KSEB
കേരളത്തിന്റെ ഊർജ്ജം

KERALA STATE ELECTRICITY BOARD Ltd
(Incorporated under the Companies Act, 1956)
Registered Office: Vydyuthi Bhavanam, Pattom,
Thiruvananthapuram – 695 004
CIN: U40100KL2011SGC027424
Website: www.kseb.in
Phone: +91 471 2514576, 2446885, 9446008884
Email: dtkseb@kseb.in

ABSTRACT

Critical Information Infrastructure - Protected systems of SLDC notified - Formation of Information Security Steering Committee (ISSC) - Sanction accorded - Orders issued.

CORPORATE OFFICE (SBU-T)

BO (FTD)No.455/2023(DIRTSO-AEE3/2022/1864) Thiruvananthapuram,Dated: 20.10.2023

Read: 1. Gazette Notification vide G.O. (P) No. 3/2022/Power dated 14.11.2022 (SRO No.1145/2022).
2. Letter No. XXXII/080/03/04/Power & Energy/08/2020(Part)-1698 dated 16.12.2022 of NCIIPC.
3. Letter No. DIRTSO-AEE3/2022/1864(7) dated 30.07.2023 of the Director[T,SO&P].
4. Letter No. CESO/EELD1/AE CYBER/CII/23-24/1029 dated 25.08.2023 of the Chief Engineer (TSO).
5. Note No. DIRTSO-AEE3/2022/1864[8] dated 19.09.2023 of the Director [T,SO&P] to the Full Time Directors (Agenda No. 16-10/2023).

ORDER

The Information Technology (IT) Act 2000 was enacted to promote the IT industry, regulate e-commerce, facilitate e-governance and prevent cyber crime in India. As per the IT Amendment Act 2008, Critical Information Infrastructure (CII), is defined as the computer resource, the incapacitation or destruction of which shall have debilitating impact on national security, economy, public health or safety. Cyber security of CII is of paramount concern to governments worldwide. The Government of India has created the National Critical Information Infrastructure Protection Centre (NCIIPC), under Section 70 A (I) of the IT Amendment Act 2008, to function as the National Nodal Agency in respect of Critical Information Infrastructure (CII) protection. In the event of any threat to the Critical Information Infrastructure (CII), the National Critical Information Infrastructure Protection Centre may call for information and give directions to the critical sectors or persons serving or having a critical impact on CII. Identification of all CII elements is the responsibility of NCIIPC.

NCIIPC and Kerala State Load Despatch Centre (SLDC), after joint evaluation has identified the following systems as CII of SLDC:

a) Supervisory Control and Data Acquisition System (SCADA), b) Automatic Demand Management System (ADMS), c) Unified Real Time Dynamic State Measurement System (URT DSM).

Based on KSEBL's request and in exercise of the powers conferred by Sub sections (1) and (2) of the IT Act, 2000, the Government of Kerala as per G.O. read as 1st above, has declared the computer resources such as SCADA, ADMS and URT DSM and the computer resources of its associated dependencies, identified as CII of SLDC, Kerala as Protected Systems. The persons who are authorized to access the notified Protected Systems have also been notified.

Further to the notification of protected systems, NCIIPC, as per letter read as 2nd above informed that in accordance with the IT (Information Security Practices and Procedures for Protected Systems) Rules 2018, an Information Security Steering Committee (ISSC) is to be formed and the order for constitution of ISSC is to be issued. The composition of ISSC shall be as below:

i. IT head or equivalent
ii. Chief Information Security Officer (CISO)
iii. Financial Advisor or equivalent
iv. Representative of NCIIPC
v. Any other expert(s) to be nominated by the organisation

The rules and responsibilities of ISSC as specified in the IT (Information Security Practices and Procedures for Protected Systems) Rules 2018 are as below:

a. All the Information Security Policies of the "Protected System" shall be approved by ISSC.
b. Significant changes in network configuration impacting "Protected System" shall be approved by ISSC.
c. Each significant change in application(s) of the "Protected system" shall be approved by ISSC.
d. A mechanism shall be established for timely communication of cyber incident(s) related to "Protected system" to ISSC.
e. A mechanism shall be established to share the results of all information security audits and compliance of " Protected system" to ISSC.
f. Assessment for validation of "Protected System" after every two years

The Chief Engineer (Transmission System Operation) as per letter read as 4th above has requested sanction for constitution of the ISSC at SLDC, Kerala with the following officers:

1. Sri. Viju Rajan John, Chief Engineer (Transmission System Operation) & CISO,SLDC Kerala
2. Sri. Praveen M.A, Chief Engineer (IT, CR & CAPs) - in the category of IT head
3. Smt. Radhika M, Finance Officer, Tender section, O/o FA - in the category of Financial Adviser or equivalent
4. Sri. Sunil K, Deputy Chief Engineer,System Operation Circle, Thiruvananthapuram - as subject expert
5. Sri. Aniruddha Kumar, Director, NCIIPC (South) - NCIIPC nominee

The matter was placed before the Full Time Directors as per note read as 5th above.

Having considered the matter in detail, the Full Time Directors, through circulation, resolved to accord sanction for the formation of the Information Security Steering Committee (ISSC) as directed by NCIIPC, with the members stated above.

Orders are issued accordingly.

By Order of the
Full Time Directors

sd/

LEKHA G
Company Secretary

To:
The Chief Engineer [Transmission System Operation]

Copy to: The Chief Engineer (IT,CR&CAPS)/ Financial Advisor/ LA&DEO/ Chief Internal Auditor/ Company Secretary
The TA to the Chairman & Managing Director / Director (Generation-Civil) / Director (Distribution, Safety, SCM & IT) / Director (Transmission, SO & Planning)/ Director (Generation - Electrical, REES, SOURA, Sports & Welfare)

The PA to the Director (Finance & HRM)
The Sr.CA to the Secretary (Administration)
The RCAO/ RAO
Stock File.

Forwarded / By Order

Assistant Executive Engineer