance across all business functions. The objectives of the cybersecurity framework are:

- **Protection of Critical Information and Assets:** Safeguard sensitive data and critical infrastructure from unauthorized access, use, disclosure, modification, and disposal—whether intentional or accidental—through technical controls, process enforcement, and personnel accountability.
- **Business Continuity and Incident Response:** Develop and periodically test business continuity and disaster recovery plans to ensure rapid identification, containment, eradication, and recovery from cybersecurity incidents, with special emphasis on phishing attacks and social engineering threats.
- **Industrial Control System (ICS) Security:** Implement robust security measures for operational technologies, including Operational control information security, Process Hazard Analysis (PHA) Health, Safety, and Environment (HSE) protocols, Safety Instrumented Systems (SIS) security requirements These controls support the safe and uninterrupted delivery of critical infrastructure services.
- **Cybersecurity Awareness and Training:** Conduct regular awareness programs for all employees and relevant third parties to promote a culture of cybersecurity vigilance and informed behaviour.
- **Continual improvement:** Ensuring continual improvement to the cyber security posture through regular audits, threat assessments, policy updates, and adoption of emerging best practices and technologies.

VII. Review and Compliance

This policy will be reviewed annually or after major changes in operations or threat landscape. Policy will be updated to reflect new risks, technologies, and compliance requirements.