This IMS Manual (Apex document) is hereby upgraded to the Annex SL 'high-level' structure for integration of multiple Management System Standards (MSS) by ISO replacing the previous BS/PAS-99:2012 model by BSI and is aligned to the requirements of ISO 9001:2015 (QMS), ISO 14001:2015 (EMS), ISO 45001:2018 (OHSMS) and ISO 27001:2013 (ISMS) standards.

This is issued and controlled by Corporate Management Representative (CMR). All amendments to this manual will be done as per procedure for control of documents.

Shri. K.V.S. Baba
Chairman and Managing Director

This Integrated Management System Manual is the property of POSOCO. Its contents shall not be reproduced either in part or in full without the written permission of the Management.
### Document Revision History

<table>
<thead>
<tr>
<th>Rev Date</th>
<th>Rev No.</th>
<th>Revision Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>20-Nov-2017</td>
<td>3.2</td>
<td>Upgraded ISO 9001 QMS from 2008 ver to 2015 ver and ISO 14001 EMS from 2004 ver to 2015 ver requirements</td>
</tr>
<tr>
<td>05-Dec-2016</td>
<td>3.1</td>
<td>Revised for change in POSOCO leadership – CEO replaced by CMD and hence, IMS Policy signed by POSOCO CMD (Shri. K.V.S. Baba)</td>
</tr>
<tr>
<td>01-Jan-2016</td>
<td>3.0</td>
<td>Revised referencing to new certification cycle</td>
</tr>
<tr>
<td>31-Mar-2013</td>
<td>2.1</td>
<td>Revised as per PAS 99:2012 Standard requirements.</td>
</tr>
<tr>
<td>15-Jan-2013</td>
<td>2.0</td>
<td>Revised to accommodate last cycle changes and integrate apex manual with ISO/IEC 27001:2013 as integrated management system within the framework of PAS 99.</td>
</tr>
<tr>
<td>03-Sep-2008</td>
<td>1.0</td>
<td>First release for Certification cycle</td>
</tr>
</tbody>
</table>
## ABBREVIATIONS USED

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGM</td>
<td>Additional General Manager</td>
</tr>
<tr>
<td>ATC</td>
<td>Available Transfer Capability</td>
</tr>
<tr>
<td>BE</td>
<td>Budget Estimate</td>
</tr>
<tr>
<td>BIS</td>
<td>Bureau of Indian Standard</td>
</tr>
<tr>
<td>BOQ</td>
<td>Bill of Quantities</td>
</tr>
<tr>
<td>CAB / EC</td>
<td>Change Advisory Board / Emergency Committee</td>
</tr>
<tr>
<td>CB</td>
<td>Circuit Breaker</td>
</tr>
<tr>
<td>CC</td>
<td>Corporate Centre</td>
</tr>
<tr>
<td>CEA</td>
<td>Central Electricity Authority</td>
</tr>
<tr>
<td>CERC</td>
<td>Central Electricity Regulatory Commission</td>
</tr>
<tr>
<td>CGS</td>
<td>Central Generating Stations</td>
</tr>
<tr>
<td>CISO</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>COMML</td>
<td>Commercial</td>
</tr>
<tr>
<td>CKm</td>
<td>Circuit Kilometer</td>
</tr>
<tr>
<td>CMD</td>
<td>Chairman and Managing Director</td>
</tr>
<tr>
<td>CMG</td>
<td>Corporate Monitoring Group</td>
</tr>
<tr>
<td>C&amp;M</td>
<td>Contract &amp; Material</td>
</tr>
<tr>
<td>CS</td>
<td>Contract Services</td>
</tr>
<tr>
<td>CPCC</td>
<td>Central Power Coordination Committee</td>
</tr>
<tr>
<td>CT</td>
<td>Current Transformer</td>
</tr>
<tr>
<td>CTU</td>
<td>Central Transmission Utility</td>
</tr>
<tr>
<td>CVT</td>
<td>Capacitance Voltage Transformer</td>
</tr>
<tr>
<td>DEPTT</td>
<td>Department</td>
</tr>
<tr>
<td>DD</td>
<td>Demand Draft</td>
</tr>
<tr>
<td>DGM</td>
<td>Deputy General Manager</td>
</tr>
<tr>
<td>DISO</td>
<td>Department Information Security Officer</td>
</tr>
<tr>
<td>DOCO</td>
<td>Date of Commercial Operation</td>
</tr>
<tr>
<td>ED</td>
<td>Executive Director</td>
</tr>
<tr>
<td>EHV</td>
<td>Extra High Voltage</td>
</tr>
<tr>
<td>EMS</td>
<td>Environment Management System</td>
</tr>
<tr>
<td>EnMS</td>
<td>Energy Management System</td>
</tr>
<tr>
<td>ERLDC</td>
<td>Eastern Regional Load Despatch Centre (located in Kolkata)</td>
</tr>
<tr>
<td>ESM</td>
<td>Environment and Social Management</td>
</tr>
<tr>
<td>ESPP</td>
<td>Environmental and Social Policy &amp; Procedures</td>
</tr>
<tr>
<td>F&amp;A</td>
<td>Finance &amp; Accounts</td>
</tr>
<tr>
<td>FL</td>
<td>Fault Locator</td>
</tr>
<tr>
<td>FACTS</td>
<td>Flexible Alternating Current Transmission System</td>
</tr>
<tr>
<td>GM</td>
<td>General Manager</td>
</tr>
<tr>
<td>GOI</td>
<td>Government of India</td>
</tr>
<tr>
<td>HBA</td>
<td>House Building Advance</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>HEP</td>
<td>Hydro Electric Project</td>
</tr>
<tr>
<td>HRM</td>
<td>Human Resource Management</td>
</tr>
<tr>
<td>HOD</td>
<td>Head of Department</td>
</tr>
<tr>
<td>HVDC</td>
<td>High Voltage Direct Current</td>
</tr>
<tr>
<td>IPR</td>
<td>Intellectual Property Rights</td>
</tr>
<tr>
<td>ISGS</td>
<td>Inter-State Generating Station</td>
</tr>
<tr>
<td>ISMF</td>
<td>Information Security Management Forum</td>
</tr>
<tr>
<td>ISMS</td>
<td>Information Security Management System</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization <em>(ISO word is adopted from a Greek word <em>isos</em> meaning equal)</em></td>
</tr>
<tr>
<td>kV</td>
<td>Kilo Volt</td>
</tr>
<tr>
<td>LTOA</td>
<td>Long Term Open Access</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LTE</td>
<td>Limited Tender Enquiry</td>
</tr>
<tr>
<td>LTC</td>
<td>Leave Travel Allowance</td>
</tr>
<tr>
<td>MOP</td>
<td>Ministry of Power</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>MR</td>
<td>Management Representative</td>
</tr>
<tr>
<td>MIS</td>
<td>Management Information System</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>MRM</td>
<td>Modern Rice Mill</td>
</tr>
<tr>
<td>MW</td>
<td>Mega Watt</td>
</tr>
<tr>
<td>MVAR</td>
<td>Mega Volt Ampere Reactive</td>
</tr>
<tr>
<td>NERLDC</td>
<td>North Eastern Regional Load Despatch Centre (located in Shillong)</td>
</tr>
<tr>
<td>NLDC</td>
<td>National Load Despatch Centre (located in New Delhi)</td>
</tr>
<tr>
<td>NRLDCC</td>
<td>Northern Regional Load Despatch Centre (located in New Delhi)</td>
</tr>
<tr>
<td>O&amp;M</td>
<td>Operation and Maintenance</td>
</tr>
<tr>
<td>OCCM</td>
<td>Operation and Coordination Committee Meeting</td>
</tr>
<tr>
<td>OHSMS</td>
<td>Occupational Health and Safety Management System</td>
</tr>
<tr>
<td>OS</td>
<td>Operation Services</td>
</tr>
<tr>
<td>PAS</td>
<td>Publicly Available Specification</td>
</tr>
<tr>
<td>PNBC</td>
<td>Powergrid National Bipartite Committee</td>
</tr>
<tr>
<td>PRBC</td>
<td>Powergrid Regional Bipartite Committee</td>
</tr>
<tr>
<td>PSDF</td>
<td>Power System Development Fund</td>
</tr>
<tr>
<td>PTW</td>
<td>Permit to Work</td>
</tr>
<tr>
<td>PX</td>
<td>Power Exchange</td>
</tr>
<tr>
<td>QA&amp;I</td>
<td>Quality Assurance and Inspection</td>
</tr>
<tr>
<td>QMS</td>
<td>Quality Management System</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>Research and Development</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Change</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SEB</td>
<td>State Electricity Board</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SLDC</td>
<td>State Load Despatch Centre</td>
</tr>
<tr>
<td>SO</td>
<td>System Operation</td>
</tr>
<tr>
<td>SRLDC</td>
<td>Southern Regional Load Despatch Centre (located in Bangalore)</td>
</tr>
<tr>
<td>STOA</td>
<td>Short Term Open Access</td>
</tr>
<tr>
<td>UI</td>
<td>Unscheduled Interchange</td>
</tr>
<tr>
<td>WRLDC</td>
<td>Western Regional Load Despatch Centre (located in Mumbai)</td>
</tr>
</tbody>
</table>
# Table of Contents

0. INTRODUCTION ........................................................................................................... 8
  0.1 GENERAL .................................................................................................................. 8
  0.2 ANNEX SL – THE ISO STRUCTURE FOR INTEGRATION OF MULTIPLE MSS .......... 9
  0.3 INTENDED AUDIENCE ......................................................................................... 12
  0.4 STRUCTURE OF IMS DOCUMENTATION ......................................................... 12
  0.5 ABOUT POSOCO .................................................................................................... 13

1. SCOPE AND APPLICABILITY OF IMS AT POSOCO .................................................. 16

2. REFERENCES .................................................................................................................. 18

3. TERMS AND DEFINITIONS ......................................................................................... 19

4. CONTEXT OF THE ORGANIZATION ........................................................................... 24
   4.1 UNDERSTANDING THE ORGANIZATION AND ITS CONTEXT ......................... 24
   4.2 UNDERSTANDING THE NEEDS AND EXPECTATIONS OF INTERESTED PARTIES .. 25
   4.3 DETERMINING THE SCOPE OF IMS .................................................................. 25
   4.4 THE “INTEGRATED MANAGEMENT SYSTEM” .................................................... 27
       4.4.1 POSOCO WORKING STRUCTURE ......................................................... 27
       4.4.2 THE IMS AT POSOCO .......................................................................... 29
       4.4.3 SEQUENCE AND INTERACTION OF PROCESSES ......................... 32

5. LEADERSHIP ................................................................................................................ 34
   5.1 LEADERSHIP AND COMMITMENT ..................................................................... 34
       5.1.1 CUSTOMER FOCUS .............................................................................. 34
       5.2 POLICY ............................................................................................................. 35
       5.3 ORGANIZATIONAL ROLES, RESPONSIBILITIES AND AUTHORITIES .......... 35
       5.3.1 CONSULTATION AND PARTICIPATION OF WORKERS ...................... 37

6. PLANNING .................................................................................................................... 38
   6.1 ACTIONS TO ADDRESS RISKS AND OPPORTUNITIES .................................... 38
       6.1.1 COMPLIANCE OBLIGATIONS .................................................................. 39
       6.1.2 DETERMINATION OF LEGAL AND OTHER REQUIREMENTS .............. 39
       6.1.3 INTEGRATED RISK MANAGEMENT ....................................................... 39
       6.2 IMS OBJECTIVES AND PLANNING TO ACHIEVE THEM ......................... 40
       6.3 PLANNING OF CHANGES ............................................................................. 40

7. SUPPORT ...................................................................................................................... 42
   7.1 RESOURCES ........................................................................................................... 42
       7.1.1 PEOPLE ....................................................................................................... 42
       7.1.2 INFRASTRUCTURE ..................................................................................... 43
       7.1.3 WORK ENVIRONMENT ............................................................................. 43
       7.1.4 MONITORING AND MEASURING ........................................................... 44
       7.1.5 ORGANISATIONAL KNOWLEDGE ......................................................... 45
   7.2 COMPETENCE ....................................................................................................... 45
   7.3 AWARENESS ........................................................................................................ 45
   7.4 COMMUNICATION ............................................................................................ 46
   7.5 DOCUMENTED INFORMATION ........................................................................... 47

8. OPERATION ................................................................................................................... 49
8.1 OPERATIONAL PLANNING AND CONTROL ................................................................. 49
8.1.1 MANAGEMENT OF RISK .................................................................................... 49
8.1.2 CHANGE MANAGEMENT ................................................................................... 50
8.2 HANDLING CONTINGENCY SITUATION .................................................................. 50
8.3 REQUIREMENTS FOR PRODUCTS AND SERVICES ............................................... 51
8.3.1 CUSTOMER COMMUNICATION .......................................................................... 51
8.3.2 DETERMINING AND REVIEWING THE REQUIREMENTS FOR PRODUCTS / SERVICES 51
8.4 DESIGN AND DEVELOPMENT ................................................................................ 52
8.5 HANDLING PROCUREMENT OF PRODUCTS AND SERVICES ............................... 52
8.6 PRODUCTION AND SERVICE PROVISION ............................................................... 53
8.6.1 IDENTIFICATION AND TRACEABILITY ............................................................... 55
8.6.2 PRESERVATION ................................................................................................... 55
8.6.3 POST-DELIVERY ACTIVITIES ............................................................................ 55
8.6.4 CONTROL OF CHANGES .................................................................................. 55
8.7 RELEASE OF PRODUCTS AND SERVICES .............................................................. 56
8.8 CONTROL OF NONCONFORMING OUTPUTS ............................................................ 56

9. PERFORMANCE EVALUATION .................................................................................. 57
9.1 MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION ..................... 57
9.1.1 GENERAL ............................................................................................................ 57
9.1.2 CUSTOMER SATISFACTION .............................................................................. 57
9.1.3 EVALUATION OF COMPLIANCE .................................................................... 57
9.1.4 ANALYSIS OF DATA .......................................................................................... 58
9.2 INTERNAL AUDIT ................................................................................................... 58
9.3 MANAGEMENT REVIEW ......................................................................................... 59

10. IMPROVEMENT ....................................................................................................... 60
10.1 GENERAL ............................................................................................................... 60
10.2 NONCONFORMITY AND CORRECTIVE ACTION .................................................. 60
10.3 CONTINUAL IMPROVEMENT .............................................................................. 61

ANNEXURE-01: RESPONSIBILITIES & AUTHORITIES ..................................................... 62
ANX-01-01: HSSE ROLES & RESPONSIBILITY ............................................................. 62
ANX-01-02: ISMS ROLES & RESPONSIBILITIES ......................................................... 65
0. INTRODUCTION

0.1 GENERAL

This Manual specifies the requirements for Establishing, Implementing, Monitoring, Reviewing, Maintaining, and Improving a documented Integrated Management System (IMS) comprising Management System Standards (MSS) for:
- ISO 9001:2015 for Quality,
- ISO 14001:2015 for Environment,
- ISO 45001:2018 for Occupational Health and Safety, and

Within the context of overall business (See Footnote # 4) requirements at Power System Operation Corporation Ltd., referred hereafter as POSOCO, at its Corporate Office (New Delhi) and all its control centers viz., NLDC (New Delhi), NRLDC (New Delhi), NERLDC (Shillong), ERLDC (Kolkata), SRLDC (Bangalore) and WRLDC (Mumbai) in accordance to Annex SL, the high-level structure from ISO for integration of multiple MSS into Integrated Management System framework.

