

Annexure Cyber Security\_Rev1

- 1.0 This annexure contains basic Cyber security details. The contractor shall ensure that his equipment complies with the latest version of the following standards. Further the contractor shall comply to the general norms and practices mentioned in the standard.
  - 1.1 IEEE-1686:2013 “Cybersecurity requirements for Intelligent Electronic Devices”
  - 1.2 IEC 62443: for security of Industrial Automation and Control, which provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems
  - 1.3 NIST SP800 Guidelines;
  - 1.4 NERC CIP Standard
  - 1.5 ISO 27001/ 27019
  - 1.6 IEC62443
  - 1.7 Any standards mentioned in the document Annexure Cyber Security – Non Disclosure Agreement – Rev 01 given below.
  
- 2.0 As per ministry of power order XXXX dt YYYY the contractor shall note the following items. Further the contractor shall sign and supply the document ( Annexure XXX) for each equipment being supplied by him.
  - 2.1 All equipment, components, and parts imported for use in the Power Supply System and Network shall be tested in the country to check for any kind of embedded malware / trojan / cyber threat and for adherence to Indian Standards ( XXX and YYYYYY).
  - 2.2 All such testing shall be done in certified laboratories that will be designated by the Ministry of Power (MoP).
  - 2.3 Any import of equipment / components / parts from “prior reference” countries as specified or by persons owned by, controlled by, or subject to the jurisdiction or the directions of these “prior reference” countries will require prior permission of Government of India.
  - 2.4 Where the equipment / components / parts are imported from “prior reference” countries, with special permission, the protocol for testing in certified and designated laboratories shall be approved by the Ministry of Power (MoP).

This is shall apply to any item imported for end use or to be used as a component, or as a part in manufacturing, assembling of any equipment or to be used in power supply system or any activity directly or indirectly related to power supply system.
  
- 3.0 The contractor shall provide a solution to store all logs generated by systems (syslogs) in a dedicated system. The system shall be able to store the logs for at least 3 years before the storage is full.
  
- 4.0 All USB ports of all hardware shall be by default disabled for mass storage devices. In case the contractor uses USB based dongles for license software then the dongles shall be whitelisted separately so that only they can be used.
  
- 5.0 The contractor shall perform whitelisting of the system. The vendor shall whitelist all services that are available as part of the operating system.
  
- 6.0 The contractor shall provide an Antivirus software and implement antivirus for the HVDC. POWERGRID currently has server with XXXX antivirus at NTAMC, manesar. This server is meant to push the regular updates to various client installations at site. Thus the vendor shall supply a antivirus server with XXXY installation at site. This server then shall be configured to connect to the server at NTAMC to get updates on regular intervals.

**Annexure Cyber Security – Non Disclosure Agreement – Rev 01**

**To be executed by the successful bidder and shall form part of the Contract Agreement.**

This **Non-Disclosure Agreement** (“Agreement”) is made effective on this.....(“Effective Date”)

By and Between,

**Power Grid Corporation of India Limited**, which expression includes its successors and assigns) having its Registered Office at B9, Qutub Institutional Area, Katwaria Sarai, New Delhi, 110019 and Corporate Office at Saudamini , Plot No. 2, Sector 29, Gurugram, Haryana , 122001, hereinafter referred as Disclosing Party / POWERGRID

And

.....having its registered office at..... which expression includes successors and assigns, hereinafter referred as Receiving Party / Vendor.

Both collectively referred to as “Parties” and individually as “Party”.

