TERMS AND CONDITIONS OF CONTRACT (TCC) (PART-B)

"FRAMEWORK AGREEMENT FOR ANTIVIRUS SOLUTION FOR BHEL"

BHARAT HEAVY ELECTRICALS IMITED

TERMS AND CONDITIONS OF CONTRACT (TCC)

1.0 OVERVIEW

1.1) Introduction:

Established in 1964, Bharat Heavy Electricals Limited (BHEL) is the largest engineering and manufacturing enterprise in India in the energy and infrastructure sector with the capability to manufacture the entire range of power plant equipment.

BHEL manufactures over 180 products under 30 major product groups and caters to core sectors of the Indian Economy viz., Power Generation & Transmission, Industry, Transportation, Telecommunication, Renewable Energy, etc. The wide network of BHEL's 17 manufacturing divisions, four Power Sector regional centers, over 100 project sites, eight service centers and 18 regional offices, enables the Company to promptly serve its customers and provide them with suitable products, Systems and services. The high level of quality & reliability of its products is due to the emphasis on design, engineering and manufacturing to international standards by acquiring and adapting some of the best technologies from leading companies in the world, together with technologies developed in its own R&D centers.

BHEL's vision is to become a world-class engineering enterprise, committed to enhancing stakeholder value. The company is striving to give shape to its aspirations and fulfill the expectations of the country to become a global player.

Currently, BHEL has around 100 plus ongoing projects.

1.2) Information Technology in BHEL:

In BHEL, Information Technology has deeply penetrated all the functional areas and it is suitably deployed in various facets of company's operations. The company has substantially introduced IT in its Engineering, Manufacturing, and Materials Management & Production functions. IT initiatives have been taken up so as to meet the emerging demands of the business challenges of the New Economy.

1.3) Infrastructure:

All Units and Divisions have their own computing resources as per their perceived needs. Local connectivity of different departments and groups have been achieved through state of the art LAN technologies (Giga Bit Ethernet/ Fiber optics). BHEL has established its Corporate Level Wide Area Network on MPLS based technology linking Manufacturing Units, Service Divisions, Project Sites and offices. This has enabled exchange of information across the Units / Divisions in a secured way. This network MPLS interconnects all locations of BHEL across the country on OFC/RF Links/VSATs.

1.4) Business Applications & Other software used:

Integrated end to end Business Applications, largely rendered in web, have been developed and used at various manufacturing units within various processes from receipt of work order to dispatch of equipment.

A number of Web based applications are being developed and implemented in various functions across various Units/Regions/Business Sectors for their local operations. Some Corporate wide web applications have also been developed over a period of time, mostly. RDBMS & J2EE is the favored technology for application development.

All engineering centers are well equipped with engineering workstations using advance Engineering Software for Designing, Modeling, Analysis and Drafting etc. Electronic Depositories, with appropriate work flow & change control, have been implemented particularly for Engineering Documents at major units.

1.5) Information Systems and ERP in BHEL:
Currently, major Manufacturing Units of BHEL have implemented Information Systems (either based on SAP ERP or developed in-house) to meet their Unit specific business requirements while Business Sectors and other Manufacturing Units/ Divisions and Regions have moderate level of computerization in place.

BHEL has implemented SAP for its unit level operations at Trichy, Hyderabad, EDN Bangalore, EPD Bangalore and HPVP Vizag. Also SAP-HCM module has been implemented in BHEL at Corporate Level.

1.6) Existing Network Infrastructure:
BHEL is using MPLS connectivity from multiple service providers to connect their locations. The BHEL locations are connected through multiple connectivity options with redundancy as required.

2.0 OBJECTIVE

The objective is to monitor and protect all the endpoints deployed across BHEL through central deployment of antivirus solution. This solution shall be integrated with the Cyber Security Operations Centre (Cyber SOC) of BHEL. As such BHEL intends to implement an Antivirus solution.