The adoption of Integrated Management System (IMS) is a strategic decision for POSOCO to help improve its overall business performance and provide a sound basis for sustainable development initiatives. Accordingly, the IMS has been established with a focus to address:

- The organization’s ability to consistently provide products and services\(^1\) that meet customer\(^2\) and applicable statutory, regulatory and other requirements\(^3\);
- Facilitating opportunities to enhance customer satisfaction and customer focus for quality, employees for occupational health & safety, society for environment, and stakeholders for information security;
- Risks and opportunities associated with its business\(^4\) context and objectives;
- The ability to demonstrate conformity to specified quality / environment / health & safety / information security management system requirements.

This manual now forms the basis for implementation of an integrated management system as per the needs of POSOCO.

---

\(^1\)Products and Services of POSOCO comprises of ensuring Integrated Operation of Regional and National Power Systems to facilitate transfer of electric power within and across the regions and trans-national exchange of power with Reliability, Security and Economy.

\(^2\)Customer of POSOCO are users of electrical grid identified by CERC directives.

\(^3\)Other Requirements comprise of compliances to Environment, Occupational Health & Safety and Information Security aspects (including policies, standards, rules and guidelines that govern these) in accordance to EMS (ISO 14001), OHSMS (ISO 45001) and ISMS (ISO 27001) standard’s requirements.

\(^4\)Business – as per ISO 9001 means those activities that are core to the purposes of the organization's existence, viz., the products and services provided by POSOCO (as explained in footnote #1 above).
0.2 ANNEX SL – THE ISO STRUCTURE FOR INTEGRATION OF MULTIPLE MSS

The Annex SL is a section of the ISO/IEC Directives part 1 that prescribes how ISO Management System Standard (MSS) standards should be written. The aim of Annex SL is to enhance the consistency and alignment of MSS by providing a unifying and agreed upon high level structure, identical core text and common terms and core definitions. The aim being that all ISO Type A MSS (in regard to management system requirement such as ISO 9001, ISO 14001, ISO 45001 and ISO 27001) are aligned and the compatibility of these standards is enhanced.

According to Annex SL, a Management System Standard shall follow the following high-level structure:

- Clause 1: Scope
- Clause 2: Normative references
- Clause 3: Terms and definitions
- Clause 4: Context of the organization
- Clause 5: Leadership
- Clause 6: Planning
- Clause 7: Support
- Clause 8: Operation
- Clause 9: Performance evaluation
- Clause 10: Improvement

**NOTE:**
While the high-level structure cannot be changed. It provides with identical core text and numbering schemes. However, sub-clauses and discipline-specific text can be added.

**BRIEF OF EACH ANNEX-SL CLAUSE**

**Clause 1: Scope**

The scope sets out the intended outcomes of the management system. The outcomes are industry specific and should be aligned with the context of the organization (clause 4).

**Clause 2: Normative references**

Provides details of the reference standards or publications relevant.
Clause 3: Terms and definitions

Details terms and definition applicable to specific standard(s) in addition to any formal industry-related standard terms and definitions.

Clause 4: Context of the organization

Clause 4 consists of four sub-clauses:

- 4.1 Understanding the organization and its context
- 4.2 Understanding the needs and expectations of interested parties
- 4.3 Determining the scope of the management system
- 4.4 The management system

As the flagstone of a management system, clause 4 determines why the organization is here. As part of the answer to this question, the organization needs to identify internal and external issues that can impact on its intended outcomes, as well as all interested parties and their requirements. It also needs to document its scope and set the boundaries of the management system – all in line with the business objectives.

Clause 5: Leadership

Clause 5 comprises of three sub-clauses:

- 5.1 Leadership and commitment
- 5.2 Policy
- 5.3 Organizational roles, responsibilities and authorities

The new high-level structure places particular emphasis on leadership, not just management. This means top management now has greater accountability and involvement in the organization’s management system. They need to integrate the requirements of the management system into the organization’s core business process, ensure the management system achieves its intended outcomes and allocate the necessary resources. Top management is also responsible for communicating the importance of the management system and heighten employee awareness and involvement.

Clause 6: Planning

Clause 6 includes two sub-clauses:

- 6.1 Actions to address risks and opportunities
- 6.2 Management system objectives and planning to achieve them

Clause 6 brings risk-based thinking to the front. Once the organization has highlighted risks and opportunities in clause 4, it needs to stipulate how these will be addressed through planning. The planning phase looks at what, who, how and when these risks must be addressed. This proactive approach reduces the need for corrective actions later on.

While integrating multiple MSS requirements, discipline-specific risks are integrated to evolve a holistic approach to risks and opportunities.
Similarly, discipline-specific objectives are identified and planning to achieve them is established.

Particular focus is also placed on the objectives of the management system. These should be measurable, monitored, communicated, aligned to the policy of the management system and updated when needed.

**Clause 7: Support**

Organizations are expected to look at the support aspects needed to meet their goals and objectives. Accordingly, clause 7 consists of five sub-clauses:

- **7.1 Resources** – These include Men, Material / Equipment / Tools, Money, Infrastructure.
- **7.2 Competence** – People to have appropriate skill and knowledge to deliver the intended products and services.
- **7.3 Awareness** – Staff having awareness on the MSS and its application in their work areas.
- **7.4 Communication** – Covers both internal and external communication appropriate to the organization’s working.
- **7.5 Documented information** – Defines the mechanism to control the documents and records.

**Clause 8: Operation**

The bulk of the management system requirements lies within this single clause as:

- **8.1 Operational planning and control**

Clause 8 addresses both in-house and outsourced processes, while the overall process management includes adequate criteria to control these processes, as well as ways to manage planned and unintended change.

**Clause 9: Performance evaluation**

Clause 9 is formed of three sub-clauses:

- **9.1 Monitoring, measurement, analysis and evaluation**
- **9.2 Internal audit**
- **9.3 Management review**

Here organizations need to determine what, how and when things are to be monitored, measured, analyzed and evaluated. An internal audit is also part of this process to ensure the management system conforms to the requirements of the organization as well as the standard and is successfully implemented and maintained. The final step, management review, looks at whether the management system is suitable, adequate and effective.

**Clause 10: Improvement**

In an ever-changing business world, not everything always goes according to plan. Clause 10 looks at ways to address (or manage) the detected non-conformities and their corrective action(s), as well as strategies for improvement on a continual basis.

Clause 10 has two sub-clauses:
10.1 Non-conformity and corrective action
10.2 Continual improvement

Adoption of Annex-SL by ISO for establishing this Apex Manual and the management system with this has been done considering:

a) It provides an overall management system framework, common terms and definitions*
b) Saves time during implementation
c) Makes it easier to integrate more than one management system
d) Reduces conflicts, duplication and misunderstanding

0.3 INTENDED AUDIENCE

This manual intends to address following audiences:

- Staff of POSOCO offices – to know about their Integrated Management System.
- Customers and interested parties external to POSOCO – to get a transparent view on the functioning of POSOCO and commitment to Public and Users of Power.
- Certifying Agency – to understand and evaluate the Integrated Management Systems at POSOCO.

0.4 STRUCTURE OF IMS DOCUMENTATION

The IMS documentation at POSOCO is structured in 4 levels as illustrated in figure below:

environment / occupational health & safety / information security policy adopted, and process flow diagram depicting identification & interaction of processes of POSOCO.

Level 2: The standard operating processes comprise of the domain-specific MSS requirements integrated to the POSOCO’s business system.

Level 3: Comprises of the management system control procedures required to ensure MSS control aspects are integrated into the POSOCO’s business system.

Level 4: The formats / templates required to establish management system records as evidence to demonstrate compliance to the implementation of the Management System Standards (MSS).

Cross references have been marked in ‘[see <chapter no.>]’ bracket with reference in italics.

0.5 ABOUT POSOCO

History

- 25th Feb 2009: The Regional Load Despatch Centers (RLDC) along with National Load Despatch Center (NLDC) at Power Grid Corporation of India Ltd. was merged to create a separate organization named POSOCO (Power System Operation Corporation).
- Year 2010: Came into existence as a Government of India Enterprise through a Gazette notification dt. 27th Sept 2010 and became operational w.e.f. 1st Oct 2010.

Mandate

POSOCO was established with a mission to ensure Integrated Operation of Regional and National Power Systems to facilitate transfer of electric power within and across the regions and trans-national exchange of power with Reliability, Security and Economy.

The Corporation has set the following objectives in line with its mission for integrated operation of regional and national power system through “National Load Despatch Centre and Regional Load Despatch Centres” to discharge the following functions: (Ministry of Power directive vide letter no. 41/20/2005-PG dated 4th July, 2008)

(i) To supervise and control all aspect concerning operations and manpower requirement of RLDCs and NLDC. All the employees and executives working with RLDCs and NLDC will be from the cadre of POSOCO. Presently POSOCO is a wholly owned subsidiary of POWERGRID. All the employees will be from the cadre of POWERGRID.

(ii) To act as the apex organization for human resources requirement of NLDC and RLDCs.

(iii) To ensure planning and implementation of infrastructure required for smooth operation and development of NLDC and RLDCs.

(iv) To coordinate the functioning of NLDC and all the RLDCs.
To advise and assist state level Load Despatch Centres, including specialised training etc.

To perform any other function entrusted to it by the Ministry of Power.

**Working**

POSOCO has its corporate office at B-9, Qutab Institutional Area, Katwaria Sarai, New Delhi. POSOCO is assigned to take up role of the Independent System Operator (ISO) in Indian power sector. POSOCO comprises the corporate centre and its Load Despatch Centres comprise National Load Despatch Centre at Delhi, backup National Load Despatch Centre at Kolkata with Regional Load Despatch Centers located as below:

<table>
<thead>
<tr>
<th>Load Despatch Centers</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>National (N)</td>
<td>New Delhi</td>
</tr>
<tr>
<td>Northern Region (NR)</td>
<td>New Delhi</td>
</tr>
<tr>
<td>North Eastern Region (NER)</td>
<td>Shillong</td>
</tr>
<tr>
<td>Eastern Region (ER)</td>
<td>Kolkata</td>
</tr>
<tr>
<td>Southern Region (SR)</td>
<td>Bengaluru</td>
</tr>
<tr>
<td>Western Region (WR)</td>
<td>Mumbai</td>
</tr>
</tbody>
</table>

One of the main reasons for the regions having uninterrupted power supply on continuous basis is timely coordination with different state utilities, ISGS and state generating stations and controlling the real time grid parameters. All this is possible largely due to the fact that the culture and system of working in POSOCO have all along been quality oriented.

All transmission grids are independently audited in three months to ensure that the grids are fail-safe.

POSOCO maintains the electrical Grid covering the whole of the country consisting of five regions. The customers of POSOCO are the users of the electrical grid and are identified by CERC directives.

The main functions assigned to NLDC are:

- Supervision Over the Regional Load Despatch Centres.
- Scheduling and Despatch of electricity over the inter-regional links in accordance with grid standards specified by the authority and grid code specified by Central Commission in co-ordination with Regional Load Despatch Centres.
- Coordination with Regional Load Despatch Centres for achieving maximum economy and efficiency in the operation of National Grid.
- Monitoring of operations and grid security of the National Grid.
- Supervision and control over the inter-regional links as may be required for ensuring stability of the power system under its control.
- Coordination with Regional Power Committees for regional outage schedule in the national perspective to ensure optimal utilisation of power resources.
• Coordination with Regional Load Despatch Centres for the energy accounting of inter-regional exchange of power.
• Coordination for restoration of synchronous operation of national grid with Regional Load Despatch Centres.
• Coordination for trans-national exchange of power.
• Providing Operational feedback for national grid planning to the Authority and Central Transmission Utility.
• Levy and collection of such fee and charges from the generating companies or licensees involved in the power system, as may be specified by the Central Commission.
• Dissemination Of information relating to operations of transmission system in accordance with directions or regulations issued by Central Government from time to time. Strangely, the projected auxiliary power consumption of coal fired thermal power plants (electricity generated minus energy met when auxiliary power consumption of all other types is assumed as nil) is shown as 3.6% (maximum) in NLDC daily reports which is absurd value (to be at least 7%)

The main responsibilities of RLDCs are:
• System parameters and security.
• To ensure the integrated operation of the power system grid in the respective region.
• System studies, planning and contingency analysis.
• Daily scheduling and operational planning.
• Facilitating bilateral and inter-regional exchanges.
• Computation of energy despatch and drawal values using SEMs.
• Augmentation of telemetry, computing and communication facilities.

Management

Headed by Chairman and Managing Director (CMD) and comprises of Board of Directors.

☛ Refer POSOCO website for latest structure.
☛ Establishment section in POSOCO maintain latest organogram along with duties and responsibilities of officers at various levels as per the organogram.
1. SCOPE AND APPLICABILITY OF IMS AT POSOCO

This manual meets the requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented Integrated Management System (IMS) within the context of business operations at POSOCO.