**WHEREAS**

- A. POWERGRID, a Govt of India Enterprise under Ministry of Power, is entrusted with the establishment, maintenance and operation of inter-state EHV transmission lines, substations & communication facilities in a coordinated and efficient manner with reliability, security and economy. Its primary business is bulk transmission of Electric Power through its EHV AC (765/400/220 /132kV) and HVDC ( $\pm 500\text{kV}/\pm 800\text{kV}$ ) transmission network.
- B. The vendor is engaged in .....
- C. POWERGRID and Vendor are desirous of pursuing a mutually beneficial relationship through the execution of Contract awarded by POWERGRID to the vendor vide No.... Dated ..... The Vendor agrees that in the course of their association for executing the said Contract Agreement, there may be sharing of confidential information between them. Through this Agreement, both parties define the obligations with respect to the confidential information.
- D. Vendor may receive from the other Party i.e. POWERGRID certain technical, non-technical, financial, business and other proprietary and confidential information in relation to their respective businesses and contract specific tasks.
- E. Due to various Information Security related risks associated with the execution of the contract, POWERGRID desires to mitigate the perceived risks and seeks to protect its physical and intellectual assets through defined agreements with the vendor.

**NOW THEREFORE**, in consideration of the above premises the sufficiency of which is hereby acknowledged, the Vendor agrees as follows:

**1. Confidential Information**

“Confidential Information” shall mean any and all information disclosed to, or otherwise acquired or identified or observed by the Receiver including its subsidiaries and affiliates, and each of their respective directors, employees, representatives and agents from the Disclosing Party and its affiliated companies, relating to the business of the Disclosing Party, or received

**Annexure Cyber Security – Non Disclosure Agreement – Rev 01**

from others that the Disclosing Party is obligated to treat as confidential, and other materials and information of a confidential nature whether communicated in writing, orally, electronically, photographically, or recorded in any other form of media, including, but not limited to, all sales and operating information, contractor's information, employee and other human resource information, existing and potential business and marketing plans and strategies, financial information, cost and pricing information, data media, know-how, designs, specifications, technical configurations, concepts, reports, methods, processes, techniques, operations, devices, , product schematics or drawings, descriptive material, patent and patent applications, trade secrets, trademarks, trade names, specifications, software (source code or object code) and the like, whether or not the foregoing information is patented, tested, reduced to practice, or subject to copyright or any other intellectual property right.

"Confidential Materials" shall mean all tangible materials containing Confidential Information, including without limitation drawings, schematics, written or printed documents, computer disks, tapes, and compact disks (CD), whether machine or user readable.

Notwithstanding the above, all Confidential Information shall be specifically marked as "CONFIDENTIAL" while disclosing the same to the Receiving Party. If the same is orally disclosed then the same to be reduced in writing and marked as "CONFIDENTIAL". Supplier, sub-contractor and other parties engaged by the Disclosing party shall have the same rights and obligations for the Confidential Information.

## **2. Obligations of Receiving Party relating to Information Security**

Vendor agrees to conform to the following requirements:

- a) All intelligent electronic devices (IEDs), including devices with embedded software, Automation servers Controllers, HMIs and associated network components wherein the data is routable (equipped with Ethernet/optical Ethernet, Serial/Optical Serial) must have capabilities to exceed or meet applicable technical requirements under IEEE-1686:2013 for satisfying IEC/ISO:62443-2-3, IEC/ISO:62443-2-4 and IEC/ISO:62443-3-3 requirements.
- b) Vendor agrees to submit required evidences for conformance to IEC/ISO:15408 for identified network based systems such as routers, firewalls, SIEMs etc.
- c) Vendor agrees to provide IT architecture details such as Firmware details, Operating System, databases, middle-ware, application frameworks and related third-party drivers, software component libraries, including usage of virtualization/container technologies, of all devices qualifying under clause (a) above to facilitate vulnerability analysis of the device. POWERGRID reserves the right to undertake appropriate black-box testing of any system, sub-system to independently ascertain vulnerability of the product/solution.
- d) Vendor agrees to enable use of Indian Regional Navigational Satellite Constellation (IRNSS) based Time Synchronization signals through appropriate use of GPS technologies that support PTP (IEEE 1588) , if available commercially.

In case the same are not available commercially, vendor may supply the GPS Clock as per their solution requirement. However, in case POWERGRID supply the Indian Regional Navigational Satellite Constellation (IRNSS) based Time Synchronization signals through

**Annexure Cyber Security – Non Disclosure Agreement – Rev 01**

appropriate use of GPS technologies that support PTP (IEEE 1588) during this contract period (up to start of the Factory System Test), Vendor shall replace the existing Clock with the POWERGRID supplied timing solution in the Control and Protection system, without any cost implication to POWERGRID.

