NACL Industries Limited

CYBERSECURITY COMPLIANCE POLICY

(As approved & adopted by the Board of Directors at its Meeting held on May 28, 2025)

Purpose

This policy outlines the framework and responsibilities necessary to ensure organizational compliance with the cybersecurity directions issued by the **Indian Computer Emergency Response Team (CERT-In)** on April 28, 2022, as mandated under **sub-section (6) of section 70B of the Information Technology Act, 2000**. These directions are legally binding and are critical for strengthening the national cybersecurity posture.

The policy specifically addresses the following areas of compliance:

A. Synchronization of All ICT System Clocks with Authorized NTP Servers:
Accurate time synchronization is vital for the integrity, traceability, and analysis of cybersecurity events. Discrepancies in system clocks can hinder incident investigation, log correlation, and evidence validation. To this end, all Information and Communication Technology (ICT) systems within the organization must ensure their internal clocks are synchronized with **Network Time Protocol (NTP)** servers authorized by the Government of India, such as those operated by the **National Informatics Centre (NIC)** or the **National Physical Laboratory (NPL)**. This synchronization must be maintained continuously to support reliable timestamping of logs and ensure forensic readiness.

B. Designation of a Point of Contact (PoC) to Interface with CERT-In:
To facilitate effective communication and coordination with CERT-In, the organization shall designate an official **Point of Contact (PoC)**. The PoC will serve as the primary liaison for all CERT-In related activities, including but not limited to incident reporting, response coordination, compliance documentation, and implementation of cybersecurity advisories and directives. The PoC must be available 24x7 or ensure an alternate mechanism for timely response. The contact details of the PoC shall be formally communicated to CERT-In and updated promptly in case of any changes.

1. **Scope:** This policy applies to all employees, contractors, and third-party service providers who manage or operate the organization's **Information and Communication Technology** (ICT) systems.

2. **Policy Statements:**

2.1 Synchronization of ICT System Clocks:

i. **Requirement:** All ICT systems must synchronize their internal clocks with the NTP servers of the National Informatics Centre (NIC) or the National Physical Laboratory (NPL), or with NTP servers traceable to these servers.

ii. **Authorized NTP Servers:**

a. **NIC:** samay1.nic.in, samay2.nic.in

b. **NPL:** time.nplindia.org

2.2 **Implementation:**

i. System administrators must configure all servers, network devices, and other ICT systems to synchronize time with the authorized NTP servers.
ii. For organizations with operations across multiple geographies, alternative accurate and standard time sources may be used, provided they do not deviate from the NTP servers of NIC or NPL.

3. Log Retention and Security

3.1 **Mandatory Log Enablement and Retention:** All service providers, intermediaries, data centres, body corporates, and government organizations associated with NACL Industries Limited shall mandatorily enable logs of all their ICT systems.

3.2 **Retention Period and Jurisdiction:** These logs must be maintained securely for a rolling period of **180 days** and must be stored **within the jurisdiction of India**, as mandated by CERT-In.

3.3 **Access and Availability:** Logs shall be made available to CERT-In as and when required for cybersecurity incident investigation or audit purposes, in accordance with applicable laws and regulations.

4. **Monitoring and Compliance:**

4.1 Regular audits must be conducted to ensure all systems are correctly synchronized.

4.2 Any discrepancies must be addressed promptly to maintain compliance.

5. **Designation of Point of Contact (PoC) to Interface with CERT-In**

5.1 **Requirement:** The organization must designate a PoC to interface with CERT-In for communication and compliance purposes.

5.2 **PoC Information Submission:**

i. The following details of the designated PoC must be submitted to CERT-In via email at info@cert-in.org.in in the specified format:

Name: Shubhashish Dutta
Designation: VP – IT & CIO
Organization Name: NACL Industries Limited
Office Address: Plot no12A,C, Opposite Corporation Bank, Nagarjuna Hills Punjagutta, Hyderabad, Telangana 500082
Email ID: shubhashish@naclind.com
Mobile Number: 9717595300
Office Phone Number: 040 24405211

6. **Responsibilities of the PoC:**

6.1 Act as the primary liaison between the organization and CERT-In.

6.2 Ensure timely reporting of cyber incidents as per CERT-In guidelines.

6.3 Coordinate incident response and compliance activities within the organization.

7. **Updating PoC Information:** Any changes to the PoC's contact information must be communicated to CERT-In promptly.

8. **Roles and Responsibilities:**
   8.1 IT Department:
   i. Implement and maintain time synchronization across all ICT systems.
   ii. Conduct regular audits to ensure compliance.
   8.2 **Designated PoC:**
   iii. Serve as the official communication channel with CERT-In.
   iv. Coordinate internal responses to cybersecurity incidents.
   8.3 **Compliance Officer:** Shall oversee adherence to this policy and facilitate training and awareness programs related to cybersecurity compliance.

9. **Enforcement:** Non-compliance with this policy may result in disciplinary action, including but not limited to suspension of system access, termination of employment, or legal action, depending on the severity of the breach.

10. **Review and Revision:** This policy shall be reviewed annually or as required to accommodate changes in regulatory requirements or organizational needs.

11. **References:**
    11.1CERT-In Directions under sub-section (6) of section 70B of the Information Technology Act, 2000, dated April 28, 2022.
    11.1 CERT-In Frequently Asked Questions on Cyber Security Directions of April 28, 2022.
12. **Conclusion:**

NACL Industries Limited is committed to maintaining the highest standards of cybersecurity in alignment with national regulations and best practices. This policy establishes a structured approach to complying with the directions issued by CERT-In under the Information Technology Act, 2000. By ensuring accurate system time synchronization and maintaining a designated Point of Contact for CERT-In coordination, the organization enhances its ability to detect, respond to, and recover from cybersecurity incidents. All stakeholders are expected to adhere strictly to this policy to safeguard the organization's digital infrastructure and contribute to national cybersecurity resilience.