INFORMATION SECURITY POLICY STATEMENT

CESC Ltd. is committed to implement the processes and systems to protect and safeguard all critical Information, Infrastructure and Data within IT and OT environment whether in paper, electronic, or any other form, from internal and external threat actors in order to ensure safe and secure generation and distribution of electricity services to consumers and allied business operations. CESC Ltd. shall ensure that this document is reviewed at the time of any major change(s) in the existing environment affecting policies and procedures or once every year, whichever is earlier. This document shall be reviewed and approved by the VP(IT). The reviews shall be carried out for assessing the following:

1) Impact on the information risk profile due to, but not limited to, the changes in information assets, deployed technology, system architecture, regulatory and/ or legal requirements; and
2) The implementation and operational effectiveness of the policies.

As a result of the reviews, additional policies could be issued, and/ or existing policies, procedures and security standards could be updated, as required. These additions and modifications would be incorporated into the document. Policies that are identified to be redundant shall be withdrawn. VP(IT) has approved the Information Security Management System (ISMS) Apex Manual based on ISO27001:2022 mandatory requirements and associated security standards and procedures. The management's commitment is:

1) To ensure the Confidentiality, Integrity and Availability of Critical Information Infrastructure (CII) and other Information processing facilities for IT and OT systems.
2) That all stakeholders are responsible for implementation of respective security policies, standards and procedures within their area of operations, and oversee adherence by their team members
3) Risks are identified, analyzed and mitigated to an acceptable level through a risk management framework and duly documented within the IT/OT Risk Management Portal
4) Security Incident management process is established and implemented to ensure that all security breaches of information security, actual or suspected, are reported, triaged and investigated
5) Business Continuity and IT Disaster Recovery plans are developed, implemented and maintained
6) Information security awareness and training are regularly arranged for all employees
7) That security vulnerability assessment to be performed periodically and mitigated
8) To ensure that all regulatory and legislative requirements from MoP, Government of India has been implemented
9) The information security management system is continually improved

Date: 17-02-2025

Version: 2.3