Cyber Security Model Contractual Clauses:

1. The OEM/Supplier/Vendor/Integrators, here in shall be referred to as "Company" and Responsible Entity as defined in CEA (Cyber Security in Power Sector) Regulation, 2021 herein shall be referred to as "Owner" and the component/equipment/system/servicesbeing procured by the Owner through the bid from the Company shall be collectively referred to as Product.

2. The Company through a digitally signed statement by thier Authorized representative shall disclose along with their bid, the existence and reasons for all known cyber security vulnerabilities or identified backdoor codes in effect till the submission of bid by the Company,in each of their Product offered for sale. Further known cyber security vulnerabilities or identified backdoor codes should be disclosed by the Company during post bid discussion if any held by the Owner. The owner reserves the right to seek compensatory security controls for mitigation of the disclosed vulnerability or identical backdoor codes along with the letter of Acceptanceof the Supply Order/Work Award Order or to reject the bid without any notice to the Company, based upon the risk evaluation of the disclosed cyber security vulnerabilities by the Company.

3. The Company through a digitally signed statement by their Authorized representative shall submit along with their Letter of Acceptance of Supply Order/Work Award Order, the details of obsolescence of any part/component of hardware/software and the list of all new cyber security vulnerabilitiesin each Product offered for sale, discovered subsequent to the submission of bid, by the Company or has come to the knowledge of the Company or been brought to the Company's knowledge, by any of their existing Customeror previous Customer, Partner or related/unrelated third Party.

4. During the currency of support agreement for the Productssupplied to the Owner or till termination of the supportagreement been communicated to the Authorized representative of the Company in writing by the Owner, the Company shall be liable to disclose details of all additional cyber security vulnerabilities, that beendiscovered by the Company or that comesin the knowledge of the Company or isbrought to the Company's knowledge by any of their existing Customer or previous Customer, Partner or related/unrelated third Party, along with cyber threat mitigation measures which needs to be taken thereof by the Owner, without any further commercial implication to the Owner.
5. During the currency of support agreement for the Products supplied to the Owner or till termination of the support agreement been communicated to the Authorized representative of the Company in writing by the Owner, the Company shall disclose details of all exploits of cyber security vulnerabilities, previously known or unknown, in all Products supplied to the Owner or similar Productssupplied to any other customer by the Company, within 24 hours of such information coming in the knowledge of Company,through any source including Cyber Security Audit carried out by CERT-In empanelled Auditors, along with cyber threat mitigation measures,which need to be taken thereof by the Owner, without any further commercial implication to the Owner.

6. The Company during the currency of support agreement for the Products supplied to the Owner and even after the expiry of the support agreement,shall inform to the Owner from time to time, through the mutually agreed digital/physical mode,in case the

Company comes across any event(s) or condition(s) that mayprobably result in, any security breach or likely risks of other compromises,withinthe Owner's IT or OT Systems and Data Bases,along with cyber threat mitigation measures, which needs to be taken thereof by the Owner,without any further commercial implication to the Owner

7. In case the Company, intentionally or unintentionally, fails to provide, or deliberately do not provide the information or fails to provide cyber threat mitigation measures to be taken thereof by the Owner,as mandated in above clauses from Sl No 2 to Sl No 6, the CommercialPerformance Guarantee of the Company submitted with the Owner shall stand forfeited without issuance of any show cause noticeby the Owner to the Company.In case if the Commercial Performance Guarantee of the Company submitted with the Owner is forfeited, the Company, their Partner Company if any, shall be debarred from the participation in future bids invited by the Owner.

8. The Company through a digitally signed statement by their Authorized representative shall certify that the cyber security features designed, recommended in the Product supplied by the Company or their Authorised Partner or Subsidiaries to the Owner, are in accordance with the defined IEC/ISO/IS Standards, best practices, Cyber laws, and Regulations,as specified by the Owner in their bid document and essential for safe and secure Operation and Maintenance of the IT/OT/ICS systems of the Owner.