3.0 GENERAL SCOPE OF WORK

3.1	The entire scope of work covered in this document and subsequent instructions to the Successful Bidder post award shall be deemed to be Successful Bidder's obligation. The scope of work / specifications detailed herein are indicative only. Anything not specifically mentioned but considered essential for effective implementation of antivirus solution shall be deemed to be covered under existing scope without any additional financial implication to BHEL.
3.2	The successful bidder shall take back to back support from OEM for the entire contract period.
3.3	The successful bidder shall install and configure the antivirus servers / management servers / intermediatory servers (BHEL shall provide the hardware along with Windows / Linux operating system) for getting updates automatically from the internet at the locations as per Annexure - I. Any other additional hardware or software components required for the successful configuration of the antivirus servers / management servers / intermediatory servers, has to be supplied by the successful bidder. In case of appliance based solution, the appliance to be provided by the bidder
3.4	The successful bidder shall carry out the migration of the logs of the existing antivirus solution to the new solution being implemented, without any loss of data
3.5	The successful bidder shall supply, install (including uninstallation of existing endpoint agent without any loss of data and services), configure and successfully test the endpoint agent for getting updates automatically from the antivirus servers / management servers / intermediatory servers / internet.

3.6	The successful bidder shall provide the mass deployment tool, if required, for endpoint agent rollout.
3.7	The successful bidder shall carry out the migration activity in case of hardware refresh / failure during the contract period. The migration shall include but not limited to uninstallation of endpoint agent from outgoing hardware, installation, configuration and successfully testing the endpoint agent on new hardware for getting updates automatically from the antivirus servers / management servers / intermediatory servers / internet
3.8	The successful bidder shall be responsible for regular updates / upgrades of the software supplied for the entire contract period.
3.9	The successful bidder shall provide the escalation mechanism for the support for the entire contract period.
3.10	The successful bidder shall provide OEM Technical Account Manager for this solution and he must be available 24 x 7 through phone, email or by being visiting site physically depending upon the severity of the problem.
3.11	In case of critical/severe virus threats, updates to be carried out immediately. In case of outbreak like situation (any other scenario – more than 10 end points infected etc.) the successful bidder has not only to provide immediate solution but to also take measures to contain the problem. If required, extra manpower may be deployed to bring situation in control without any extra cost.
3.12	The successful bidder shall provide Resident Engineer at locations as per Annexure-I. The Resident Engineer should be OEM certified support engineer.
3.13	The Resident Engineer at one location will also attend the calls of other BHEL locations in nearby region.
3.14	The Resident engineers shall be available as per BHEL timings on all working days as per BHEL calendar. However, during urgency, resident engineers may be asked to come on holidays.
3.15	The successful bidder shall provide 5 days training to BHEL through OEM certified trainer on technical aspects of endpoint management, antivirus servers / management servers / intermediatory servers.
3.16	For the endpoints having unsupported/end of life OS, the successful bidder shall provide the antivirus support.
3.17	The successful bidder shall also provide the endpoint agent for Windows Server 2012(R2), Windows Standard and Data Center Edition and later releases during the contract period. The management of these agents shall be provided and configured as part of solution.

3.18	The successful bidder shall provide the antivirus logs, if required, to BHEL at the end of the contract period.

4.0 Framework Agreement

4.1The framework agreement (FA) shall be for a period of six (06) months.

4.2 Modalities of contract

4.2.1 BHEL intends to implement the antivirus solution for a period of three (03) years.

4.2.2 BHEL also intends to buy antivirus licenses for home endpoints for a period of three (03) years.

4.2.3 The Purchase Order(PO) shall be placed by respective locations and therefore, the payment shall be done by respective Units accordingly.

4.2.4 The common end date for all the Purchase Order(PO) shall be 31st Dec 2023.

4.2.5 Once Rates are finalized, the Framework agreement (FA) rates shall be valid for a period of 6 months from the date of award of Framework agreement (FA) during which respective BHEL units shall place PO for their requirements for supplying Antivirus Solutions for a period of upto 36 months however having common end date of 31.12.2023.

5.0 Terms of Payment:

As per Clause 6.0 of SCC.