- e) Vendor commits to ensure, its adherence to secure software development life-cycle processes as per IEC/ISO:24748-1 or a similar standard and commits itself for voluntary disclosure of vulnerabilities in the system. Vendor agrees to develop and provide patches, including those of the third-party software components, for the vendor disclosed vulnerabilities and also for the vulnerabilities discovered/ reported by any third party organization. The vendor agrees to ensure supply and installation of patches up to the defect liability period of the system.
- f) For all software, operating system, software patches, version upgrades, firmware images etc authorized by the Vendor to be installed during the Life-Cycle of the project, the Vendor agrees to inform POWERGRID through a digitally signed email, the **SHA-256** checksum of all software components.
- g) The Vendor agrees to provide a list of all equipment and processes where data encryption is used. All required details for Key Management shall be provided to POWERGRID. POWERGRID at its own cost, shall supply requisite digital certificates/keys for installation and configuration of such systems as may be required for securing its interest.
- h) POWERGRID shall provision Notebook PCs as per recommendations of the Vendor, which shall be only authorized device from which access to the network in use by POWERGRID, shall be permitted for any preventive maintenance, update and configuration.
- i) The Vendor agrees to sign an undertaking as per Annexure-A, for its commitment to ensure bug and malware-free software/ software patches/ embedded software/ firmware in systems such as PLC Cards/ Logic Cards/ other microprocessor based intelligent systems. The Vendor agrees to declare with each shipment, whether during initial supply stage or subsequent repairs, diagnostics or upgrades, that it shall be solely responsible for any Criminal and/ or Civil Liabilities arising from failures due to such malware/bug. The vendor further agrees to send a digitally signed statement by email, detailing SHA-256 checksum of all firmware/software components installed during any field/factory activity.
- j) The Vendor agrees not to access through use of WiFi/ Bluetooth based networking to any device anywhere in the controlled network. All Bluetooth/ WiFi devices shall be disabled from associated firmware and Operating System in applicable devices of the controlled network.
- k) The vendor agrees to submit details of all devices equipped with Serial Ports (RS232C/RS485/USB etc including with Optical interface), Virtual Serial Ports and Serial over Ethernet. Only POWERGRID permitted devices shall be attached to serial ports. The Vendor agrees to provide systems to log details of any serial devices connected during the operation of the equipment.

### **3. Protection of Confidential Information**

#### **a. Use**

The Receiving Party understands and acknowledges that the Confidential Information has been developed or obtained by the Disclosing Party by the investment of significant time, effort and expense, and that Confidential Information is a valuable, special and unique

**Annexure Cyber Security – Non Disclosure Agreement – Rev 01**

asset of the Disclosing Party. Therefore, the Receiving Party agrees to hold in confidence and not to disclose the Confidential Information, to any person or entity without similar obligations agreed between the Receiving Party and such person or entity. The Receiving Party will use the same standard of care it would use to secure and safeguard its own confidential information of similar importance, but in no event less than reasonable care.

**b. No copying.**

The Receiving Party will not copy or modify any Confidential Information without the prior written consent of the Disclosing Party, except where such copy or modification is required for the purpose of the execution of the contract. Any permitted reproduction of confidential information must contain all confidential or proprietary legends which appear on the original. The Receiving Party shall immediately notify the Disclosing Party in the event of any loss or unauthorized disclosure or use of the confidential information.

**c. Permitted disclosures.**

The Receiving Party shall permit access to the Disclosing Party's confidential information solely to the Receiving Party's Representatives and contractors who (i) have a need to know such information; and (ii) have signed the specified confidentiality agreement / similar contract conditions in favour of Receiving Party

All staff of Receiving Party (on-roll or outsourced) shall be bound by the terms of this Agreement. The Vendor agrees to individually authorize each of the member of staff assigned with the project, binding them individually with the terms of similar to this Agreement during and also post-employment.