Locations covered:
A. Corporate Centre
   61, 9th Floor, IFCI Tower, Nehru Place, New Delhi 110 000
   Website: www.posoco.in

B. National Load Despatch Centre (NLDC)
   B-9, Qutab Institutional Area, Katwaria Sarai, New Delhi 110 016.
   Website: www.nldc.in

C. Regional Load Despatch Centres (RLDC’s)
   1. Northern Regional Load Despatch Centre (NRLDC)
      18-A, Saheedjeet Singh Sansanwal Marg, Katwaria Sarai, New Delhi 110 016.
      Website: www.nrldc.in

   2. Eastern Regional Load Despatch Centre (ERLDC)
      14, Golf Club Road, Tollygunge, Kolkata – 700 033.
      Website: www.erldc.org

   3. Southern Regional Load Despatch Centre (SRLDC)
      29, Race Course Cross Road, Bangalore-560 009.
      Website: www.srldc.in

   4. Western Regional Load Despatch Centre (WRLDC)
      Plot No.F-3, MIDC Area, Marol, Opposite SEEPZ, Andheri (East), Mumbai 400 093.
      Website: www.wrldc.in

   5. North Eastern Regional Load Despatch Centre (NERLDC)
      Dongtieh, Lower Nongrah, Lapalang, Shillong 793 006.
      Website: www.nerldc.org
Departments / functions broadly included are:

<table>
<thead>
<tr>
<th>Grid Operation</th>
<th>Market Operation</th>
<th>Logistics</th>
<th>NLDC – Market Operation</th>
<th>POSOCO Corporate Centre</th>
</tr>
</thead>
<tbody>
<tr>
<td>- MIS Group</td>
<td>- Regulatory Affairs Group</td>
<td>- EnMS &amp; DTS Group</td>
<td>- Ancillary Services</td>
<td>- PSDF</td>
</tr>
<tr>
<td>- System Studies Group</td>
<td></td>
<td>- Software Development &amp; Maintenance Group</td>
<td>- Human Resources</td>
<td>- Corporate HR (incl. Admin &amp; Training also)</td>
</tr>
<tr>
<td>- Protection Group</td>
<td></td>
<td>- IT Group</td>
<td>- Finance and Accounts*</td>
<td>- Corporate Finance*</td>
</tr>
<tr>
<td>- Scheduling Group in Real Time Operation</td>
<td></td>
<td>- Technical Support Services:</td>
<td>- Legal Affairs / Law*</td>
<td>- Company Secretary*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Auxiliary Maintenance Group</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Civil Maintenance Group</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:**
* marked Department’s activities for requirements of ISO 9001:2015 are not covered under the scope of Certification.

POSOCO need to comply with statutory, regulatory and other requirements and these are separately maintained (refer: IMS-02: SOPs – Chapter 5: Identification of Legal and Other Requirements).

Based on POSOCO’s mandate (see section 0.5: About POSOCO), an appropriate integrated policy statement on quality / environment / health & safety / information security has been framed by POSOCO [see 5.2].
2. REFERENCES

The following standards and guidelines are referred for establishing this manual:

- ISO 31000:2009  Risk Management – Principles and Guidelines
3. TERMS AND DEFINITIONS

QMS related the terms and definitions appearing in ISO 9001:2015 is applicable.
EMS related the terms and definitions appearing in ISO 14001:2015 is applicable.
OHSMS related the terms and definitions appearing in ISO 45001:2018 is applicable.
ISMS related the terms and definitions appearing given in ISO/IEC 27001 apply.

For risk management specific, the terms and definitions appearing in ISO 31000:2009 is applicable.

<table>
<thead>
<tr>
<th>Technical Terms (Source: IEGC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITEM</td>
</tr>
<tr>
<td>Act</td>
</tr>
<tr>
<td>Agency</td>
</tr>
<tr>
<td>Authority</td>
</tr>
<tr>
<td>Automatic Voltage Regulator (AVR)</td>
</tr>
<tr>
<td>Beneficiary</td>
</tr>
<tr>
<td>Black Start Procedure</td>
</tr>
<tr>
<td>Bulk Power Transmission Agreement (BPTA)</td>
</tr>
<tr>
<td>BIS</td>
</tr>
<tr>
<td>Captive Generating Plant (CGP)</td>
</tr>
<tr>
<td>Capacitor</td>
</tr>
<tr>
<td>CEA</td>
</tr>
<tr>
<td>CERC</td>
</tr>
<tr>
<td>Central Transmission Utility (CTU)</td>
</tr>
<tr>
<td>Connection Agreement</td>
</tr>
<tr>
<td>Connection Point</td>
</tr>
<tr>
<td>Constituent</td>
</tr>
<tr>
<td>Term</td>
</tr>
<tr>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Demand</td>
</tr>
<tr>
<td>Despatch Schedule</td>
</tr>
<tr>
<td>Disturbance Recorder (DR)</td>
</tr>
<tr>
<td>Data Acquisition System (DAS)</td>
</tr>
<tr>
<td>Drawal Schedule</td>
</tr>
<tr>
<td>Entitlement</td>
</tr>
<tr>
<td>Event</td>
</tr>
<tr>
<td>Event Logger (EL)</td>
</tr>
<tr>
<td>Ex-Power Plant</td>
</tr>
<tr>
<td>Fault Locator (FL)</td>
</tr>
<tr>
<td>Flexible Alternating Current Transmission System (FACTS)</td>
</tr>
</tbody>
</table>
| Force Majeure                          | Any event which is beyond the control of the agencies involved which they could not foresee or with a reasonable amount of diligence could not have foreseen or which could not be prevented and which substantially affect the performance by either agency such as but not limited to :-
   a)Acts of God, natural phenomena, including but not limited to floods, droughts, earthquakes and epidemics;
   b)Acts of any Government domestic or foreign, including but not limited to war declared or undeclared, hostilities, priorities, quarantines, embargoes;
   c)Riot or Civil Commotion
   d)Grid’s failure not attributable to agencies involved..
<p>| Forced Outage                          | An outage of a Generating Unit or a Transmission facility due to a fault or other reasons which has not been planned. |
| Generating Company                     | Generating Company means any company or corporate body or body of individuals, whether incorporated or not, or artificial juridical person, which owns or operates or maintains a generating station. |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generating Unit</td>
<td>An electrical Generating Unit coupled to a turbine within a Power Station together with all Plant and Apparatus at that Power Station (up to the Connection Point) which relates exclusively to the operation of that turbo-generator.</td>
</tr>
<tr>
<td>Grid Standards</td>
<td>Grid Standards specified by the Authority under clause (d) of the Section 73 of the Act.</td>
</tr>
<tr>
<td>Extra High Voltage (EHV)</td>
<td>Where the voltage exceeds 33,000 volts under normal conditions, subject, however, to the percentage variation allowed by the Authority.</td>
</tr>
<tr>
<td>Independent Power Producer (IPP)</td>
<td>A generating company not owned/ controlled by the Central/State Government.</td>
</tr>
<tr>
<td>Indian Electricity Grid Code (IEGC)</td>
<td>A document describing the philosophy and the responsibilities for planning and operation of Indian power system specified by the Commission in accordance with sub section 1(h) of Section 79 of the Act.</td>
</tr>
<tr>
<td>Inter-State Generating Station (ISGS)</td>
<td>A Central/other generating station in which two or more states have shares and whose despatch scheduling is to be coordinated by the RLDC.</td>
</tr>
<tr>
<td>Inter State Transmission System (ISTS)</td>
<td>Inter-State Transmission System includes i) any system for the conveyance of electricity by means of a main transmission line from the territory of one State to another State ii) The conveyance of energy across the territory of an intervening State as well as conveyance within the State which is incidental to such inter-state transmission of energy (iii) The transmission of electricity within the territory of State on a system built, owned, operated, maintained or controlled by CTU.</td>
</tr>
<tr>
<td>Licensee</td>
<td>Licensee means a person who has been granted a licence under Section 14 of the Act.</td>
</tr>
<tr>
<td>Load</td>
<td>The MW/MWH consumed by a utility/ installation.</td>
</tr>
<tr>
<td>Long-term customer</td>
<td>A person availing or intending to avail access to the ISTS for a period of 25 years or more and who has signed BPTA with the transmission licensee.</td>
</tr>
<tr>
<td>Maximum Continuous Rating (MCR)</td>
<td>The normal rated full load MW output capacity of a Generating Unit which can be sustained on a continuous basis at specified conditions.</td>
</tr>
<tr>
<td>Net Drawl Schedule</td>
<td>The drawl schedule of a beneficiary after deducting the apportioned transmission losses (estimated).</td>
</tr>
<tr>
<td>Operation</td>
<td>A scheduled or planned action relating to the operation of a System.</td>
</tr>
<tr>
<td>Operation Co-ordination Committee (OCC)</td>
<td>A committee of RPC with members from all the Constituents which decides the operational aspects of the Regional Grid.</td>
</tr>
<tr>
<td>Operating range</td>
<td>The operating range of frequency and voltage as specified under the Operating Code (Chapter-6) of IEGC.</td>
</tr>
<tr>
<td>Pool Account</td>
<td>Regional account for</td>
</tr>
</tbody>
</table>
(i) payments regarding unscheduled interchanges (UI Account) or
(ii) reactive energy exchanges (Reactive Energy Account), as the case
may be

POWERGRID Power Grid Corporation of India Limited which has been notified as
CTU.

Power System Power System means all aspects of generation, transmission,
distribution and supply of electricity and includes one or more of the
following, namely:
(a) generating stations;
(b) transmission or main sub transmission lines;
(c) sub-stations;
(d) tie-lines;
(e) load despatch activities;
(f) mains or distribution mains;
(g) electric supply lines;
(h) overhead lines;
(i) service lines;
(j) works.

Reactor An electrical facility specifically designed to absorb Reactive Power.

Regional Energy Account (REA) A Regional Energy Account, for the billing and settlement of ‘Capacity
Charge’, ‘Energy Charge’, ‘UI Charge’ and ‘Reactive Charge’.

Regional Grid The entire synchronously connected electric power network of the
concerned Region, comprising of ISTS, ISGS and intra-state systems.

Regional Load Despatch Centre (RLDC) ‘Regional Load Despatch Centre’ means the Centre established under
sub-section (1) of Section 27 of the Act.

Share Percentage Share of a beneficiary in an ISGS notified by Government of India or as
agreed to in the agreement between ISGS and its beneficiaries

Single Line Diagram (SLD) Diagrams which are a schematic representation of the HV/EHV
apparatus and the connections to all external circuits at a Connection
Point incorporating its numbering nomenclature and labelling.

Spinning Reserve Part loaded generating capacity with some reserve margin that is
synchronized to the system and is ready to provide increased
generation at short notice pursuant to Despatch instruction or
instantaneously in response to a frequency drop.

SEB The State Electricity Board including the State Electricity Department.
SERC State Electricity Regulatory Commission
SSNNL Sardar Sarover Narmada Nigam Ltd.
State Load Despatch Centre(SLDC) ‘State Load Despatch Centre’ means the Centre established under
subsection of Section 31 of the Act.
State Transmission Utility (STU) ‘State Transmission Utility’ means the Board or the Government
Company specified as such by the State Government under sub-section
(1) of Section 39 of the Act.
<table>
<thead>
<tr>
<th>Static VAR Compensator (SVC)</th>
<th>An electrical facility designed for the purpose of generating or absorbing Reactive Power.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Block</td>
<td>Block of 15 minutes each for which Special Energy Meters record specified electrical parameters and quantities with first time block starting at 00.00 Hrs.</td>
</tr>
<tr>
<td>Transmission License</td>
<td>A License granted under Section 14 of the Act to transmit electricity.</td>
</tr>
<tr>
<td>Transmission Planning Criteria</td>
<td>The policy, standards and guidelines issued by the CEA for the planning and design of the Transmission System.</td>
</tr>
<tr>
<td>User</td>
<td>A term utilized in the various sections of the IEGC to refer to the persons/agencies using the ISTS, as more particularly identified in each section of the IEGC.</td>
</tr>
</tbody>
</table>
4. CONTEXT OF THE ORGANIZATION

4.1 UNDERSTANDING THE ORGANIZATION AND ITS CONTEXT

Based on mandate of the organization [see section 0.1 footnote 1], its strategic direction and that affect its ability to achieve the intended result(s) of its IMS, the external and internal issues\(^5\) have been determined that is relevant to its purpose.

A. Issues external to POSOCO:

- Compliance to requirements (i.e., rules and regulations) stipulated by statutory and regulating agencies (both at Local and National Government level) viz., IEGC, IE Act, IPR Act, Orders and Regulations passed by CERC, CEA, etc.
  - POSOCO have developed necessary mechanism for identifying and accessing the legal and other requirements which are applicable as well as which may become applicable as a result of new legislation/or amendment of existing Acts/Rules. Mapping of applicable legal requirements [see Annexure-02] and processes is done as and when there is a change in the process.
  - Having a MOU with POWERGRID for monitoring various performance parameters, including customer satisfaction, throughout the year at regular intervals.
- Services under ‘Right to Information Act’ is provided to those who apply for getting the information by approaching appropriate authorities of the concerned area.
- Handling of citizen grievances and taking suggestion/feedback to improve POSOCO’s activities and efficiency.

B. Issues internal to POSOCO:

- Governance, POSOCO structure, roles and accountabilities. This includes:
  - Policies, objectives and the strategies that are in place to achieve them,
  - Capabilities, understood in terms of resources and knowledge and competence (e.g., capital, time, people, processes, systems and technologies)

\(^5\) External issues (or context) are external environment in which the organization seeks to achieve its objectives. External context includes:

1) the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
2) key drivers and trends having impact on the objectives of the organization; and
3) relationships with, and perceptions and values of external stakeholders.

Internal issues (or context) are internal environment in which the organization seeks to achieve its objectives. Internal context includes:

1) governance, organizational structure, roles and accountabilities;
2) policies, objectives, and the strategies that are in place to achieve them;
3) the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
4) information systems, information flows and decision-making processes (both formal and informal);
5) relationships with, and perceptions and values of, internal stakeholders;
6) the organization's culture;
7) standards, guidelines and models adopted by the organization; and
8) form and extent of contractual relationships.
o Information systems, information flows and decision-making processes (both formal and informal).
  • Using IT for automation of operations (to the extent possible) to achieve efficiency.
  • The departments of POSOCO units have developed procedures to capture discrepancies with respect to data/information flow with the customers and address the same for timely mitigation.