6.0 Delivery, installation and configuration timelines:

Item	Delivery, installation and configuration
Antivirus Server	Within 7 days after the date of award of Purchase Order(PO).
Server Endpoints	Within 7 days after the date of award of Purchase Order(PO).
Desktop / Laptop endpoint	Within 15 days (where the no. of licenses is less than or equal to 2000) after the date of award of Purchase Order (PO). whichever is later. Within 30 days (where the no. of licenses is more than 2000) after the date of award of Purchase Order(PO), whichever is later.

7.0) Service Level Agreement (SLA):

Item	Support required	Resolution time	Penalty
Antivirus Server	24x7	Within 24 hrs of logging the complaint	Per day ATS charges for the no. of PCs updating from the antivirus server after 24hrs

Endpoint agent in PCs / Laptops	12x7	Within 12 hrs of logging the complaint	ATS charges for no. of PCs in which Antivirus is not functioning. After 7 business days, additionally Rs.50 per day will be deducted.
Antivirus agent in Servers	24x7	Within 12 hrs of logging the complaint	ATS charges for no. of servers in which Antivirus is not functioning. After 1 business day, additionally Rs.100 per day will be deducted.

Note: Deduction towards penalty for antivirus server and antivirus agent shall be limited to quarterly ATS charges as per the contract for that quarter for that Unit.

Description	**Support Required**	**Parameter**	**Penalty**
Resident Engineer(RE) Availability	Onsite Availability as per BHEL timings on all working days as per BHEL calendar	Absence of Resident Engineer without any substitute	RE charges for no. of days absent without any substitute.

8.0 Special Clauses:

8.1 All the licenses provided by the successful bidder shall be in the name of BHEL.

8.2 The license quantity may vary +-10%.

8.3 The successful bidder shall get the OEM to analyse the advisories received from CERT-In, STQC & other government agencies/ trusted sources regarding endpoint protection and provide the action within 24hrs.

8.4 If services in one or more locations (Units/divisions) are not satisfactory, BHEL will have the right to terminate the contract for said services in full or part for that location at the risk and cost of Vendor. At other locations services may continue. In no case BHEL's work should suffer.

9.0 Requirement Details [Annexure-1]:

S. No.	Unit	No. of Endpoints (PCs/Laptops)	No. of Servers (Windows based)	Total no. of Licenses Required	No. of Resident Engineer and location	Antivirus / Management / Intermediatory Server Location
1	BAP, RANIPET	1591	83	1674	1	
2	HEEP & CFFP, HARIDWAR	2535	45	2580	1	1
3	CFP, RUDRAPUR	146	2	148		
4	CORP. OFFICE	930	34	964	2	1
5	CORP. R&D, HYD.	385	10	395		
6	EDN, BANGALORE	1773	15	1788	1	1
7	EMRP, MUMBAI	45	2	47		
8	EPD, BANGALORE	370	5	375		
9	FSIP, JAGDISHPUR	342	6	348		
10	HEP, BHOPAL	3180	23	3203	1	1
11	HERP,VARANASI	155	5	160		
12	HPEP, HYDERABAD	2650	150	2800	1	2
13	INDUSTRY SECTOR	240	30	270		
14	IO, NEW DELHI	78	2	80		
15	ISG, BANGALORE	440	10	450		
16	IVP, GOINDWAL	123	2	125		
17	PIPING CENTRE	185	10	195		
18	PPPU, THIRUMAYAM	250	10	260		
19	PS-ER, KOLKATA	650	20	650		
20	PS-HQ	86	4	90		
21	PS-Mktg	170		170		
22	PS-NR	450	0	450		
23	PS-PEM	700	22	722		
24	PS-PMG	80	0	80		
25	PS-SR, CHENNAI	630	30	660		
26	PS-SSBG	149	0	149		
27	PS-TS	90	4	94		
28	PS-WR, NAGPUR	600	15	615		
29	ROD	200	1	201		
30	TBG	550	5	555		
31	TIRUCHY	3420	70	3490	1	1
32	JHANSI	766	10	776		
33	HPVP, VISAKHAPATNAM	393	5	398		
				24962	8	7