**d. Additional obligations.**

The Receiving Party shall

- (i) notify the Disclosing Party promptly of any material unauthorized possession, use or knowledge, or attempt thereof, of the Disclosing Party's confidential information by any person or entity which may become known to the Receiving Party;
- (ii) promptly furnish to the Disclosing Party full details of the unauthorized possession, use or knowledge, or attempt thereof;
- (iii) use reasonable efforts to assist the Disclosing Party in investigating or preventing the recurrence of any unauthorized possession, use or knowledge, or attempt thereof, of confidential information;
- (iv) use reasonable efforts to cooperate with the Disclosing Party in any litigation and / or investigation against third parties deemed necessary by the Disclosing Party to protect its proprietary rights;
- (v) promptly use all reasonable efforts to prevent a recurrence of any unauthorized possession , use or knowledge of confidential information;
- (vi) comply with the directives of authorized agencies of Government of India, through appropriate technical configurations and custom modifications to achieve compliance as sought by them from time to time; and
- (vii) extend its services as may be required, at least once annually, during the Information Security audits.

**e. Unauthorized Disclosure of Information.**

If it appears that the Receiving Party has disclosed (or has threatened to disclose) Confidential Information in violation of this Agreement, the Disclosing Party shall be entitled to an injunction to restrain the Receiving Party from disclosing, in whole or in part, the Confidential Information. The Disclosing Party shall not be prohibited by this provision from pursuing other remedies, subject to suitable notice of the same to Receiving Party and Receiving Party wilfully neglecting such notice or duties under the Agreement after such notice including a claim for losses and damages.

**f. Exceptions**

The following shall not be considered as Confidential Information:

- (a) Any information that the Receiving Party can show by documentary evidence was in its possession prior to the disclosure to it hereunder; or
- (b) Any information that comes into the possession of the Receiving Party's Representatives, from another party who is under no obligation to the other to maintain confidentiality of such information; or
- (c) Any information that becomes generally known other than through the fault of the Receiving Party,
- (d) Any particular portion of the Confidential Information which was developed by Receiving Party's Representatives independently of and without reference to any Confidential Information or other information that the Disclosing Party has disclosed in confidence to any third party.
- (e) Information available in the public domain whether in tangible or intangible form.
- (f) Information that is not proprietary or confidential to the Disclosing Party but an

**Annexure Cyber Security – Non Disclosure Agreement – Rev 01**

information received from third party not connected to the Project.

(g) Information that has not been marked by the Disclosing Party as “Confidential”.

The burden of proving these exceptions to the provisions of this Agreement resides with the Receiving Party.

**4. Remote Support.** Remote Support shall be permitted only as per POWERGRID ISO27001 Policy and Procedures. Further, remote support will only be permitted from within geographical boundaries of India. POWERGRID reserves the right to only permit the remote support with the presence of POWERGRID’s authorized representative at the remote end.

**5. Compelled Disclosure.** In the event that Receiving Party or any of Receiving Party’s Representatives is requested or required (by oral questions, interrogatories, requests for information or documents, subpoena, civil investigative demand or similar incidents) to disclose any of the Confidential Information to the authorities as per mandatory law, it is agreed that Receiving Party or Receiving Party’s Representatives, as the case may be, will provide Disclosing Party with prompt notice of such request(s) so that Disclosing Party may seek an appropriate protective order or other appropriate remedy and/or waive compliance with the confidentiality provisions of this Agreement. In the event that such protective order or other remedy is not obtained, or Disclosing Party grants a waiver hereunder, Receiving Party or Receiving Party’s Representatives may furnish that portion (and only that portion) of the Confidential Information which Receiving Party is legally compelled to disclose and will exercise reasonable efforts to obtain assurance that confidential treatment will be accorded any Confidential Information so furnished.