9. The Company shall ensure that Product supplied against the Supply Order/Work Award Order under consideration or against re-order in part or full against previous Supply Order/Work Award Order, as well as the modifications, reconfiguration,upgradation, changes in Parameters, settings proposed to be made to the existing Architectural layout or utilization of Cyber Assets, as part of the execution of Supply Order/Work Award Order, are in accordance with the defined IEC/ISO/IS Standards, best practices, Cyber laws, and Regulations, as specified by the Owner in their bid document and essential for safe and secure Operation and Maintenance of the IT/OT/ICS systems of the Owner. All modifications shall be carried out by the Company as per mutually written agreement between Owner and Authorized representative of the Company, before its implementation/commencement of Supply Order/Work Award Order. The Owner shall be responsible for consulting cyber security experts and for arranging the necessary support to the Company, if any modifications are to be made to the existing Architectural layout or utilization of Cyber Assets.

10. In case, the Company has been awarded the Maintenance & Support Contract for a part or the entire IT and OT System of the Owner:
    (i) The Company shall provide a host-based malware detection scheme for the control system network and equipments as per the IEC/ISO/IS Standards mentioned in the bid document of the Owner.
    (ii) The Company shall certify the adequacy of the system performance of the deployed host-based malware detection scheme for quarantine (instead of automatically deleting) suspected infected files and the Company shall also provide the scheme for updating the Malware signatures.
    (iii) The Company shall also test major updates to malware detection applications and provide performance measurement data on the impact of using the malware detection applications in an active system. Any commercial implication related to update/upgrades for malware detection and protection will be borne by Owner.

11. The Companythrough a digitally signed document by their Authorized representative shall submit to the Owner, in detailthe tried and tested backup and disaster recovery technologyand plan for the Product as practised by the Company till the time of submission of bid.The Owner shall be free to implement such technology and Plan on their Own orengage the Company at a mutually agreed costor get it implemented through a Third Party, provided that the liability, cost and responsibilities of such implementation shall rest on the Owner.

12. In case, the Company accepts the Supply Order/Work Award Orderoffered with or without Maintenance & Support contract for part or entire IT or OT System of the Product, then, on demand made by Owner, the Company shall provide documentation detailing all applications, utilities, system services, scripts, configuration files, databases, and all other software required and the appropriate configurations, including revisions and/or patch levels for each of the computing & Storage systems to the extent deemed necessary for safe and secure operation and maintenance of IT and OT System to be carried out by the Owner himself or through any third Party.

13. The Company shall advise Owner as per mutually agreed Terms and Conditions on the measures to be followed by the Owner during Operation and Maintenance of the IT and OT System in accordance with applicable IEC/ISO/ISStandards and best practices, which shall include but are not limited to, cyber security policies and procedures, documentation and training requirements, continuous monitoring of assets for tampering and intrusion, periodic evaluation for asset vulnerabilities, implementation and update of appropriate technical, physical, and operational standards, and offline testing of all software/firmware patches/updates prior to placing updates into IT and OT Systems of the Product.

14. The Company shall provide a listing of services required for all ICT based sub-systems and applications of the Product supplied by them to the Owner. The listing shall include all ports and services required for normal operation as well as any other ports and services required for emergency operation/maintenance of the Product. The listing shall also include an explanation or cross reference furnished by the Company or by any authorised Person on behalf of Company, to explain why each service is deemed necessary for operation and maintenance of the supplied Product.

15. The Company shall certify and provide proof that all default passwords have been reset with hardened passwordand services are patched to current released version till the time of completion of SAT procedure and issue of successful SAT completion certificate by the Owner. The Company shall be liabe to provide, within and up to a pre-negotiated period, appropriate software and service updates to mitigate threats from all vulnerabilities associated with the Product and to maintain the established level of system security. Any additional cost related to such upgrades after the pre negotiated period shall be borne by the Owner.