10.0 Technical Specifications [Annexure-2]:

Make and model of the product quoted			
Product SKU			
Antivirus Specifications			**Bidder's Compliance (Yes/No)**
General Feature			
1	The solution should be purpose build, unified agent for all features with on-premise architecture		
2	The solution should be deployable for Virtual solution like vmware/ hyper-V and VDI.		
3	The solution should have tamper protection against malware that attempt to disable security measures.		
Endpoint Protection			
4	Malware Protection	The solution must protect against all kinds of viruses, Trojans, worms and any other forms of exploits by blocking files (executable/malicious) in real-time.	
5		The solution should be capable of detecting malware by scanning multi levels of compressed files.	
6		The solution should be able to detect malware in the files packed using real-time compression algorithms as executable files.	
7		The solution must protect the endpoints on the network using stateful inspection.	
8		The solution shall also protect against other malwares such as Spyware, adware, dialers, joke programs, remote Access and hacking tools, which can be used with malicious intent	
9		The solution shall be able to scan only those file types which are potential virus carriers (based on true file type).	
10		The solution should be able to do on-access scan and heuristic (behavioral) scan of the files.	
11		The solution should be able to detect suspicious network traffic. It shall allow blocking of all traffic from the originating endpoint.	
12		The solution must provide the flexibility to create firewall rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users.	
13	Web reputation	The solution shall provide detection and blocking of Command and control (C&C) traffic and prevent access of malicious and suspicious websites.	
14	Browser Exploit Protection	The solution should identify the web browser exploits and prevent the exploits from being used to compromise the web browser.	
15	Outbreak Prevention	The solution must provide outbreak prevention to limit/deny access to specific shared folders, block ports, and deny write access to specified files and folders on selected endpoints in case there is an outbreak	
16		The solution should have a manual outbreak prevention feature that allows administrators to configure port blocking, block shared folder, and deny writes to files and folders manually	

17	Machine Learning	The solution should provide machine learning to detect emerging unknown security threats, which does not have any signatures	
18		The solution should be able to score both good and bad behaviors of unknown applications, enhancing detection and reducing false positives without the need to create rule-based configurations to provide protection from unseen threats i.e. zero-day threats.	
19	Sandbox Integration	The Solution should have option to integrate with Sandboxing Solution for detection of zero day malwares and Ransomware attacks.	
20	Application Control	The solution should provide application whitelisting using regular expression, reputation score and certificate. The solution should be able to create user defined whitelist.	
21		The solution should provide file reputation and global usage details to allow cross checking of known good/bad files.	
22		The solution should block any changes / tampering of whitelisted applications / codes, like DLL's, System files, registry etc.	
23	Behavioral Monitoring	The solution shall protect against unauthorized encryption (ransomware) or modification and provides detailed information.	
24		The solution shall protect against fileless malware and shall utilize behavioral techniques to detect malware based on the behavior of the file.	
25		The solution shall be able to detect and block process execution chains. It should be able to detect when a malicious application tries to execute a trusted application.	
26	Data Exfiltration Detection	The solution should be able to prevent mass mail worms.	
27		The solution should have capability of anti-spoofing i.e., prevent the transmission of data to a hacker system who has spoofed the IP or Mac Address of the endpoint.	
28	Action Taken	The solution should have the capability to repair, quarantine, block, delete or process kill on detection of malware / Suspicious activity.	
29		Damage rollback - The solution should allow removal of detected malicious file, affected registry entries and any new files dropped by malware.	
30		User Alerting - The solution shall provide alerts to users in case of any security incident along with a course of action, in case of any failure to clean	
	Device Control/ Preventing Data Leakage		
31		The solution should automatically scan external devices (CDs/DVDs, USB devices) as soon as they are accessed to PC, Server, Laptop	
32		The solution should automatically allow standard USB Keyboards, USB Printers, USB Scanners and mouse (Human interface devices)	
33		The solution should allow blocking of physical devices on USB such as removable storage devices, Bluetooth, Wi-Fi network cards, and other plug and play devices.	