• Training related aspects for skill development and competency building.

• Relationship with, and perception and values of, internal stakeholders. This includes:
  o The relevant departments of POSOCO units having developed procedures for ensuring pertinent information is communicated to and from employees and interested parties with regard to IMS issues.
  o POSOCO’s culture.
  o Standards, guidelines and models adopted by POSOCO.

• The form and extent of contractual relationship and identifying key interfaces between systems, potential conflicts that may arise and a process for resolving them.

The annual plans and long-term plans are made to address these issues. Accordingly, the IMS at POSOCO is implemented and its effectiveness maintained in accordance with integrated MSS requirements of ISO 9001:2015 / ISO 14001:2015 / ISO 45001:2018 / ISO 27001:2013 and applicable legal and other requirements [refer IMS-02: SOPs – Chapter 5: Identification of Legal and Other Requirements].

4.2 UNDERSTANDING THE NEEDS AND EXPECTATIONS OF INTERESTED PARTIES

The interested parties and their needs & expectations determined by POSOCO that are relevant to the IMS have been identified – refer IMS-02: SOPs – Chapter 2 for details.

The IMS is designed to continuously monitor & address these needs and expectations.

4.3 DETERMINING THE SCOPE OF IMS

Based on the internal and external issues [see 4.1], the needs and expectations of its interested parties [see 4.2], and the products / services it provides [see footnote #1 in section 0.1], the Scope Statement for Certification at POSOCO has been identified –


The scope of IMS allows ‘Risks and Opportunities’ and ‘Business Planning’ to be determined, which forms the basis of POSOCO’s Business [see footnote #4 in section 0.1].

Following is the scope statement for the IMS consisting of ISO 9001:2015 (QMS), ISO 14001:2015 (EMS), ISO 45001:2018 (OH&SMS) and ISO 27001:2013 (ISMS) for POSOCO:

Integrated Operation and Control of Indian Electricity Grid including transnational exchange of Power through National and Regional Load Despatch Centres, involving System operation, Market operation, Logistics, Operation & Maintenance of Supervisory Control, Data Acquisition (SCADA) / Energy Management System (EnMS), Establishment functions and other tasks entrusted by the Ministry of Power, Govt. of India and Central Electricity Regulation Commission.

<table>
<thead>
<tr>
<th>ISO Standard</th>
<th>Exclusion/s</th>
</tr>
</thead>
</table>
| ISO 9001:2015 (QMS)|  • Clause 8.5.1(f) – Control of production and service provision (point f)  
JUSTIFICATION: Output of all processes can be verified prior to delivery and hence validation of processes is not required.  
• Clause 8.5.3 – Property belonging to customers or external providers  
JUSTIFICATION: There are no property of customer or external provider that requires care while it is under POSOCO’s control or being used by POSOCO for delivering its products and services. |
| ISO 14001:2015 (EMS)|  • Nil, all clauses are applicable. |
| ISO 45001:2018 (OH&SMS)|  • Nil, all clauses are applicable. |
| ISO 27001:2013 (ISMS)|  • Controls identified in SoA (Statement of Applicability) viz.,  
Control 6.2.2 Teleworking  
Control 10.1.1 Policy on use of cryptographic controls  
Control 10.1.2 Key Management  
Control 14.1.2 Securing application services on public networks  
Control 14.1.3 Protecting application services transactions  
Control 14.2.1 Secure development policy  
Control 14.2.5 Secure system engineering principles  
Control 14.2.6 Secure development environment  
Control 18.1.5 Regulation of cryptographic controls  

 Refer IMS-01-Anx1: Statement of Applicability (SoA) document for JUSTIFICATION.
4.4 THE “INTEGRATED MANAGEMENT SYSTEM”

The IMS at POSOCO is based on the process approach where the inputs, controls and outputs are determined and the interrelation between various processes of system operations are identified and maintained involving various departments to provide products and services to its customers by complying to the management system control procedures and using the P-D-C-A (Plan-Do-Check-Act) approach for continual improvement to its quality, environment, health & safety and information security performance.

4.4.1 POSOCO WORKING STRUCTURE

POSOCO works on rules and regulations stipulated by Statutory & Regulatory Agencies and instructions received from Min. of Power. The main objective of POSOCO’s working is to monitor the performance and efficiency of working of the electrical grids (comprising power generation / transmission / distribution etc. companies) in India divided into 5 grids viz., North, West, South, East, and North-East.
- Customers of POSOCO are Users of Electrical Grid as identified by CERC directives.
- Products and Services of POSOCO comprises of ensuring Integrated Operation of Regional and National Power Systems to facilitate transfer of electric power within and across the regions and trans-national exchange of power with reliability, security and economy.

Diagram below depicts the ‘business’ department inter-relationships and the functional processes at POSOCO:
4.4.2 THE IMS AT POSOCO

The EMS – OH&SMS – ISMS aspects are embedded into the QMS aspects of process approach and risk management mechanism to establish the IMS at POSOCO with specific requirements of QMS – EMS – OH&SMS – ISMS addressed appropriately.

The purpose of respective QMS – EMS – OH&SMS – ISMS international standards are briefly given below:

- **ISO 9001:2015 Quality Management System (QMS)**
  
The ISO 9001:2015 international standard for quality management system employs the:
  
  - process approach, which incorporates the PDCA (Plan-Do-Check-Act) cycle; and
  - risk-based thinking

  with an aim to meet customer requirements and enhance customer satisfaction.

  The **process approach** enables an organization to plan its processes and their interactions. Within this, the PDCA cycle enables an organization to ensure that its processes are adequately

---

Document Classification: INTERNAL
resourced and managed, and that opportunities for improvement are determined and acted on. Thus, the approach enables the organization to control the interrelationships and interdependencies among processes of the system so that the overall performance of the organization can be enhanced.

The **risk-based thinking** enables an organization to determine the factors that could cause its processes and its QMS to deviate from the planned results. Hence, it emphasizes to put in place preventive controls to minimize negative effects and to maximize use of opportunities as they arise. While doing this, the external and internal issues of the organization are determined taking into account the customer and applicable statutory and regulatory requirements to understand the needs and expectations of interested parties.

- **QMS risk-based thinking** involves identifying process risks and opportunities that has the potential to impact the delivery of organization’s products and services and/or the customer satisfaction.

- **ISO 14001:2015 Environment Management System (EMS)**
  The ISO 14001:2015 international standard for environment management system provides a framework for sustainable development and social responsibility of an organization with focus on organization’s commitment to proactive initiatives to protect the environment, and further, the organization shall extend its control and influence on the environmental impacts associated with product use and end-of-life treatment or disposal (i.e., the lifecycle perspective).

  - The environmental risk assessment and treatment comprises of environmental aspects (Cause) and environmental impacts (Effect), known as Aspect-Impact, and is integrated to the process risks and opportunities identified through the QMS risk-based thinking.

  The ISO 45001:2018 international standard for occupational health and safety management system deals with the organization’s responsibility for the occupational health and safety aspects of its employees (staff and workers) and others who can be affected by its activities by promoting and protecting their physical and mental health. The primary aim of organization is to prevent work-related injury and ill-health to workers and to provide safe and healthy workplace.

  - The OH&S risk assessment comprises of hazard identification and risk analysis, known as HIRA, and is integrated to the process risks and opportunities identified through the QMS risk-based thinking.

  The ISO 27001:2013 international standard for information security management system provides a framework for secure information by ensuring Confidentiality – Integrity – Availability (CIA) tripod, where information includes both paper-based and electronic form as well as information processing facilities, including how the information is processed / stored / transferred / archived / destroyed. Information Security (or, InfoSec in short) aims to provide management with an assurance mechanism regarding security of its business information from potential security breach.

  - The InfoSec risk assessment is integrated to the process risks and opportunities identified through the QMS risk-based thinking.
The ISMS standard recommends in its Annexure-A having 14 domains divided into 35 control objectives and each control objective having 1 or more controls thus making a total of 114 controls.
4.4.3 SEQUENCE AND INTERACTION OF PROCESSES

Interested Parties
(Regulators – CERC & CEA, Min. of Power, State Power Boards and Regional Power Committees)

Customers
(Users of Electric Grid as per CERC directives)

The POSOCO Business
Core to the Business
SCADA
Customer facing
IT

Business enabling
System Operation (or, Grid Management)
Market Operation
Technical (or, Auxiliary) Services

Business support
Corporate Planning
Renewable Energy
Legal

External Providers
(Registrars, Service Providers, Consultants, etc.)

Company Secretary
Finance

External Providers
Regulatory Cell
Contracts

4.4.3 SEQUENCE AND INTERACTION OF PROCESSES

Customers
(Users of Electric Grid as per CERC directives)

Interested Parties
(Regulators – CERC & CEA, Min. of Power, State Power Boards and Regional Power Committees)

Market Operation
System Operation (or, Grid Management)

The POSOCO Business

Core to the Business
SCADA
Customer facing
IT

Business enabling

External Providers
(Registrars, Service Providers, Consultants, etc.)

Company Secretary
Finance

Regulatory Cell
Contracts

Legal
HR & Admin
Renewable Energy

Document Classification: INTERNAL
(a) POSOCO has determined the criteria and methods needed to ensure that both the operation and control of these processes are effective;

(b) POSOCO has ensured the availability of resources and information necessary to support the operation and monitoring of these processes;

(c) POSOCO has systems in place to monitor, measure, analyze these processes and implement actions necessary to achieve planned results and continual improvement of the organization’s overall performance; and

(d) There are adequate controls on outsourced activities; POSOCO has not outsourced any core activity related to its operations. The extent of controls is based on the impact of the outsourced activity on quality, environment, health & safety and information security. These controls are defined by HODs considering applicable legal requirements and POSOCO policies.
5. LEADERSHIP

5.1 LEADERSHIP AND COMMITMENT

For IMS purposes, CMD, POSOCO, is the ‘Top Management’. The CMD is supported by Board of Directors and Functional Heads (HOD’s) in reviewing the health of the IMS and take IMS improvement decisions.

The top management has demonstrated its leadership and commitment to the IMS through following actions:

- Adequate integration of the IMS requirements in to the organization’s business processes by considering all the requirements of Quality / Environment / Health & Safety / Information Security MSS while establishing the documentation of IMS.
- Ensuring adequate resources are provided for the IMS implementation by nominating Corporate Management Representative (CMR) and formation of relevant teams [see 5.3.1] to implement the Quality / Environment / Health & Safety / Information Security MSS requirements.
- Setting of IMS Objectives [see 6.2] comprising Quality / Environment / Health & Safety / Information Security aspects and periodically reviewing the achievement of the intended outcomes (objectives) by performing management reviews [see 9.3]; directing and supporting to contribute towards the effectiveness of IMS and promoting continual improvement of processes and practices in line with IMS requirements.
- Promote understanding and implementation of IMS through training [see 7.2 and 7.3].
- Supporting other relevant management roles to demonstrate leadership as it applies to areas of their responsibility such as:
  o Directing and supporting the persons to contribute to the effectiveness of IMS
  o Ensuring that the IMS achieves its intended Outcomes
  o Promoting continual improvement

5.1.1 CUSTOMER FOCUS

[Specific to ISO 9001:2015 Clause 5.1.2]

Meeting customer requirements and ensuring enhancing customer satisfaction is of utmost importance to POSOCO at all levels of its operations. The customer perspective typically includes:

- Monitoring of various performance parameters of POWER GRID throughout the year at regular intervals in accordance to MOU signed between POSOCO and Management of POWER GRID.
- POSOCO departments which have direct customer interface regularly interact with the external customer to understand their requirements and obtain customer satisfaction data [see 9.1.2]
for analysis. Procedures are in place to capture discrepancies with respect to data/information flow with the customers and address the same for timely mitigation.

- Relevant departments of POSOCO units ensure pertinent information is communicated to and from employees and interested parties with regard to IMS issues.

These are elaborate arrangements to ensure ‘customer requirements’ are met.

5.2 POLICY

Following is the IMS Policy Statement adopted by POSOCO:

**INTEGRATED MANAGEMENT SYSTEM POLICY OF POSOCO**

We are committed to:

- Ensure reliable and integrated power system operation in an efficient and effective manner, with safety, security and optimal utilization of national resources, in conformity to legal and regulatory provisions deploying latest technologies.
- Facilitate and promote environment friendly technologies.
- Ensure safe, occupational hazard free and healthy work environment.
- Continually improve our IMS to enhance quality of our services, security of information assets, and control of pollution, reduce environmental impact of our activities & services, and improve our OH&S performance.
- Compliance of all applicable legal and regulatory requirements relating to all four standards (QMS/EMS/OHSMS/ISMS)

This policy will be reviewed annually and be made available to the public and all other stakeholders, viz. Our Customers, Our Employees, Our Suppliers and shareholders of POSOCO.

(K.V.S. Baba)
CMD (POSOCO)
Date:

The IMS Policy statement is available as a documented information throughout POSOCO offices as a means of communication and understood by all. Further, it provides a framework for establishing and reviewing IMS objectives.

5.3 ORGANIZATIONAL ROLES, RESPONSIBILITIES AND AUTHORITIES

The organization structure for Unit is defined by unit head. The top management of unit supports the continual improvement in its IMS performance, to achieve various set objectives. Top management is
committed to provide required resources and guide employees to excel in their roles. Key process indicators for each department related to service quality are defined by unit head and are communicated to HODs.

The unit organization chart is available on the website of the respective RLDC/NLDC.

Top management has appointed a Corporate Management Representative to implement and operate IMS at all locations of POSOCO through respective unit MR. MRs appraises top management of their unit and CMD about performance of IMS regularly through Corporate MR in conjunction with Unit Head.

The Information Security Management Forum (ISMF) of POSOCO includes representation of RLDCs/NLDC and is responsible for the establishment, implementation, operation, monitoring, review, maintenance and improvement of Information Security Management System (ISMS) at POSOCO.

The unit CISO is appointed by the POSOCO’s ISMF which is represented by the unit heads and unit MRs.

---

Refer Annexure-01 for Responsibilities & Authorities
MRs ensure all employees of POSOCO understand the importance of their roles in IMS establishment, implementation and maintenance and take responsibility of aspects of Quality and HSSE in their work areas.