16. The company shall inform theOwner about any conflict between the software components/ versions/ services/ ports used by the supplied Products and the pre-existing application.The Company and Owner shall resolve such conflicts as per mutual terms and conditions. The Company shall remove a software component if not required

for the operation and maintenance of the system or application, with the Owner's due written permission only. The Company shall maintain documentation on what has been removed and shall furnish this information to the Owner as and when called for by the Owner. Responsibility with Company is limited to the set of unused software, application, utilities as may be brought into the Owner's environment by the Company and not the ones any pre-exiting in the environment. The Owner is expected to put in place an established "Change Management Procedure" which may be shared with the Company if essential for cyber security.

17. The Company shall notify the Owner in writing on the non-standard operation carried out by the Owner's Employees and that the Company shall not be held liable for Vulnerabilities exposed by the listed incorrect operation carried out bythe Owner'sEmployees or any person other than those working on behalf of the Company. However, the Company shall stand for prosecution and bear any consequential loss or damage suffered by the Owner from exposure to such Vulnerabilities which were known to the Company and intentionally not disclosed to the Owner or no measures were suggested for mitigation of risk from such known vulnerabilities.

18. The Owner shall have the right, but not the obligation, at all reasonable times to inspect/test the Product for being Counterfeit or Tainted and to test for presence of any embedded hardware or software Trojan in the Product.

    (i) The Company shall provide all reasonable assistance and facilities and access for such inspection and cyber testing at the Company's Factory, at Company's Supplier's facilities, or at the facilities of any Subcontractor where any part (hardware or software) of the Product has been or are being fabricated, manufactured or integrated.

    (ii) Inspection and cyber testing of the Product if carried out by the Owner shall in no way relieve the Company from its obligations for FAT and SAT mandated in the Supply Order or any other examination of Tests provisioned under the mutually extended Terms and Conditions or any Agreement entered between the Owner and the Company.

    (iii) The company shall extend the necessary support to the Owner in collecting the required evidence from the Product for reporting any security incident.

    (iv) The Owner shall not infringe any IPR of the Company or Company's Suppliers in any form during any inspection and cyber testing if carried out by the Owner in exercise of their right as per clause at Sl. No. 18(i).

    (v)The Owner shall provide reasonable notice period to the Company for any inspection and cyber testingif to be carried out by Owner and the expenses if any on account of inspection and cyber testing shall be borned either by Owner or the Company as per the mutually agreement.

19. Should any Employee of Companyif required or to be permitted the Logical Access or unescorted physical access to the Cyber Assets of the Owner or of any of their Affiliates, that are identified as "Critical Infrastructure" or as "Protected System" by NCIIPC {constituted under IT Act 70A}, then theEmployee of the Company shall meet

pre-requisites mandated by Owner prior togaining access to any such "Critical Infrastructure" or "Protected System" of the Owner.

(i) Therefore, when any secured electronic or physical access is needed or to be permitted, all Employees of the Company identified as above in this provision shall:
   (a) abide by and shall have successfully completed the Company-administered background screening requirement.
   (b) have undergone successfully the mandatory Cyber Security training prescribed by the Owner, for all of their "Critical Infrastructure" and "Protected System" as per CEA(Cyber Security in Power Sector) Regulations 2021.
   (c) have a valid Company Identification document and should have been listed in Company's Management System for tracking purposes;

   Pursuant to this clause in order to ascertain fitness, qualification and integrity of Employees identified for executing Works awarded to the Company, the Company shall perform background investigation on these Employees of their Company or of their Supplier or of Subcontractors assigned to execute such Work on behalf of the Company at the Owner's site or at facilities of the Company, their Suppliers/Sub Contractors.

   (d) in the event that the Company or their Supplier or Sub-Contractor
      (i) determines that any of the Employee permitted access pursuant to this clause no longer requires access or
      (ii) terminates the employment of any of the Employeehaving valid permission to such an access.

   pursuant to this clause, Company shall notify Owner in writing within 24 hours of such determination or termination.