34		The solution shall provide management of plug and play devices and allow restrictions on their usage to Monitor, Block or make the device Read-Only along with the option of providing exceptions	
35		The solution shall allow classification of USB devices as allowed / not allowed USB devices. The solution shall allow exclusion of allowed USB devices by using their vendor ID, product ID or serial number	
36		The solution shall provide logs of the device control feature to detect attempts of connecting not-allowed devices	
37		The solution should provide the functionality of file transfer logging and audit-trail capabilities, the log shall include hostname, file name, transfer direction, file size, etc.	
38		The solution should prevent data loss via USB	
		Endpoint Detection and Response (EDR)	
39		The solution should provide context-aware endpoint detection and response (EDR). Custom detection, intelligence, controls, recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack.	
40		The solution should be able to perform threat sweep based on the threat feeds (IP Address, Files, URLs, Domain)	
41		The solution shall perform sweep across endpoints using user-defined search criteria like User Name, File - Name, File - Hash, IP address, Hostname.	
42		The solution should be able to perform the root cause analysis of an incident.	
43		The solution should be able to search and analyze data regarding critical breach or potential attack.	
44		The solution should provide the advance response capabilities like Kill process, Isolate device, Block process.	
45		The solution shall allow consuming of root cause like domains, file-hashes and shall also allow blocking of the files/file-hashes/domains/URLs identified by the root cause.	
		Security Definition Updates	
46		The OEM should have a 24/7 security service update and should support real time updates of the system on release.	
47		The solution should have a central server with high availability for getting the updates from the OEM. The updates shall flow from the central server to the endpoints through the multiple intermediatory servers.	
48		The central / management server should be able to download updates from different source if required, which could be the vendor's update server, any other server.	
49		The solution must have the flexibility to roll back the Virus Pattern and Virus Scan Engine if required via the web/management console.	
50	Incremental Updates	The solution should allow for incremental update of definitions to reduce the network traffic.	

51	Roaming Clients	The solution should provide a mechanism for updates of roaming devices or clients which are not connected to corporate network.	
52		When the PC is connected to network after a long period, the endpoint agent should get updated by itself once it is connected to the network.	
		Management	
53		The solution should be managed from a single centralized console and should provide integrated management for endpoint security solution. It should be able to deploy, manage, and update agents and policies from one management platform.	
54		The solution shall provide the enterprise-wide visibility of the status of all the deployed components from a central dashboard. The dashboard shall provide a summarized view to analyze top threats & summary of malware traffic or any other threats	
55		Multiple Management servers should be installed in high availability mode (active/standby or active/active). The servers should be able to synchronise between them. Any additional clustering software/hardware required should be bundled with the solution.	
56		All components of solution should be managed from a centralized server/console.	
57		The solution should provide a central view of threat detections, logs, threat intelligence for endpoints.	
58		The solution shall have provision to centrally manage the scan schedule and frequency for endpoints. The solution must support logical grouping of various endpoints into separate groups with separate AV policies. Endpoints should have an option to postpone the scan.	
59		The solution should be able to do full scan of files / folders with a choice of specifying directories and file extensions not to be scanned.	
60		Host user (normal/admin) should not be able to uninstall/remove the endpoint security agent.	
61		The solution shall provide hierarchical grouping of machines and policy deployment	
62		The solution should support IPv6.	
63		The solution shall provide detection of endpoints that do not have the agent installed	
64		The solution must have readymade policies including –	
		a) To make all removable drives read only ,	
		b) To block program from running from removable drives	
		c) Protect clients files and registry keys	
		d) Block modifications to host files	
65		Endpoint Platforms should support Windows 8.1/10 and later releases during contract period.	