The responsibility and authority for product & service related activities are released by the management of the unit through key performance indicators for individual process and office circulars. These KPIs are uploaded in the ekpi portal and updated by respective departments / functions.

Authority and competency requirements for all posts in the organization structure are documented in Corporate HR policy. HSSE Committee is constituted in each Unit comprising of HODs of all Departments to look into the Health, Security, Safety and Environmental matters. HSSE Committee Leader is the unit MR.

Effective measures are taken to ensure everyone at POSOCO knows their individual and collective responsibilities.

5.3.1 CONSULTATION AND PARTICIPATION OF WORKERS

[Specific to ISO 45001:2018 Clause 5.4]

As per ISO 45001:2018, the term “Worker” means “person performing work or work-related activities that are under the control of the organization”. Hence, all managerial and non-managerial staff can be termed as ‘Worker’ in POSOCO.

POSOCO has established a mechanism, through worker representation, for consultation and participation (involvement) of workers at all applicable levels and functions in the development, planning, implementation, performance evaluation and actions for improvement in the OH&SMS.

Emphasising the consultation and participation of workers is intended to apply to persons carrying out the work activities who are impacted by work activities or other factors in the organization.

Training on OH&S aspects to workers at periodic intervals is provided with an aim that people understand hazards and risks related to OH&S aspects, understand measures they need to adopt to ensure safety at workplace and avoid work-related incidents, etc.
6. PLANNING

IMS planning involves addressing three (3) aspects, namely:

1) Identification of risks and opportunities having potential to:
   a. Impact the product/service delivery and/or customer satisfaction (the QMS risks);
   b. Significant environmental impacts (the EMS risks), taking into account:
      i. Environmental aspects of its activities, products and services that it can control and those that it can influence, considering a lifecycle perspective;
      ii. Abnormal conditions and reasonably foreseeable emergency situations; and
      iii. The compliance obligations that it must meet.
   c. Impact the health and safety of employees (both managerial staff and non-managerial workers) at workplace (the OH&SMS risks, taking into account identification of:
      i. Hazards;
      ii. OH&S risks and opportunities; and
      iii. Legal and other requirements it has to meet.
   d. Determine loss / compromise / unavailability of information and gaps / weaknesses determined against controls defined in Annex-A of ISO 27001:2013 (the ISMS risks);

   and accordingly having mitigation strategy(ies) in place.

2) Setting of objectives (encompassing quality – environment – health & safety – information security) – and these are monitored for achievement and necessary improvement actions.

3) Planning of changes to Business Processes (which becomes part of the deployed QMS) resulting into relooking / reviewing the associated EMS / OH&SMS / ISMS risks & opportunities and the procedures / policies / processes for any updating.

6.1. ACTIONS TO ADDRESS RISKS AND OPPORTUNITIES

While planning for IMS, POSOCO has considered:

- The Internal and external issues identified in section 4.1 above; and
- Needs and expectations of interested parties identified in section 4.2 above

And accordingly, has developed a mechanism to identify risk and opportunity that needs to be addressed to

(a) Assure IMS in place can achieve intended outcome;
(b) Prevent, or reduce undesired effects;
(c) Enhance desirable effects; and
(d) Achieve continual improvement.
A documented guideline has been established to identify and evaluate the QMS / ISMS risks, EMS aspect Impact, and OH&SMS HIRA resulting into establishing and maintaining an integrated risk sheet. Refer documents:

- IMS-02: Standard Operating Procedure (SOP) – Chapter 1: Risk Assessment Methodology
- IMS-01-Anx4: Integrated Risk Sheet

### 6.1.1 COMPLIANCE OBLIGATIONS

**[Specific to ISO 14001:2015 Clause 6.1.3]**

POSOCO has determined and have access to the compliance obligations like applicable legal, operational, interested party requirements related to environmental aspects.

POSOCO has determined how these compliance obligations apply to the organization through HSSE Committee meetings or participation and consultation process.

POSOCO maintains documented information of its compliance obligations as applicable.

### 6.1.2 DETERMINATION OF LEGAL AND OTHER REQUIREMENTS

**[Specific to ISO 45001:2018 Clause 6.1.3]**

POSOCO has determined and have access to up-to-date legal requirements and other requirements that are applicable to its hazards, OH&S risks and the OH&S management system.

POSOCO has determined how these legal requirements and other requirements apply to the organization and what needs to be communicated through HSSE Committee meetings.

POSOCO maintains documented information of its legal requirements and other requirements as applicable.

### 6.1.3 INTEGRATED RISK MANAGEMENT


POSOCO has established an integrated risk management framework encompassing quality – environment – health & safety – information security risk assessment and mitigation.

Refer documents:

- IMS-02: Standard Operating Procedure (SOP) – Chapter 1: Risk Assessment Methodology
- IMS-01-Anx4: Integrated Risk Sheet

For InfoSec risks, based on applicable controls drawn from Annex-A of ISO 27001:2013, POSOCO has established a **Statement of Applicability (SoA) (IMS-01-Anx1)** document.
6.2 IMS OBJECTIVES AND PLANNING TO ACHIEVE THEM

Measurable objectives of POSOCO have been established comprising quality (ISO 9001) / environment (ISO 14001) / health and safety (ISO 45001) / information security (ISO 27001) aspects and for its performance monitoring POSOCO has established the Key Performance Indicators (KPI’s) to each objective.

The objectives, along with detailed activity programme through KPI’s, have been issued by the Corporate MR and communicated to unit MRs / CISOs / Unit Heads respectively, which in turn have been further communicated to all the employees.

Refer IMS-01-Anx3: IMS Objectives and Achieving via Key Performance Indicators (KPIs) document.

The IMS objectives are linked to the IMS Policy statement.

When planning how to achieve these objectives, POSOCO has developed a programme by denoting what, who, when, how and what resource requirements needed to achieve each milestone to ultimately meet the defined objectives. These objectives and programmes are based on significant environmental aspects, health and safety hazards, business risks, information security risks and the IMS Policy, other applicable requirement and commitment to continual improvement of POSOCO processes.

A detailed program is planned for each KPI with targets, accountabilities, monitoring frequencies and reporting structure established by POSOCO. The results of KPIs are presented every half yearly for Management’s collective review to enhance the performance of POSOCO’s service provision. The KPIs will also lead to showcase the internal and external co-ordinated activities with defined controls as targets and measurement matrices to achieve the intended results.

Adequate resources are provided and the tracking and monitoring of progress on these objectives is done by unit heads on six monthly bases and reviewed for adequacy during management reviews.

Progress on objectives and its targets are reviewed in MRCM meetings every six months.

In case of new technology /project or a change in aspects due to change in legal or other requirements, existing objectives and programmes has to be reviewed and revised to meet the changed requirements.

Due consideration is also given to customer requirements and changes in the demands while setting and updating its IMS objectives.

6.3 PLANNING OF CHANGES

[Specific to ISO 9001:2015 Clause 6.3]

Changes to POSOCO’s Operational Procedures and Processes are done in controlled manner. Following aspects are considered:
(1) The purpose of the changes and their potential consequences;
(2) The integrity of the quality management system;
(3) The availability of resources; and
(4) The allocation or reallocation of responsibilities and authorities.

The changes are reviewed by CMR and approved by CMD. The changes to documentation are maintained in document revision history.
7. SUPPORT

7.1. RESOURCES

POSOCO has determined and provided necessary resources to accomplish the IMS standard requirements which are needed to implement, maintain and continually improve the efficiency and effectiveness of IMS system in place.

Resources are listed, documented and updated in the form of Assets for InfoSec purposes.

Identification of resources required for individual unit is done by HODs and it is reviewed in MRCMs and sanctioned by unit head. Resource is projected for 5-year time block for regulatory approval and implementation.

7.1.1. PEOPLE

[Specific to ISO 9001:2015 Clause 7.1.2]

POSOCO determines and provides manpower as defined under provisions of relevant regulation for effective implementation of its IMS system and for the operation and control of its operational procedures and processes by framing a Competency Matrix (IMS-01-Anx2) that specify the education, knowledge and skills required to carry out the work at different levels.

➔ Information Security aspects [ISO 27001:2013 Clause 7.1]

Information Security Controls specified under Control A.7 (Human resource security) have been embedded within POSOCO’s human resource department functioning as well as contract department functioning and includes:

❖ Prior to employment (Control Objective A.7.1)

Purpose: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

Includes: Controls related to screening / background verification checks done in accordance to laws, regulations and ethics and proportional to business requirements, terms and conditions of employment / contractual agreements stating their and organization’s responsibilities for information security.

❖ Disciplinary process (Control A.7.2.3)

➔ Control Objective A.7.2 (During Employment) is partially applied here and other controls under section 7.2 and section 7.3 of this manual.

Purpose: To take actions against employees who have committed any information security breach.

Includes: A formal disciplinary process in place and communicated to all employees.

❖ Termination and change of employment (Control Objective A.7.3)

Purpose: To protect the organization’s interests as part of the process of changing or terminating employment.
Includes: Controls related to validity of information security responsibilities and duties for a predefined period after termination or change of employment and the same being communicated to employee or contractor and is enforced.

7.1.2 INFRASTRUCTURE

[Specific to ISO 9001:2015 Clause 7.1.3]

The infrastructure needed to achieve conformity to service requirements, environment & health and safety and information security concerns are determined by the respective HODs. POSOCO management after ascertaining the needs takes necessary action to provide the infrastructure.

The infrastructure includes buildings, workspace, computers, intranet/internet facilities, cafeteria, utilities, process equipment’s, test and measuring equipment’s, software, transport and communication.

The support services needed (where appropriate) for maintenance of the infrastructure are planned by the concerned departments of each unit.

All process equipment’s are replaced as per depreciation given as per RLDC fee & charges regulations.

7.1.3 WORK ENVIRONMENT

[Specific to ISO 9001:2015 Cl. 7.1.4, ISO 14001:2015 Cl. 7.1, ISO 45001:2018 Cl. 7.1, ISO 27001:2013 Cl. 7.1]

A suitable work environment is a combination of human and physical factors.

➔ Environment for the Operation of Processes [ISO 9001:2015 Clause 7.1.4]

For the environment necessary for the operation of processes and to achieve conformity of its products and services, emphasis is given to physical factors such as maintain temperature, heat, humidity, light, airflow, hygiene, noise which are conducive to work, as well as ensuring social (e.g., calm, non-confrontational, etc.) and psychological (e.g., stress-reducing, etc.) factors at work.


POSOCO has ensured taking care of environmental issues as well as health hazard & work safety factors in its work areas. Ergonomics are considered while deciding desks, chairs and other office infrastructure. A special emphasis is given while designing control room work environment. The parameters related work environments are monitored on a regular basis where applicable and the records are maintained in the department.

➔ Information Security aspects [ISO 27001:2013 Clause 7.1]

Information Security Controls specified under Control A.11 (Physical and environmental security) have been embedded within POSOCO’s work environment and includes:

✓ Secure Areas (Control A.11.1)

Purpose: To prevent unauthorized physical access, damage and interference to the organization’s information and information processing facilities.
Includes: Controls related to physical security perimeter, physical entry, securing offices / rooms and facilities, delivery and loading areas, etc.

Equipment (Control A.11.2)

Purpose: To prevent loss, damage, theft or compromise of assets and interruption to the organization’s operations.

Includes: Controls related to equipment siting / protection and maintenance, supporting utilities (e.g., power fluctuations), cabling security (i.e., power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage), asset removal and security off-premises, secure disposal or reuse of equipment, etc. as well as enforcing policy on clear desk and clear screen.

7.1.4 MONITORING AND MEASURING

[Specific to ISO 9001:2015 Clause 7.1.5, ISO 27001:2013 Control objective A.12.4 (Logging & monitoring)]

General [ISO 9001:2015 Clause 7.1.5.1]

POSOCO has determined and provided the resources needed to ensure valid and reliable results when monitoring or measurement is used to verify the conformity of services to requirements.

POSOCO has ensured that the resources provided:

a) Are suitable for the specific type of monitoring and measurement activities being undertaken;

b) Are maintained to ensure their continuing fitness for their purpose

POSOCO has retained appropriate documented information as evidence of fitness for purpose of monitoring and measurement resources.

Measurement Traceability [ISO 9001:2015 Clause 7.1.5.2]

When measurement traceability is a requirement or is considered by the organization to be an essential part of providing confidence in the validity of measurement results. Measuring equipment will be:

a) Calibrated or verified, or both, at specified intervals, or prior to use, against measurement standards traceable to international or national measurement standards; when no such standards exist, the basis used for calibration or verification are retained as documented information.

b) Identified in order to determine their status;

c) Safeguarded from adjustments, damage or deterioration that would invalidate the calibration status and subsequent measurement results.

POSOCO has determined if the validity of previous measurement results has been adversely affected when measuring equipment is found to be unfit for its intended purpose and shall take appropriate action as necessary.
→ **Logging and Monitoring**  [ISO 27001:2013 Control Objective A.12.4]

Controls stipulate recording event logs of user activities including system administrator and system operator, exceptions, faults as well as reviewing regularly. The logging facilities and log information shall be protected against tampering and unauthorized access. Clocks of all information processing systems within the organization or the security domain shall be synchronized to a single reference time source.

### 7.1.5 ORGANISATIONAL KNOWLEDGE

**[Specific to ISO 9001:2015 Clause 7.1.6]**

POSOCO has determined the knowledge necessary for the operation of its processes and to achieve conformity of services. This knowledge has been maintained and made available to the extent necessary. When addressing changing needs and trends, POSOCO has considered its current knowledge and has determined how to acquire or access any necessary additional knowledge and required updates.

### 7.2 COMPETENCE

POSOCO has established through its HR policies appropriate competence requirements and selection criteria to ensure people are hired / recruited on basis of appropriate education, skills and experience relevant to the job they perform.

Further, during their employment, POSOCO HR dept. ensures essential professional skills are provided to staff through periodic capacity building / training programmes to enhance their skills relevant to their job.

→ **Information Security aspects**  [ISO 27001:2013 Clause 7.1]

Information Security Control A.7.2.1 (related to security aspects of employees during employment) specified under Control Objective A.7.2 have been embedded within POSOCO’s human resource department functioning as well as contract department functioning and includes:

- **Management responsibilities (Control A.7.2.1)**
  
  All employees and contractors are required to apply information security in accordance to established policies and procedures of the organization.


