MANGALORE ELECTRICITY SUPPLY COMPANY LIMITED
(Government of Karnataka Undertaking)
CIN: U 40109 KA 2002 SGC 030425

MESCOM/EE(IT)/AEE(IT-1)/AE(IT-3)/2019-20/CYS-01 Date: 19 DEC 2019

CIRCULAR

Sub: Guidelines for physical and Cyber Security in MESCOM reg.

Ref:
1. Office Memorandum of Government of India No: (204430) dated 05.05.2017.
2. Office Memorandum of Government of India No: 1/6/2011/IT/Pt-III (235943) dated 09.05.2017.
3. Letter NO: 1/12/2019/IT (248297) dated 04.09.2019 from Ministry of Power, Govt. of India.
4. T. O. Official Memorandum No: GM/AGM(A)/AO(A)/SA/2019-20/8237-248 dated 16.09.2019.
5. Letter No: 1/6/2011-IT-IV (236746) dated 09.10.2019 from Under-Secretary to Government of India.
6. Letter No: 1/12/2019/IT (248297) dated 18.10.2019 from S. K. G. Rahate Add. Secretary, Ministry of Powers, Govt. of India.
7. Proceeding of meeting held by Additional Chief Secretary, Energy Department dated 02.11.2019.
8. Proceeding of meeting held by Director (Technical), KPTCL dated 06.11.2019.
9. T.O. Approved Note No: 173/17-18/IT para (30) dated 18.12.2019.

*****

In view of Cyber-attacks on critical infrastructure, the Ministry of Power (MoP) by CERT-Distribution, Govt. of India, has directed to take necessary steps to prevent cyber incidents from various cyber-attacks in Power Distribution Systems.

Vide reference (3), National Cyber Security coordinator has advised to Identify Critical Information Infrastructure (CII) in Power Sector in accordance with the provisions of Section 70 of Information Technology (IT) Act 2000 and guidelines has been issued for mitigation of cyber security threats in Power Sector vide reference (5).

As per the directions vide reference (5), Executive Engineer (Ele)-IT and Assistant Executive Engineer (Ele)-IT have been nominated as Chief Information Security Officer (CISO) and Alternate Chief Information Security Officer respectively in MESCOM vide reference (4).

Further, Additional Chief Secretary, Energy Department, Govt. of Karnataka has issued direction on Cyber Security and Identification of Critical Information Infrastructure (CII) in Power Sector vide reference (7). As such SCADA Center, Sub-Stations, MESCOM Data Center, All modules of R-APDRP, Web based Applications have been identified has Critical Information Infrastructure (CII).

The action is to be taken in accordance with the guidelines for mitigation of Cyber Security threats in Power Sector issued by National Critical Information Infrastructure Protection Centre (NCIIPC).

In this regard, I am directed to communicate the following guidelines on physical and Cyber Security measures in MESCOM;

- All offices Pc's/Desktops/Laptops should have reliable Operating System Software, Antivirus Software installed for detecting and removing virus, malware, adware and spyware. Periodical updates of software patches firmware, applications etc., shall be carried out as a basic cyber hygiene practice.
- The Login ID's and Passwords issued to concerned officers /employees should not be shared with any one. Many of the passwords are weak and hackers could easily crack to the passwords. So, the Secure Password using alpha-numeric with special character shall be used and periodically the Secure Password shall be changed.
- All the systems should be connected over a Firewall to monitor network traffic – inbound and outbound. Unwanted websites/portals shall be blocked at the firewall.
- Never open or reply to suspicious-looking emails even if they appear to be from a known sender and do not click on suspicious links or download attachments.
- Weekly Back-up of critical data shall be made to an external hard drive regularly or scheduled automated backups can be performed to ensure regular backup activity.
- Statistical data for study purpose may be given only to entity authorized by GoI/GoK/MD and only after duly signing Non-Disclosure Agreement. Utilities may share only required statistical information and refrain from sharing the critical data or giving access to the system.
- CCTV cameras should be installed at all the critical infrastructure, substations, SCADA Center and important offices. CCTV footages should be monitored regularly and immediate necessary steps should be taken in the instance of security breach.
- All Sub-stations should be provided with CCTV Cameras where outsourced agency staff are working and control room should be established to monitor.
- The consumer personal data and information should not be shared with any external agency.

Any incident on Cyber Security breaches immediate necessary action shall be taken and report shall be sent to the undersigned officer for further needful.

19/12/19

Approved by
Managing Director, MESCOM

Chief Information Security Officer(CISO),
Executive Engineer(Ele)(IT),
MESCOM, Mangaluru.

Copy to:

1. Chief Engineer (Electy), O&M Zone, MESCOM, Mangaluru/Shivamogga.
2. Superintending Engineer (Ele), (Tech/Coml/Proj/Procu), MECOM, Corporate Office, Mangaluru.
3. Superintending Engineer (Ele), O&M Circle, MESCOM, Mangaluru/ Udupi/ Shivamogga/ Chikkamagaluru.
4. Superintending Engineer (Ele), SCADA&DCC MESCOM, Shivabhag, Kadri, Mangaluru.
5. Company Secretary, Corporate Office, MESCOM, Mangaluru.
6. Deputy General Manager (Tech), KPTCL, Corporate Office, Kaveri Bhavan, Bangalore – 560009.
7. All Executive Engineer (Ele), Corporate Office, MESCOM.
8. All Executive Engineer (Ele), Civil/O&M Division/MRT, MESCOM.
9. All Account Officer, Corporate Office, MESCOM.
10. All Account Officer, O&M Division, MESCOM.
11. All Account Officer (I/A), O&M Division, MESCOM.
12. SPS to MD/DT, Corporate Office, MESCOM, Mangaluru.
13. PS to CFO/FA(I/A), Corporate Office, MESCOM, Mangaluru.
14. MF/OC.