(ii) The Company shall be held responsible and shall have to bear the cost of the damages resulting to the Owner's Asset, Facilities, Business interruptions or damage to the Owner's reputation, out of any cyber incident resulting of any misconduct,on site or remotely, directly or indirectly by the Employee(s) of the Company or the Employee(s) of the Supplier or Subcontractor..

20. The Company shall abide by the Owner's approved patch management and patch update process. The Company shall provide patch updates affecting security within a pre-negotiated period as identified in the patch management process. The Company shall apply, test, and validate the appropriate patch updates and/or workarounds on a baseline reference system before updation process.The company shall communicate to the owner all patch update/software configuration files/database with check sum of the package files, through digitally signed encrypted message. Mitigation of any vulnerabilities found,shall be carried out within a pre-negotiated period by the Company. Any system upgrade provided bythe Company to the Owner,commercial implications shall be settled at mutually agreed prices.

21. With the due approval of the Owner, the Company shall disable, through software or physical disconnection, all redundant communication ports and removable media drives. The Owner shall password protect the BIOS from unauthorized changes unless it is not technically feasible, in which case Owner shall document this case and provide mitigation measures. On Owner's demand, Company shall provide a documented list of

all disabled or removed USB ports, CD/DVD drives, and other removable media devices.

22. With the due approval of the Owner, theCompany shall configure the network devices to limit access to/from specific locations, where appropriate, and provide documentation of the configuration. With the due approval of the Owner, the Company shall configure the system to allow the system administrators the ability to re-enable devices if the devices are disabled by software and provide documentation of the configuration. The Owner is expected to put in place an established "Change Management Procedure".

23. The Company shall haveand provide to the Owner the documentation of a written flaw remediation process. Company shall provide appropriate software updates and/or workarounds to mitigate all vulnerabilities associated with the flaw in the Product within and up to a pre-negotiated period. After Company is made aware of or discovers any flaws, Company shall provide notification of such flaws affecting security of softwaresupplied by the Company, within and up to a pre-negotiated period. Notification shall include, but is not limited to, detailed documentation describing the flaw with security impact, root cause, corrective actions, commercial implication if any, etc.

24. In addition to the foregoing, the Company shall immediately notify Owner in writing if the Company at any time discovers any part of the Work to be defective or not in accordance with the Work Award Order.

25. The Company shall comply with the Owner's Application Security standardsas mentioned in the bid document, whenever Owner seeks Coding for Security enhancement.

26. The Company shall provide a process for Owner's Employee(s) to submit problem reports and remediation requests to be included in the system security. The process shall include tracking history and corrective action status reporting. The Company shall review and report their initial action plan within 24 hours or pre-negotiated period whichever is later of submitting the problem reports. Company shall secure reportsonproblemregarding security vulnerabilities from public discloser and notify Owner of all problems and remediation steps, regardless of origin of discovery of the problem. Company shall inform Owner in writing of flaws within applications and operating systems in a reasonable period and provide corrective actions, fixes, or monitoring guidance for vulnerability exploits associated with the flaw. Company shall provide an auditable history of flaws including the remediation steps taken for each. Any commercial implication related to update / upgrades will be borne by Owner, if it is beyond the support period of the Product as agreed by the Company.

27. In case the technical required of the Owner demands,the Company shall provide a detailed plan for appropriate physical security mechanisms. Company shall provide lockable or locking enclosures for control system components (e.g., servers, clients, and networking hardware). The Company shall provide locking devices with a minimum of two keys per lock identifiable to each lock, and keyed or not keyed alike depending on Owner requirements. Company shall recommend a room locking device(s) where the equipment and workstations are located, if not already installed by Owner. Company

shall verify and provide documentation that unauthorized logging devices are not installed (e.g., key loggers, cameras, and microphones). Company shall provide two-factor authentication for physical access control.

28. The Company shall provide a system whereby account activity is logged and is auditable both from a management (policy) and operational (account use activity) perspective. Company shall time stamp, encrypt, and control access to audit trails and log files. The Company shall ensure audit logging does not adversely impact system performance requirements. Company shall provide read-only media for log creation.