### 7.3 AWARENESS


New joinees are provided awareness on IMS as part of their induction process.
All staff need to mandatorily undergo trainings and re-trainings on IMS awareness at periodic intervals to ensure they understand the requirements of the ISO 9001:2015 (QMS) / ISO 14001:2015 (EMS) / ISO 45001:2018 (OH&SMS) / ISO 27001:2013 (ISMS) standards and appropriately implement in their respective work areas.

⇒ Information Security aspects [ISO 27001:2013 Clause 7.1]

Information Security Control A.7.2.2 (related to information security awareness, education and training during employment) specified under Control Objective A.7.2 have been embedded within POSOCO’s human resource department functioning as well as contract department functioning and includes:

▪ Information security awareness, education and training (Control A.7.2.2)
  All employees and relevant contractors receive appropriate awareness education and training and regular updates of organizational policies and procedures relevant to their job function.


7.4 COMMUNICATION

The relevant internal and external communication is maintained at POSOCO and is given below. POSOCO ensures the method of communication and language used is appropriate to the needs of the workforce and in a form that they can easily understand the information being provided to them.

⇒ Internal Communications
  • IMS-led communication: The documented IMS is made available to all personnel through intranet system (portal) and changes / updates are communicated to all via email.
    ▪ All personnel are encouraged to access the same and make themselves familiar with it.
    ▪ Prominently displaying the IMS Policy statement within office premises.
    ▪ POSOCO ensure that objectives (KPI’s), customer expectations and information security aspects w.r.t. information sharing, storing, deletion and archival, and processing are clearly understood and applied and accordingly the processes / procedures are implemented by all in their work areas.
    ▪ Clearly understand the compliance requirements and obligations pertaining to EMS and OH&SMS so as to act accordingly.
  • Meetings and team briefings: Monthly meetings are held on predefined dates to understand operational issues, progress of work and take informed decision. Records of these meetings are maintained.
• **E-Mails**: An inter-office email facility is provided to enable better, effective and timely communication among the staff and external entities. These are treated as formal means of communications.

- **External Communications**
  - **Customer-centric**: These are carried out on basis of operational and administrative requirements, in relation to
    - Service information, enquiries, contracts or order handling and amendments.
    - Address complaints/issues reported.
    - Records of redressal communication and meetings with Customers, Stakeholders and Interested Parties is maintained and tracked to closure.
    - Obtain customer feedbacks including appreciations, media reports, etc. of customers.
  - **Supplier-centric**: These are carried out with an aim to monitor product/service procurement ease, timely payments to suppliers, etc. and areas that require intervention from concerned depts.
  - **Statutory and regulatory agencies**: Reports and other expected communications are done in a timely manner to ensure compliance with legal, statutory and regulatory requirements related to operations.
  - **Stakeholders / interested parties**: Reports and other expected communications with other stakeholders are done on routine basis and on need basis.

### 7.5 DOCUMENTED INFORMATION

Organizational information that is required is controlled and maintained as:

- Integrated Management System (IMS), which includes the Apex manual, POSOCO’s operational processes and procedures, supporting SOPs and IMS Formats required to be maintained to evidence IMS implementation;
- Evidence of results achieved (records).

The organization ensures that the documents required for the management system are:

- Periodically reviewed and changes approved prior to release;
- Identified as per its current revision status;
- Legible (i.e., adequately protected from loss of confidentiality, improper use and/or loss of integrity) and readily identifiable (i.e., relevant version of applicable document is available at points of use);
- Prevented from unintended use when obsolete (if these obsolete documents are retained for future reference then suitable identification is applied to them);
- Documents of external origin that is necessary for the planning and operation is identified; and
- Access, retrieval, use, distribution and disposition is controlled.
Documented information retained as evidence of conformity (i.e., records) are protected from unintended alterations. The identification, storage, retention, retrieval and disposition of records is controlled.

IMS documentation structure is elaborated in section 0.4 of this manual.

Refer: IMS-03: IMS Control Procedures, Chapter 1 on “Control of Documented Information” for details.
8. OPERATION

8.1 OPERATIONAL PLANNING AND CONTROL

Business inter-relationships (depicted in section 4.4.1) and POSOCO’s functional processes (depicted in section 4.4.3) of this manual ensure that POSOCO in its operations ensure requirements for the provision of products and services are met through:

(a) Determining the requirements for the products and services;
(b) Establishing criteria for the processes and acceptance of products and services;
(c) Determining the resources needed to achieve conformity to products and service requirements;
(d) Implementing control of the processes in accordance with the criteria.
   a. POSOCO shall implement and control the processes needed to meet information security requirements and to implement actions determined via section 6.1 of this manual, including plans to achieve information security objectives determined via section 6.2 of this manual.
   b. POSOCO shall ensure adapting work to workers.
(e) Maintaining and retaining documented information to the extent necessary:
   a. To have confidence that the processes have been carried out as planned.
   b. To demonstrate the conformity of products and services to their requirements.

8.1.1 MANAGEMENT OF RISK

[Specific to ISO 27001:2013 Clause 8.2 and 8.3, ISO 45001:2018 Clause 8.1.2]

Risk identification and planning to mitigate the risks is one of the key expectations of IMS to ensure business operates in a planned and controlled manner.

(a) POSOCO performs information security risk assessment at planned intervals or when significant changes are proposed or occur, taking into account the criteria established (refer: IMS-02: Standard Operating Procedure (SOP) – Chapter 1: Risk Assessment Methodology).

The information security risk treatment plans identified are implemented. Documented information of the results of information security risk assessment and risk treatment are retained for a period of at least 2 years.

(b) POSOCO ensures OH&S aspects are implemented in a controlled manner by following hierarchy:
   a. Eliminate the hazard;
   b. Substitute with less hazardous processes, operations, materials or equipment;
   c. Use engineering controls and reorganization of work;
   d. Use administrative controls, including training; and
e. Use adequate Personal Protective Equipment (PPE) – provided by POSOCO at no cost to workers.

(c) Consistent with lifecycle perspective in EMS, POSOCO:

a. Determines appropriate environmental requirements during procurement of its products and services;

b. Communicate relevant environmental requirements to external providers, including contractors;

c. Considers the need to provide information about potential significant environmental impacts associated with the transportation or delivery, use, end-of-life treatment and final disposal of its products and services.

8.1.2 CHANGE MANAGEMENT


Where deviations from planned arrangements happen, these are appropriately controlled and review of consequences of unintended changes is carried out taking into account to mitigate any adverse effects as necessary.

As regards OH&S, planned changes (whether temporary or permanent) are controlled and considers workplace locations and surroundings, working conditions, equipment, workforce, changes to legal and other requirements, knowledge or information gained about hazards and OH&S risks, and technology changes.

8.2 HANDLING CONTINGENCY SITUATION


POSOCO have developed procedures to ensure that the organization is able to respond to the accidents and foreseeable emergency and disaster situation and for preventing and mitigating the information security, environmental and OH&S impacts associated with them considering the total business risk on the organization.

After identifying the potential emergency situations and based on the past experiences, action plans have been developed to overcome the emergency. In case of occurrence of such a situation a HSSE committee is formed to analyse the risk and necessary corrective and preventive action taken to prevent its recurrence.

Wherever practicable, mock drills to check the emergency preparedness are carried out at regular intervals as per established procedures. This mock drills / business continuity plan (BCP) covers service continuity, environment, OH&S attributes and the information security check points. Risk assessment is also conducted on contract works/service provision to ensure they do not put organization at risk and whenever there is a change in organization or methods of working like organization structure, operational procedure, inclusion of new equipment etc. Before installation or implementation proper risk assessment will be conducted.

Refer: IMS-02: Standard Operating Procedures (SOPs) – Chapters:
1) **Chapter 6: Emergency Operating Procedure** → covers fire, bomb threat and terrorist attack.
2) **Chapter 7: Procedure for Emergency Preparedness and Response** → covers QMS service operations, environmental emergencies and OH&S emergencies
3) **Chapter 8: Procedure for Disaster Recovery** → covers testing of disaster recovery plans and maintaining records.

### 8.3 REQUIREMENTS FOR PRODUCTS AND SERVICES

[Specific to ISO 9001:2015 Cl. 8.2]

This involves communication with customer and determining and reviewing the requirements for products and services.

#### 8.3.1 CUSTOMER COMMUNICATION

POSOCO has determined and implemented effective arrangements for communicating with customers relating to product information. Communications with customer includes:

1) Providing information relating to products and services through various means and media such as correspondence, catalogue, website information, etc.;
2) Handling enquiries. Customers will be contacting POSOCO to seek information / clarifications related to grid operations, legal provisions, billing, etc.
3) Obtaining customer feedback relating to products and services through media reports on performance and through direct interactions. These feedbacks may be positive in form of compliments or tips and may also be negative in form of a complaint or an expression of disapproval. POSOCO has an elaborate mechanism to capture customer feedbacks (including complaints) and resolve appropriately.
4) Establishing specific requirements for contingency actions, when relevant [see 8.2].

#### 8.3.2 DETERMINING AND REVIEWING THE REQUIREMENTS FOR PRODUCTS / SERVICES

Determination of requirements for products and services includes two (2) aspects to be considered:

(a) **Explicit**: Characteristics that the product / service is required to exhibit (i.e., the product’s / service’s inherent characteristics) and its delivery requirements; and

(b) **Implicit**: Other requirements that do not relate to the products/services that may form part of customer requirements.

POSOCO ensures requirements for products and services are defined, including any applicable statutory and regulatory requirements as well as those that are considered necessary by POSOCO.

POSOCO ensures it can meet the claims for the products and services it offers by conducting a review before committing to supply products and services to customer. The review consists, at a minimum, of:

- Requirements for delivery and post-delivery activities;
- Requirements not stated by customer but necessary for the specified or intended use — supplying the product/service ensuring retaining product’s inherent properties;
- Ensuring adherence to any legal (statutory and regulatory) requirements applicable to products and services.

The review results are retained in form of documented information, including changes / amendments and ensure relevant personnel are aware of changed requirements.

8.4 DESIGN AND DEVELOPMENT

[Specific to ISO 9001:2015 Cl. 8.3 and ISO 27001:2013 Control Domain A.14 (for specific Controls see SoA)]

POSOCO software development is generally outsourced. Only minor / small development of tools and web-based application software for internal use is made by IT team. Therefore, design and development is partially applicable.

The IT team ensures software is tested functionality-wise before releasing to users. For any small application software made, the IT team at end of successfully completing the development cycle prepare Technical Specifications document that notes the purpose, methodology, front-end GUI, backend database tables / entity relationships / triggers / procedures and views created etc. with an aim for future reference.

While developing small applications, IT team ensures security aspects are taken care during design and development stage.

8.5 HANDLING PROCUREMENT OF PRODUCTS AND SERVICES


POSOCO has outsourced few of its activities which are controlled and adequately monitored, e.g.,

a) HR functions are managed by hired staff on temporary basis
b) Routine monitoring of SCADA is outsourced to various agencies (like SEIMENS, etc.).

Based on perceived risks from outsourcing, relevant degree of control and monitoring is done.

- Supplier agreements contain requirements to comply with POSOCO’s environmental, health & safety and information security policies and procedures and is agreed to be adhered by staff of such outsourced agencies.

Staff deployed by outsourced agency in IT & SCADA functions have access to POSOCO’s business information and/or information processing facilities. POSOCO has made separate arrangements to have a signed NDA (Non-Disclosure Agreement) with such agencies as part of contract.

- Agreements with suppliers includes suppliers to address risks associated with ICT (Information and Communication Technology) services and product supply chain for them to ensure supplier has adequate mechanism to handle situations in case of failure from their end-suppliers.
POSOCO ensures it applies criteria for the evaluation, selection, monitoring of performance, and reevaluation of external providers, based on their ability to provide processes or products and services in accordance with requirements.

Evaluation and selection of external providers (suppliers of products and services) are through invitation to tender that clearly stipulate the evaluation and selection criteria. Results of supplier evaluation and selection is maintained.

POSOCO has ensured the adequacy of requirements prior to their communication to external provider.

Based on the identified requirement of various materials / equipment / services, purchasing or contracting of individual packages are affected in the form of Letter of Award (LOA) or Purchase Order (PO) or Contract Agreement on the basis of the following:

a) Technical Specification: Technical Specifications covering requirements for approval of product, procedures, processes and equipment’s if any, tender drawings, tests and inspection requirements. Quality Assurance and Inspection requirements and Authorization for Despatch clearance

b) Conditions of Contract: Terms of payment, Applicable Indian/International Standards, Delivery Schedule, Obligations of POSOCO, Environment and safety aspects (if applicable), Confidentiality and non-disclosure clauses

c) Qualifying Requirement

d) Sub-vendor duly approved

In order to have consistency and transparency in procurement process, Works and Procurement Policy covering pre-award and post-award activities have been issued by Corporate Office for implementation.

Wherever necessary before authorizing Despatch of material or equipment, inspection is carried out to ensure conformance to specified requirements. It is only after ascertaining that the product meets the specified requirements that authorization for Despatch is issued to the supplier.

Once the bidder gets selected, performance monitoring of the product & service supplier is carried out. The extent of control primarily takes into consideration:

(a) The ability to consistently meet customer and applicable regulatory requirements;

(b) Determine the verification, or other activities, necessary to ensure that the externally provided processes, products and services meet requirements.

(c) Regular reviews of supplier services carried out encompassing OH&S and information security aspects;

(d) Monitoring to the extent required depending on type of outsourcing is ensured keeping in view the quality and environmental aspects needed to be adhered by staff of outsourced agency.

8.6 PRODUCTION AND SERVICE PROVISION
POSOCO is required to plan and carry out their activities under controlled conditions.

Information Security aspects is embedded into POSOCO’s working in accordance to ISMS Policies and Procedures (IMS-01-Anx4) document. POSOCO has developed security practices to ensure security of information and information processing facilities through ISMS policies and procedures which are tested at defined intervals.