66	Agent Installation	Should be able to deploy the endpoint agent using the following mechanisms: a) Client Packager (Executable & Microsoft Installer (MSI) Package Format) b) Web install page or through the Web Console of the management station. c) Login Script Setup d) Remote installation e) From a client disk image f) Inbuilt capability or through AD or through SCCM All the client components should be installed using the single client package.	
67	Role Based Administration	Central management console should support role based access control	
68		The solution shall support multiple administrator accounts. Each administrator account shall be configurable with the desired level of management privileges for different components	
69	Log Management	The solution shall be able to receive logs from the managed components and endpoints and store them centrally. The solution shall also provide the functionality to integrate these events with SIEM.	
70		The endpoint client should store event data generated while it is disconnected from the corporate network and forwards it on reconnection	
71	Endpoint Quarantine	The solution shall have provision of restricting network access to an infected endpoint as per administrator requirement	
Reporting			
72	The solution should support report customization and allow viewing directly using a web browser and/or as a dashboard using the same management console for the endpoints.		
73	The solution should support atleast the following formats for exporting data: CSV, HTML, XML, Acrobat PDF		
74	The solution must be able to send notifications whenever it detects a security risk on any endpoint or during a security risk outbreak, via E-mail or SNMP trap		
75	The solution should have a feature that notifies administrators about security risk or viruses outbreaks. This should be configurable on number and type of occurrences of new risks or viruses or logs and the time period within which they must occur to trigger the notification on any computer, on a single computer, or on distinct computers.		
76	Solution should be able to generate downloadable reports from existing and customizable templates.		
77	The solution shall provide the feature to send the reports via E-mail on fixed time intervals or event driven basis.		
78	The solution should provide the customizable/standard reports group/Unit wise		
79	The solution should be able to generate a reports of clients which should include fields		
80	a.Username in computer		
81	b.Hostname		
82	c. Network parameters		
83	d.Definition update in client		
84	e.Client status Online/Offline		
85	f. Client version/ Agent version		
86	g. Outdated/ Unmanaged endpoints		

11.0 Unpriced rate schedule [Annexure-3]:

S. No.	Item	Endpoint (PCs / Laptops / Servers) (A)	Per license cost (B)	Total license cost (C=A*B)
1	Incremental Upgrade/ Cross Platform license cost of Endpoint (PCs / Laptops / Servers) Protection (as per Scope of Work)	24962		

	Item	Endpoint (PCs / Laptops / Servers) (A)	Per month per license cost (B)	Total ATS cost (D=A*B*36)
2	Annual Technical Support(ATS) charges	24962		

	Item	No. of REs (A)	Per month per RE cost (B)	Total RE cost (E=A*B*36)
3	Resident Engineer (RE) charges	8		

Total Cash Outflow for 36 months (C+D+E)	

All prices should be exclusive of taxes.

Total offered price in words (C+D+E): Rs……

……

S. No.	Applicable taxes	%age

Note:

1. The rate should be quoted in INR.
2. Evaluation of L1 will be decided on the basis of Total Cash Outflow for 36 months (Excl. Taxes) (C+D+E).
3. The total cost should be mentioned in this format. The prices should be fixed and should avoid use of vague terms as “Extra as applicable’.

Seal & Signature of the Company

12.: Non-Disclosure Agreement [Annexure – 4]

This Agreement is made and entered into as of the last date signed below (the "Effective Date") by and between **Bharat Heavy Electricals Ltd.(BHEL),** a Public Sector Organization having its principal place of business at BHEL House, Siri Fort, New Delhi - 110049 and _____, a _____ corporation, hereinafter called "The Bidder", whose principal mailing address is _____ .

WHEREAS in order to pursue the mutual business purpose of this particular project as specified in Bid document to implement a Project Management solution, **BHEL** and the Bidder have an interest in participating in discussions wherein either Party might share information with the other that the disclosing Party considers to be proprietary and confidential to itself ("Confidential Information"); and

WHEREAS the Parties agree that Confidential Information of a Party might include, but not be limited to that Party's:

1. business plans, methods, and practices;
2. personnel, customers, and suppliers;
3. inventions, processes, methods, products, patent applications, and other proprietary rights; or
4. specifications, drawings, sketches, models, samples, tools, computer programs, technical information, or other related information;

NOW, THEREFORE, the Parties agree as follows:

