

Receipt No. 2649
Date: 21/10/26
Office of the Executive Director (HR)
Manipur State Power Company Ltd.
Keishampat Junction, Imphal - 795001

MANIPUR STATE POWER COMPANY LIMITED

Keishampat Junction, Imphal - 795001

Corporate Office:-

Electricity Complex, Patta No. 1293 under 87(2),

Fax : +91 385 245070

Khwai Bazar, Keishampat, Imphal - 795001, Manipur, INDIA

Tele: +91 385 245005

SLDC MANIPUR/MSPCL ☎: +91 385 2436192, +91 385 2436177, +91 7085056485, +91 7005706662

Office Order

Imphal, the 5th Oct. 2026

10/7-26
No.6/1/(SLDC)MSPCL/CYBER/2026/ Whereas, the Government of Manipur, vide Gazette Notification No. 6 dated 1st July 2026, has declared the Supervisory Control and Data Acquisition (SCADA) System and Energy Management System (EMS), being the Critical Information Infrastructure (CII) of the State Load Despatch Centre (SLDC), Manipur under Manipur State Power Company Limited (MSPCL), along with the computer resources of its associated dependencies, as **Protected Systems** under sub-section (1) of Section 70 of the Information Technology Act, 2000 (21 of 2000);

Accordingly, in pursuance of sub-section (2) of Section 70 of the Information Technology Act, 2000; the undersigned hereby authorizes access to the Protected Systems as follows:

- The Managing Director authorizes all employees of SLDC to access the Protected System, as per their roles and responsibilities.
- The General Manager(SLDC) or all DGMs under SLDC may authorize team members of contractual Managed Service Providers (MSPs) or third-party vendors, if any, to access the Protected System on a need basis. Such authorization shall be issued in writing before access is granted.
- The General Manager(SLDC) or all DGMs under SLDC may authorize external consultants, regulators, Government officials, auditors, and other stakeholders to access the Protected System on a case-by-case basis. Such authorization shall be issued in writing before access is granted.

Any unauthorized access, misuse, or violation of the conditions of authorization shall attract appropriate action under the provisions of the Information Technology Act, 2000, and other applicable laws, rules, and regulations.

This order shall come into force with immediate effect and shall remain in force until further orders.

Th. Bimol Singh
Managing Director, MSPCL

Copy to:-

1. The Executive Director (Tech/Civil & Gen/FA/HR), for kind information.
2. All General Managers, MSPCL.
3. File

Bimol
P. upload in company website
21/10/26

MANIPUR



GAZETTE

PUBLISHED BY AUTHORITY

No. 6 Imphal, Wednesday, July 1, 2026 (Asadha 10, 1948)

CONTENTS

	Pages		Page(s)
Part I Appointments, Postings Transfers Powers, Leave and other Personal Notices.	Nil	Part III Orders, Notifications and Rule of the Government of India	Nil
Part II(A) Resolutions, Regulations, Orders, Notifications and Rules etc.	33	Part IX Advertisements, Registration and notices by the Governments Offices	9
Part II(B) Orders, Notifications and Rules of the High Courts.	5		

(Separate paging is given on each part in order that it may be filed as a separate compilation)

Part-II(A)
GOVERNMENT OF MANIPUR
SECRETARIAT: POWER DEPARTMENT

NOTIFICATION

Imphal, the 24th June, 2026

No. MSPCL-5/2/2021-POWER-PD: In exercise of the powers conferred by sub-section (1) of Section 70 of the Information Technology Act, 2000 (21 of 2000), the Government of Manipur hereby declares the Supervisory Control and Data Acquisition (SCADA) System & Energy Management System (EMS) of State Load Despatch Centre (SLDC), Manipur under Manipur State Power Company Limited (MSPCL), constituting critical information infrastructure together with the computer resources associated therewith and its dependencies, as a Protected System for the purposes of the said Act.

This notification shall come into force on the date of its publication in the Official Gazette.

NEILENTHANG TELIEN,
Secretary (Power),
Government of Manipur.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

69A. Power to issue directions for blocking for public access of any information through any computer resource.—(1) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

69B. Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security.—(1) The Central Government may, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The intermediary or any person in-charge of the computer resource shall, when called upon by the agency which has been authorised under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation.—For the purposes of this section,—

(i) “computer contaminant” shall have the meaning assigned to it in section 43;

(ii) “traffic data” means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, data, size, duration or type of underlying service and any other information.]

70. Protected system.—¹[(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Explanation.—For the purposes of this section, “Critical Information Infrastructure” means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.]

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

²[(4) The Central Government shall prescribe the information security practices and procedures for such protected system.]

³[**70A. National nodal agency.**—(1) The Central Government may, by notification published in the Official Gazette, designate any organisation of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.

1. Subs. by Act 10 of 2009, s. 35, for sub-section (1) (w.e.f. 27-10-2009).

2. Ins. by s. 35, *ibid.* (w.e.f. 27-10-2009).

3. Ins. by s. 36, *ibid.* (w.e.f. 27-10-2009).