POSOCO is responsible to provide real time grid operations – schedule and Despatch of electricity within and across the regions through secure and economic operation of the regional grid in accordance with grid code. Appropriate controls are deployed with due concern to security, stability, economy and efficiency of the regional grid and national grid. Quality aspects controlled by way of consideration of following factors:

- Quality of people – competence to do the job with the required proficiency.
- Quality of resources – capability of IT and SCADA systems, money, information (w.r.t. degree of accuracy / completeness / usability / validity).
- Quality of materials – adequacy of physical properties, their consistency and accuracy to ensure acceptance criteria have been met.
- Quality of measurement – units, values, timing and integrity by correctly identifying the measurements to be taken, the units of measure, the target values and when to take them and control the integrity of measurement at appropriate stages.
- Implementation of actions to prevent human error.
- Implementation of release, delivery and post-delivery activities [see 8.6 and 8.5.3].

POSOCO determines and plans activities associated with significant environmental aspects under EMS and work-related hazards and risks under OH&SMS, requiring controlled measures. Environment / health & safety aspects controlled by way of consideration of following factors:

- Physical environment – level of temperature, cleanliness, humidity, etc. need to be taken care.
- Work environment health & safety – degree of physical stress, physiological stress, motivation. It is important to identify the human factors required in the work environment.

OCP’s are applicable to specific areas and activities and it is acknowledged that absence of the same may cause deviations from the IMS policy and objectives. These OCP’s:

(i) stipulate the operating criteria;
(ii) refer to the identified EHS hazards related to goods, equipment, services and processes used by the organization, including their adaptation to human capabilities.

OCPs are communicated to suppliers, contractors and visitors whenever necessary.
Documented Operational Control Procedures (refer: IMS-02-Anx1: OCPs) are established, implemented and maintained to ensure that such activities are performed under controlled conditions. POSOCO has measures in place to control all the outsourced processes in line with IMS standard requirements. POSOCO has mechanism in place to control planned changes and unintended changes by taking action to mitigate any adverse effect as necessary. POSOCO has ensured that it manages changes in its operation to ensure that any new risk introduced are controlled.

8.6.1 IDENTIFICATION AND TRACEABILITY

[Specific to ISO 9001:2015 Cl. 8.5.2]

POSOCO uses suitable means to identify outputs when it is necessary to ensure the conformity of services.

POSOCO identifies the status of output with respect to monitoring and measurement requirements throughout the service provision.

POSOCO controls the unique identification of the output where traceability is a requirement and retains the documented information necessary to enable traceability.

8.6.2 PRESERVATION

[Specific to ISO 9001:2015 Cl. 8.5.4]

POSOCO ensures preservation of conformity of product during internal processing (procurement and products & services delivery to the intended destination through appropriate reporting and measures (accuracy and authenticity).

8.6.3 POST-DELIVERY ACTIVITIES

[Specific to ISO 9001:2015 Cl. 8.5.5]

POSOCO meets post-delivery requirements associated with its service delivery which typically include:

- Meeting the applicable statutory and regulatory requirements;
- Customer requirements and feedbacks, including complaints;
- Potential undesired consequences associated with its services;
- The use and intended lifetime of its products and services.

The primary focus during post-delivery is customer oriented wherein customers may be wanting prompt resolution to the problems / issues / concerns encountered.

8.6.4 CONTROL OF CHANGES

[Specific to ISO 9001:2015 Cl. 8.5.6]

POSOCO reviews and control changes to the extent necessary to ensure continuing conformity with requirements.
8.7 RELEASE OF PRODUCTS AND SERVICES

[Specific to ISO 9001:2015 Cl. 8.6]

Planned arrangements at appropriate stages have been implemented by POSOCO to verify that the product and service requirements have been met.

Release of products and services to Customer shall not proceed until the planned arrangements have been satisfactorily completed, unless otherwise approved by a relevant authority.

8.8 CONTROL OF NONCONFORMING OUTPUTS


POSOCO ensures that outputs that do not conform to their requirements are identified and controlled to prevent their unintended use or delivery. POSOCO takes appropriate action based on the nature of the nonconformity and its effect on the conformity of services. This shall also apply to nonconforming services detected during or after the provision of services.

POSOCO deals with nonconforming outputs in one or more of the following ways:

a) Correction;
b) Segregation, containment, return or suspension of provision of services
c) Informing the customer
d) Obtaining authorization for acceptance under concession,
e) Conformity to the requirements are verified when nonconforming outputs are corrected.

POSOCO retains documented information that

(a) Describes the nonconformity;
(b) describes the actions taken;
(c) describes any concessions obtained;
d) Identifies the authority deciding the action in respect of the nonconformity.

Refer: IMS-03: IMS Control Procedures, Chapter 5: on “Control of Non-Conforming Activity / Service” for details.
9. PERFORMANCE EVALUATION

9.1 MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION

In order to evaluate process efficiency and process effectiveness, it is essential to evaluate the process performance.

9.1.1 GENERAL

POSOCO identifies Key Performance Indicators (KPI’s) to measure and monitor its business processes for effective performance for each financial year. These KPI’s are maintained using the ekpi portal which respective departments / functions in each POSOCO location update on a quarterly basis. For the subsequent financial year, the KPI’s are reviewed with the CMD to ensure if any existing KPI may be removed and/or add new KPI’s.

Records of monitoring and measurements are maintained.

Refer: IMS-02: Standard Operating Procedures (SOPs) – Chapter 3: Procedure for Monitoring and Measurement.

9.1.2 CUSTOMER SATISFACTION

[Specific to ISO 9001:2015 Cl. 9.1.2]

Customer focus [see 5.1.1] is the primary moto of POSOCO operations. The customers for POSOCO are the users of Power System. They include SEBs, Transmission Companies, Generation Companies, Traders, Power exchanges etc.

Periodically once every 6 months, before each internal audit cycle, feedback is obtained from as many customers with whom POSOCO has dealt in the last 6 months and data is compiled to determine the trends and customer perception as to whether the organization has met the customer requirements.

Refer: IMS-04: IMS Formats,

1. Section FRM-02: RLDC Customer Feedback Form for feedbacks obtained from POSOCO customers by RLDCs
2. Section FRM-03: NLDC Customer Feedback Form for feedback obtained by NLDC from RLDCs as their internal customers.

9.1.3 EVALUATION OF COMPLIANCE

[Specific to ISO 14001:2015 Cl. 9.1.2 and ISO 45001:2018 Cl. 9.1.2]

The concerned departments of POSOCO have developed procedures to periodically evaluate compliance with applicable legal requirements as well as to the other requirements applicable to the organization. Records of such evaluations are maintained by concerned departments.

Refer: IMS-02: Standard Operating Procedures (SOPs) – Chapter 4: Procedure for Evaluation of Compliance Obligations.
9.1.4 ANALYSIS OF DATA

The data collected from internal audits, customer feedback and various monitoring points at the departmental levels, is analysed on regular basis in the meetings of the department where HOD and the departmental executives participate.

In cases, where improvements are required, corrective action teams are constituted to analyse the data and evolve possible solutions for improvements. Where appropriate, problem solving tools, trends and statistical techniques are used for analysing the data.

The analysis provides the information related to:

- Customer satisfaction
- Conformity of product/service requirements
- Characteristics of trends of processes and products including opportunity for preventive actions
- Suppliers
- Causes of accidents/near misses
- Environmental performance
- Information Security

Factors considered for analysis include the following considerations:

- Metrics obtained from process measurements is converted into information and knowledge for the organization’s benefit
- Appropriate priorities of processes are established.
- Measurement methods and indicators are reviewed periodically (normally once a year) to ensure its accuracy and completeness on a continual basis.
- Measuring customer satisfaction to evaluate organization’s performance.

The results of data analysis are used to evaluate:

- Conformity of products/services provided by POSOCO
- The degree of customer satisfaction
- The overall performance and effectiveness of the IMS deployed within POSOCO
- If operational planning has been implemented effectively
- The effectiveness of actions taken to address risks and opportunities
- The performance of external providers of services, consultancy and goods/material.

9.2 INTERNAL AUDIT

An audit of the IMS processes is done once in six (6) months to determine if the documented processes and the requirements of the Management System Standards (MSS) viz., ISO 9001:2015, ISO 14001:2015, ISO 45001:2018 and ISO 27001:2013 are being met, effectively implemented and maintained.

Trained personnel, not having direct responsibility of the activity being audited, conduct audits.
Process owners / auditee ensure that actions on detected non-conformities are taken without undue delay.

CMR along with Unit MR's maintains an internal audit plan and is responsible for scheduling, organizing and maintaining records of these audits. Results of audits and status is presented to CMD, POSOCO [see 9.3].

Refer: IMS-03: IMS Control Procedures, Chapter 2: Internal Auditing for details.

9.3 MANAGEMENT REVIEW

Review of the IMS is done once in six (6) months, generally a week after internal audit cycle covering all the functions (sections/departments) of POSOCO has been completed, with CMD wherein POSOCO discuss in accordance to set agenda points.

The results of the reviews and actions arising out of these reviews are documented and records maintained by MR for tracking and follow-up.

Refer: IMS-03: IMS Control Procedures, Chapter 4: Management Review of IMS for details.
10. IMPROVEMENT

10.1 GENERAL

Improvements taken up for discussion in MRM (Management Review Meeting) forum are primarily with a view to enhance customer satisfaction. It essentially focuses on:

- Taking corrective actions on detected non-conformities, and
- Continually improve the performance of IMS within the organization.

10.2 NONCONFORMITY AND CORRECTIVE ACTION

Handling non-conformities

POSOCO has defined the controls and related responsibilities and authorities for dealing with

- a) System operations to control nonconforming grid situations with respect to system parameters are controlled through corrections and corrective actions on real time basis.
- b) Undesired events like accidents and incidents.

Undesired events during product realization are dealt with by

- a) Taking action to mitigate or deal with the consequences arising from the event, control and correct it
- b) Resorting to corrective action, implement and review the effectiveness of any corrective action taken
- c) Maintaining records of the action taken (responsibility: observer of the event) and make changes to IMS as necessary.
- d) Reporting to the appropriate authority,

Corrective Action

In order to prevent recurrence of detected nonconformities and undesired events by eliminating their causes, the concerned process in-charge or the Environment and Safety Committee or Information Security Management Forum, as appropriate, takes corrective action commensurate with their effects. Documented procedure defines requirements for reviewing the undesired events and nonconformities (including customer complaints and determining their causes,

- a) Evaluating the need for action,
- b) Determining and implementing the action needed,
- c) Recording and reviewing the results of action.

Refer: IMS-03: IMS Control Procedures, Chapter 3: Correction and Corrective Action for details.
10.3 CONTINUAL IMPROVEMENT

POSOCO aims for continual improvement to increase the effectiveness of its Integrated Management System (IMS) through use of IMS policy, objectives, audit results, analysis of data, corrective and preventive actions and management reviews. The concerned regional heads set measurable objectives, taking into consideration the improvements needed in the processes and the services.

POSOCO is committed to observe transparency and consistency in all its operations. In order to maintain integrity & efficiency of the organization, various measures like workshops to educate the employees so that systems and procedures are adhered at every stage of service delivery. Planned & regular inspection, review of systems & procedures and rotation of manpower are done. This in turn contributes towards consistency, transparency and improvements in the functioning of POSOCO.

Top Management of POSOCO is committed to development and implementation of Integrated Management System and in continually improving its effectiveness. Various systems and procedures established under the Integrated Management System emphasize organizational commitment for meeting customer, interested parties and statutory / regulatory requirements.
ANNEXURE-01: RESPONSIBILITIES & AUTHORITIES

ANX-01-01: HSSE ROLES & RESPONSIBILITY

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Responsibility</th>
<th>Roles &amp; Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Establish overall direction, ultimate responsibility for HSSE performance</td>
<td>RLDC/NLDC Head</td>
</tr>
<tr>
<td>2</td>
<td>Develop HSSE Objectives, targets and programs</td>
<td>Corporate MR and Unit MR</td>
</tr>
<tr>
<td>3</td>
<td>Risks assessment, Operational controls, Monitoring overall HSSEMS performance</td>
<td>Respective HOD</td>
</tr>
<tr>
<td>4</td>
<td>Regulatory and other compliance</td>
<td>HSSE Manager</td>
</tr>
<tr>
<td>5</td>
<td>Ensure continual improvement</td>
<td>UNIT Head, HODs, MRs, HSSE Manager</td>
</tr>
<tr>
<td>6</td>
<td>Identify customers/interested parties expectations</td>
<td>UNIT Head, HODs, MRs, HSSE Manager</td>
</tr>
<tr>
<td>7</td>
<td>Suppliers performance evaluation</td>
<td>HOD – Technical Service &amp; Contracts</td>
</tr>
<tr>
<td>8</td>
<td>Comply with defined procedures and operational control</td>
<td>HODs, HSSE Manager</td>
</tr>
</tbody>
</table>

**Corporate Management Representative (CMR)**

POSOCO have nominated Deputy General Manager (Market Operation), SRLDC, Bengaluru as the nodal officer (Corporate Management Representative, abbreviation as ‘CMR’) to coordinate the communication necessary for understanding and implementing the IMS across POSOCO offices. In addition to his assigned responsibilities in SRLDC, for IMS purposes he is responsible for the following:

a) The promotion of ISO 9001:2015 (QMS) awareness and the customer focus to meet customer and other stakeholder needs and expectations;

b) The promotion of HSSE (see footnote #6 for HSSE in section 5.3 in this manual) awareness and compliance requirements;

c) Reporting on the IMS performance and on improvement opportunities to management;

d) Ensuring that the integrity of IMS is maintained when changes to IMS are planned and implemented.

e) Liaison with external parties (IMS consultants, IMS certification agencies & their auditors and Service Providers claiming conformance to ISO 9001 / ISO 14001 / ISO 45001 / ISO 27001 certifications in their contracts) on matters relating to the IMS.

**Unit MR**

To enhance effectiveness of IMS implementation, Unit MR’s has been nominated by each Unit Head across POSOCO offices.
With change of people arising due to transfers, promotions and retirements, it is the responsibility of Unit Management Representative to interact with the new officers joining to appraise about the IMS documented processes and organize awareness / trainings.