1. Either Party may disclose Confidential Information to the other Party in confidence provided that the disclosing Party identifies such information as proprietary and confidential either by marking it, in the case of written materials, or, in the case of information that is disclosed orally or written materials that are not marked, by notifying the other Party of the proprietary and confidential nature of the information, such notification to be done orally, by e-mail or written correspondence, or via other means of communication as might be appropriate.
2. When informed of the proprietary and confidential nature of Confidential Information that has been disclosed by the other Party, the receiving Party ("Recipient") shall, for a period of three (3) years from the date of disclosure, refrain from disclosing such Confidential Information to any contractor or other third party without prior, written approval from the disclosing Party and shall protect such Confidential Information from inadvertent disclosure to a third party using the same care and diligence that the Recipient uses to protect its own proprietary and confidential information, but in no case less than reasonable care. The Recipient shall ensure that each of its employees, officers, directors, or agents who has access to Confidential Information disclosed under this Agreement is informed of its proprietary and confidential nature and is required to abide by the terms of this Agreement. The Recipient of Confidential Information disclosed under this Agreement shall promptly notify the disclosing Party of any disclosure of such

Confidential Information in violation of this Agreement or of any subpoena or other legal process requiring production or disclosure of said Confidential Information.

3. All Confidential Information disclosed under this Agreement shall be and remain the property of the disclosing Party and nothing contained in this Agreement shall be construed as granting or conferring any rights to such Confidential Information on the other Party. The Recipient shall honor any request from the disclosing Party to promptly return or destroy all copies of Confidential Information disclosed under this Agreement and all notes related to such Confidential Information. The Parties agree that the disclosing Party will suffer irreparable injury if its Confidential Information is made public, released to a third party, or otherwise disclosed in breach of this Agreement and that the disclosing Party shall be entitled to obtain injunctive relief against a threatened breach or continuation of any such breach and, in the event of such breach, an award of actual and exemplary damages from any court of competent jurisdiction.

4. The terms of this Agreement shall not be construed to limit either Party's right to develop independently or acquire products without use of the other Party's Confidential Information. The disclosing party acknowledges that the Recipient may currently or in the future be developing information internally, or receiving information from other parties, that is similar to the Confidential Information. Nothing in this Agreement will prohibit the Recipient from developing or having developed for it products, concepts, systems or techniques that are similar to or compete with the products, concepts, systems or techniques contemplated by or embodied in the Confidential Information provided that the Recipient does not violate any of its obligations under this Agreement in connection with such development.

5. Notwithstanding the above, the Parties agree that information shall not be deemed Confidential Information and the Recipient shall have no obligation to hold in confidence such information, where such information:

   5.1. Is already known to the Recipient, having been disclosed to the Recipient by a third party without such third party having an obligation of confidentiality to the disclosing Party; or

   5.2. Is or becomes publicly known through no wrongful act of the Recipient, its employees, officers, directors, or agents; or

   5.3. Is independently developed by the Recipient without reference to any Confidential Information disclosed hereunder; or

   5.4. Is approved for release (and only to the extent so approved) by the disclosing Party; or

   5.5. Is disclosed pursuant to the lawful requirement of a court or governmental agency or where required by operation of law.

6. Nothing in this Agreement shall be construed to constitute an agency, partnership, joint venture, or other similar relationship between the Parties.

7. Neither Party will, without prior approval of the other Party, make any public announcement of or otherwise disclose the existence or the terms of this Agreement.
8. This Agreement contains the entire agreement between the Parties and in no way creates an obligation for either Party to disclose information to the other Party or to enter into any other agreement.
9. This Agreement shall remain in effect for the entire contract period unless otherwise terminated by either Party giving notice to the other of its desire to terminate this Agreement. The requirement to protect Confidential Information disclosed under this Agreement shall survive termination of this Agreement.

IN WITNESS WHEREOF:

FOR AND ON BEHALF OF **FOR AND ON BEHALF OF**

_____ **BHARAT HEAVY ELECTRICALS LTD.**

Signature: _____ **Signature:**_____

Name: _____ **Name:** _____

Designation: _____ **Designation:** _____

Date: _____ **Date:** _____

Witness **Witness**

1. 1.
2. 2.