29. The Company shall provide a configurable account password management system that allows for selection of password length, frequency of change, setting of required password complexity, number of login attempts, inactive session logout, screen lock by application, and denial of repeated or recycled use of the same password. Company shall not store passwords electronically or in Company supplied hardcopy documentation in clear text unless the media is physically protected. Company shall control configuration interface access to the account management system. Company shall provide a mechanism for rollback of security authentication policies during emergency system recovery or other abnormal operations, where system availability would be negatively impacted by normal security procedures, but such rollback shall not be automatic, and would require the specific affirmative agreement of Owner.

30. The Company shall configure hostsOperator workstation with least privilege file and account access and provide documentation of the configuration. The Company shall configure the necessary system services to be executed at the least user privilege level, possible for that service and provide documentation of the configuration. Upon the completion of the task of changing or disabling access to such files and functions as directed by the Owner, the Company shall provide documented evidence that the tasks has been successfully completed.

31. The Company shall recommend which specific accounts need to be active and those that can be disabled, removed, or modified. The Company shall disable, remove, or modify all the accounts pursuant to the approved recommendation from Owner. The owner shall be responsible for correct usage and maintenance of the defined accounts.

32. The Owner, shall retain and maintain at least oneset of record of all documents obtained or generated in the course of the execution of the Work Awarded to the Company, for a period of five years, from the date of the completion of the Work, at a designated archive defined by competent Authority.

33. In the event of any damages caused by the Owner, any resultant work to be done by the Company to make good, the Work shall be at,Nil/additional, cost and time,as mutually agreed between the Owner and Company, on case to case basis. Both Owner and the Company shall have responsibilities e.g. the holistic, state-of-the-art security concept which Owner has put in place, and such concept shall include, but not limited to the following:
    (i) installation of updates as soon as provided/made available by the Company
    (ii) complying with security advisories of the Company
    (iii) regular vulnerability scanning and testing

(iv) robust password policy
(v) firewalls, network client authentication, malware scanners, etc.

34. Limitation of Liability

(i) The obligations of Company in relation to or in connection with cyber threats, set forth in this Agreement, shall be the exclusive remedy and in lieu of any other rights and remedies the Owner may have, with respect to cyber threats and any damage suffered therefrom, whether under contract, law or otherwise.
(ii) Unless otherwise mutually agreed in writing, any right of the Owner to claim damages resulting from or related to cyber threats, such as but not limited to loss or manipulation of data, downtime, business interruption, lost profit, cost for product reset and/or data reconstruction, regardless of the legal basis, but in particular resulting from any duty under the Agreement, is hereby excluded.
(iii) In General, the Company is responsible and liable, till the mutually agreed time period, for mitigating all vulnerabilities associated with the Product and maintaining the established level of system security in the system of the Owner.
(iv) In particular Company assumes no liability whatsoever for damage caused by

(a) Owner's intrusive security testing;
(b) unauthorized modification of the system configuration or security level;
(c) the installation of patches which are not authorized by Company; or
(d) the Owner delaying the self-installation of patches made available by Company.

(iv) Under no circumstances, Company'sliability arising from any act or omission relating to cyber threats,shallexceed the aggregate liability stated in the contract or Supply Order/Work Award Order, to which this document is an integral part, and such liability shall relate only to claims arising from reasonably foreseeable acts or circumstances.

35. Definitions for various terminology used in this Agreement e.g. security breach, material adverse effect, vulnerability, etc shall be **in accordance with international standard e.g. ISO/IEC series 27000, 27001, IS 16335, IEC 62443**

36. Clauses from Sl No 4 to Sl No. 35 shall be the part of an Agreement which shall become binding upon both the parties when executed by duly authorized representatives of each party either through a written signature and seal, or through a digital signature (DSC) and shall be an integral part of the Supply Order No. _____ / Work Order No----------/ Contract No. _____. Any amendments to this agreement shall be made in a written or digital form duly signed and stamped by authorized representatives of each Party.