Following responsibilities have been assigned to Unit MR:

a) Ensure that processes needed for the IMS is established, implemented and maintained;

b) Evaluate the performance of IMS at periodic intervals by data analysis;

c) Provide inputs to CMR with an overall status of IMS health and data analysis trends and recommend areas that may need improvement; and

d) Participate during MRM (Management Review Meeting) and provide inputs for improvement in the IMS, through CMR, to CMD for decision.

Unit Head Responsibility
The Unit Head is ultimately responsible for the Company’s HSSE performance. He shall ensure that all personnel, who manage and are involved in operations, comply with the HSSE aspects of the Program.

Process Owners/HOD Responsibility
Although the success of any HSSE program requires the combined efforts of management, Process Owners, and the worker, the process owner is the key man. It is the degree to which the process owner applies the intent of the program and the principles of HSSE that governs the success of this program. This being an area of mutual interest between the process owner and the employees, and the Process Owner must lead the way in developing the HSSE program.

Some of the Process Owner's responsibilities are:

- Always set a good example for HSSE.
- Give adequate HSSE instruction to each and every new employee.
- Ensure the understanding by all employees that the violation of established safe work practices is a violation of company rules.
- Promote the proper use and care of protective equipment on each job.
- Promptly report all injuries to the HSSE Manager or designated Safety Officer.
- Conduct routine HSSE inspections of his area for unsafe conditions and procedures and ensure the proper use and maintenance of protective equipment.
- Initialize and forward all necessary accident reports to the HSSE Manager or designated Safety Officer, such as: Accident Report, Near Miss Reports, Unsafe Condition Reports, etc.

HSSE Manager
The coordination of the company’s HSSE program shall be the responsibility of the HSSE Manager. Duties include:
• Advising and making recommendations to all personnel in the company.
• Monitor the overall HSSE program and help identify critical areas.
• Manage and comply with local and industry specific safety and environmental reporting requirements.
• Keep management informed of the HSSE performance of the various departments and recommend appropriate actions to improve performance.
• Develop and implement HSSE-training programs.
• Administer and report to management on the status of workers’ compensation claims and property damage insurance claims.
• Issue work permits.
• Procurement of PPE – Ensure IS compliance
• Evaluate compliance to legal & other requirements relevant to HSSE.

Employee Responsibility
POSOCO Management and Process Owners shall encourage the individual employee to cooperate in every respect with the company’s HSSE program, so that the day-to-day operations may be carried on in such a manner, as to ensure the safety of himself, his fellow employees, the client and company property.

Therefore, each employee is charged with the following responsibilities:
• Observe all safety rules and regulations.
• Report any unsafe conditions or practices to your Process Owner.
• Know how to perform jobs assigned and perform them properly.
• Do not undertake any job you do not understand—ask your immediate Process Owner if there are any questions or any doubt.
• Wear and use all safety equipment required by the job to be performed.
• Participate in safety meetings held by your process Owner.
• Report all injuries immediately to your Process Owner.
• Cooperate with Process Owner when injury and accident investigations are being made so that accident causes can be determined and corrective action taken.
• Report any and all defective tools or equipment immediately.

HSSE Committee Meetings
Regular HSSE meetings shall be held at all units in accordance with Company policy. The frequency of the meetings will be contingent upon the particular activity or risk, and or client requirements. Routine HSSE meetings will be conducted at least once in 6 months.
ANX-01-02: ISMS ROLES & RESPONSIBILITIES

Chairman & Managing Director (CMD)
The CMD’s responsibilities, with respect to IT security, are as follows:
- Ensure that POSOCO has established IT security program;
- Approve the constitution of ISMF
- Allocate sufficient resources necessary for the protection of POSOCO’s IT assets;
- Hold POSOCO’s managers accountable for the security of the IT assets under their control;
- Approve unit CISO as decided by ISMF; and ensure that staff, facilities, and IT processing assets with appropriate national security clearances are available in the all units/locations of Power Systems Operation Corporation (POSOCO).

Information Security Management Forum
The Information Security Management Forum (ISMF) of POSOCO includes representation of RLDCs/NLDC and is responsible for the establishment, implementation, operation, monitoring, review, maintenance and improvement of Information Security Management System (ISMS) at Power Systems Operation Corporation (POSOCO). The responsibilities of the ISMF include:
- Ensuring that Information security objectives and plans are established for ISMS.
- Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the organization’s regulations and the need for continual improvement.
- Providing sufficient resources to develop, implement, operate and maintain the ISMS.
- Identifying the acceptable levels of risk for the Information Assets.
- Periodically reviewing the status of Power Systems Operation Corporation’s (POSOCO) Information Security Management System (ISMS).
- Reviewing and monitoring remedial work related to Information security incidents.
- Approving new or modified information security policies and procedures.
- Approving major initiatives in enhancing Information security.
- Ensuring that an internal audit is carried out every six months and when required in case of any major changes in POSOCO’s business and/or functioning, and a third-party audit is carried out annually.
- Providing competent training and, if necessary, employing competent personnel to satisfy the security requirements of Power Systems Operation Corporation (POSOCO)
- If needed reporting the security posture of Power Systems Operation Corporation (POSOCO) to the Management board and investors every quarter/year.

The ISMF Team has to meet on half yearly (six monthly) basis to discuss and review the security program. This meeting shall be chaired by the CMD of POSOCO.

During Implementation
- Ensure all the recommendations assigned to people from their respectively allocated teams are implemented and followed-up for, from the Risk Mitigation Plan. Also gain an understanding of how the risk assessment is carried out.
- Gain a thorough understanding of the standard: ISO 27001
- Coordinate with the Information Security Management Forum (ISMF) to provide updates on the status of implementation of controls
- Understand and implement the newly formed policies and procedures which form a part of the implementation
- Advise and guide teams for maintaining records (example: change management records)
- Act as single point of contact for managing all information security-related aspects for the team being assigned to them
- Consolidate implementation progress reports and review along with IMS and Chief Information Security Officer (CISO)

After implementation and certification
- Conduct periodic risk assessments
- Communicate the results (Risk Assessment Report) to the IMS team and CISO and follow-up with the risk owners for treating the risks
- Identify any new information security requirements as a result of any process/procedure change or as a result of any additions or deletions in service description or product specification or formations or merger of departments
- Check for records on an ad-hoc basis
- Conduct surprise audits with users to ensure diligent implementation of policies and procedures
- Conduct quarterly or bi-annual internal audits and draft and maintain the corrective and preventive action plans (also follow up on the same)
- Update and draft any necessary documentation for surveillance audits
- Evaluate tools to automate assessments in consultation with technical consultants
- Maintain and present the security measurement figures as decided from the Metrics and Measurement document
- Ensure regular mock drills - power and fire are conducted. Also execute walk-through with teams to test the business continuity plan
- Conduct regular security awareness sessions for batches of employees

Chief Information Security Officer (CISO)
The unit CISO is appointed by the POSOCO’s ISMF which is represented by the unit heads and unit MRs. With respect to IT Security, the CISO’s responsibilities are as follows:
- Ensure that appropriate levels of security are applied to all IT assets (whether retained in-house or under the control of contractors);
- Oversee, define, plan, budget, and implement the IT security program;
- Approve and issue IT security program policy, procedures, and guidance;
- Ensure that the IT security program integrates fully into enterprise architecture and capital planning and investment control processes;
- Ensure that IT assets are developed and operated in full compliance with Department and POSOCO’s policies, as well as ISO 27001’s IT security-related directives;
- Ensure that all IT assets owned or operated by or for POSOCO’s are accredited and that all IT assets are assigned to an IT system;
- Ensure that IT security is planned and implemented across POSOCO throughout all phases of the System Development Life Cycle;
- Serve as a co-accreditor of all IT assets. Operating Unit Directors are the designated approving authority (accepting operating risk) for the operating unit’s IT assets, but the CIO must co-accredit all IT assets;
- Ensure that positions with significant IT security responsibilities are held by staff with sufficient training and education qualifications as well as by staff who have had appropriate background checks;
- Provide a means for staff to electronically identify all IT users such that staff will be able to easily differentiate between government employees, contractors, foreign nationals with countries of association, and other associates;
- Ensure that staff responsible for oversight of POSOCO’s classified IT processing efforts receive extensive training from the agencies that sponsor those efforts, including yearly refresher briefings presented by those agencies;
- Ensure that all cleared staff receive an extensive briefing presented by a qualified staff member relevant to their clearance level that describes in detail all individual IT responsibilities prior to granting access to any classified assets;
- Ensure that all cleared staff receive a comprehensive yearly awareness briefing presented by a qualified staff member of individual IT responsibilities relevant to their clearance level as a condition of continued access to any classified assets;
- Provide an IT processing procedures manual for classified information to all cleared staff; and
- Provide an IT processing procedures manual to all staff that includes processing procedures for information commonly considered “sensitive information.”
- Coordinate implementation of the IT security program;
- Develop IT security program policy, procedures, standards, and guidance consistent with Departmental and ISO 27001’s requirements.
- Assist with the development of IT system specific policy, procedures, and safeguards;
- Implement and manage an IT security awareness and training program;
- Assist with the planning and budgeting of IT security functions for POSOCO
- Establish and maintain an IT security certification and accreditation program. This includes ensuring that all assets have completed and maintained security plans, risk assessments, contingency plans, and security self-assessments;
- Ensure that an objective, independent review and approval process exists for both security plans and procurement requests to validate the adequacy of proposed security safeguards;
- Communicate security requirements to POSOCO’s management and staff and serve as a resource on effective IT security practices;
- Act as a liaison between the Department and POSOCO on Department-wide security initiatives, incident response activities, and on fulfilling IT security reporting requirements;
- Conduct POSOCO -wide intrusion detection and vulnerability monitoring; and
- Create and maintain an incident response capability.
Departmental Information Security Officers (DISO)

Department Information Security Officers are directly responsible for the security of the assets under their purview. DISO have the following responsibilities:
- Ensure that appropriate levels of security are applied to all the assets and that sufficient resources are planned and assigned to maintain the required level of security;
- Work closely with and support the CISO in implementing the POSOCO’s IT security program;
- Ensure all assets are developed and operated in full compliance with Department and policies (e.g., annual user training requirements) as well as ISO 27001’s IT security-related directives and mandates;
- Account for IT security in capital investment plans which must include all IT resources (e.g., labour, hardware, software, maintenance) for procurement, maintenance, and replacement of all assets;
- Ensure IT security is planned and implemented throughout all phases of the System Development Life Cycle;
- Ensure that department positions with significant security responsibilities are held by staff with sufficient training and education qualifications as well as by staff who have had appropriate background checks;
- Appoint an ISO (Information Security Officer). In those cases where the department is located at different sites, an ISO shall be appointed for each site.
- Designate alternate ISO(s) for when the primary ISO(s) is unavailable;
- Assign ownership of IT resources such that all department resources are assigned to a particular system and such that all assets have a designated system owner;
- Serve as the Designated Approving Authority (accepting operating risk) for the department’s assets along with the CIO who co-acredits all IT assets;
- Ensure that staff responsible for oversight of POSOCO’s classified information processing efforts receive extensive training from the agencies that sponsor those efforts, including yearly refresher briefings presented by those agencies;
- Ensure that all cleared staff receive an extensive briefing presented by a qualified staff member relevant to their clearance level that describes in detail all individual IT responsibilities prior to granting access to any classified assets; and
- Ensure that all cleared staff receive a comprehensive yearly awareness briefing presented by a qualified staff member of individual IT responsibilities relevant to their clearance level as a condition of continued access to any classified assets.
- Coordinate the implementation of the security program within their Department (e.g., coordinating certification and accreditation activities);
- Assist with the planning, budgeting, and implementation of IT security for the Department;
- Assist system owners in developing security plans, risk assessments, security self-assessments, contingency plans, security controls, and system specific policies;
- Serve as contact points for all security related issues for the Department and act as a liaison to the CISO;
- Participate in the development of IT security policies, procedures, and guidance;
And Communicate IT security requirements to POSOCO’s management and staff and serve as a resource on effective IT security practices.
- Actively monitor the system to ensure adequate security levels are properly maintained;
- Assist and advise the system owner on system security issues throughout the system’s life cycle;
- Assist in the determination of an appropriate level of security commensurate with the level of sensitivity;
- Participate in certification and accreditation activities for the system. This includes assisting in the development and maintenance of system security plans, risk assessments, security self-assessments, contingency plans, policies, and procedures;
- Assist in handling and investigating incidents in cooperation with the system owner and under direction of the CISO;
- And cooperate with the staff of other interconnected assets to ensure consistent levels of security.

**IT Head**

IT Head designated to maintain the system or parts of the system. Each system will have one or more formally designated assets administrators responsible for the entire system and may have other assets administrators responsible for parts of the system. Each system administrator is responsible for the secure operation and maintenance of the IT elements under their control. Specifically, system administrators have the following responsibilities:
- Ensure that IT system technical and operational security controls are being implemented and maintained according to the sensitivity level of the system and the data being processed;
- Assist in the development and maintenance of required security documentation and related activities (e.g., system administration and operational procedures and manuals);
- Know which assets or parts of assets for which they are directly responsible (e.g., network equipment, servers, and LANs);
- Ensure that appropriate levels of security are applied to all IT assets;
- And assist the SSO, the system owner, and the department IT Security Officer as necessary.
- Coordinate with appropriate administrators (System/network) and ISOs to ensure that their databases and applications are being adequately protected commensurate with the sensitivity level of the data being processed;
- Operate databases and applications in a secure manner;
- Manage user accounts in a timely and secure manner (e.g., disabling accounts);
- Assist in the development and maintenance of required security documentation and related activities (e.g., application administration and operational procedures and manuals);
- Know which applications and databases for which they are directly responsible;
- And assist the ISO, the system owner, and the department IT Security Officer, as necessary.

**All Authorized Users (employees, vendors and contractors)**

The success of IT security programs ultimately depends on the commitment of each user. Users are to:
- Operate IT assets in a secure and responsible manner;
- Know and abide by all applicable policies and procedures. This includes reading and understanding POSOCO’s and system-specific rules of behaviour regarding inappropriate use or abuse of POSOCO’s resources;
- Participate in security awareness and training activities;
- Know which assets or parts of assets for which they are directly responsible (e.g., printer, desktop, specific support service, etc.);
- Know the sensitivity of the data they handle and take appropriate measures to protect it;
And Report incidents to their ISO and the POSOCO’s CISO using the method devised.