**6. Information Security Audit.** POWERGRID reserves the right to undertake a second party / third party Information Security Audit at any point as may be required, to ascertain the risk/ vulnerability/ threats and the Vendor agrees to take necessary corrective measures in-situ or within a defined time frame, as the case may be.

**7. Term and Termination**

This Agreement shall be valid during the contractual period w.e.f. the date of signing of the main contract agreement.

**8. Return of Confidential Information.**

Upon the written request of the Disclosing Party, the Receiving Party shall return to the Disclosing Party all written materials / digital media containing the Confidential Information to the extent possible by the Receiving Party. The Receiving Party shall also deliver to the Disclosing Party written statements signed by the Receiving Party certifying that all materials have been returned within ~~five (5)~~ thirty (30) days of receipt of the request. Any unreturned Confidential Information shall be required to be maintained with similar confidentiality obligation for 10 years or as per applicable law, whichever is longer.

**9. Remedies.**

Receiving Party acknowledges that money damages may be incalculable and an insufficient remedy for any breach of this agreement by Receiving Party and that any such breach may cause Disclosing Party irreparable harm. Accordingly, Receiving Party

**Annexure Cyber Security – Non Disclosure Agreement – Rev 01**

also agrees that, in the event of any breach or threatened breach of this Agreement, Disclosing Party, in addition to any other remedies at law or in equity it may have, shall be entitled, without the requirement of posting a bond or other security, to equitable relief, including injunctive relief and specific performance.

**10. Relationship of Parties**

Neither party has an obligation under this Agreement to purchase any service or item from the other party, or commercially offer any products using or incorporating the Confidential Information. This Agreement does not create any agency, partnership or joint venture.

**11. No Grant of Proprietary Rights**

The Receiving Party recognizes and agrees that, except as expressly and specifically set forth in this agreement, nothing herein shall be construed as granting any proprietary right, by license, implication, estoppel or otherwise, to any of the Disclosing Party's, confidential information, trade mark, trade name or to any invention or any patent right that has issued or that may issue based on such confidential information. All information disclosed is provided "as is" without any warranties of any kind.

**12. Governing Law**

This Agreement shall be governed by and interpreted in accordance with the Indian laws without regard to its conflict of law principles. In particular, the provisions of Information Technology Act 2000, and rules framed thereunder shall be applicable. Further the outline of system level requirements shall be in conformance to IS:16335-2015 standard. The applicable Information Security Policy shall be the ISO-27001:2013 policy and procedures of POWERGRID as modified from time to time.

**13. Jurisdiction and Venue.** In connection with any litigation arising hereunder, Parties hereby

- (i) irrevocably and unconditionally submit to the exclusive jurisdiction of courts in Delhi and
- (ii) Further that disputes if any, shall be dealt with as per the provisions of the dispute settlement clause mentioned in the contract / General Conditions of Contract (GCC).

**14. General Provisions.**

- (a) This Agreement sets forth the entire understanding of the Parties regarding confidentiality. Any amendments must be in writing and signed by both parties.
- (b) This Agreement is intended to facilitate only the exchange of Confidential Information and is not intended to be, and shall not be construed to create a teaming agreement, joint venture association, partnership, or other business organization or agency arrangement and no Party shall have the authority to bind the other without the separate prior written agreement thereof.
- (c) This Agreement contains the entire agreement and understanding between the Parties hereto relating to the subject matter hereof and supersedes all other prior agreements and understandings, both written and oral, between the Parties with respect to the subject matter hereof. This Agreement may be executed in several counterparts, each of which will be

**Annexure Cyber Security – Non Disclosure Agreement – Rev 01**

deemed an original, and all of which taken together will constitute one single Agreement between the Parties with the same effect as if all the signatures were upon the same instrument.

**IN WITNESS WHEREOF**, the parties hereto have executed this Agreement at ..... by their duly authorized representatives as of the date first set forth above.

**Power Grid Corporation of India Limited**

**Signature:** \_\_\_\_\_

**Signature:** \_\_\_\_\_

**Name:**

**Name :**

**Title**

**Title :**

