CYBER SECURITY POLICY

1. Preamble

Cyberspace is a complex environment consisting of interactions between people, software, and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks. In the light of the growth of IT in the sphere of business, providing right kind of focus for creating secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices and networks, has become one of the compelling priorities. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the need of the hour. The objective of this policy is to ensure proper access to and usage of IT resources and prevent their misuse by the users.

2. Purpose

The purpose of the policy is to protect information and information infrastructure from cyber incidents through a combination of processes, guidelines, technology and cooperation. This policy governs the usage of IT Resources from an end user's perspective. This Policy defines what we want to protect and what we expect of our system users. It describes user responsibilities, such as protecting confidential information and creating nontrivial passwords and describes how we will monitor the effectiveness of our security measures.

3. Scope and Applicability

This policy applies to Tulsyan NEC Limited ("hereinafter referred as "TNECL" or "Company"). The Company also expects independent contractors and all involved in the value chain to uphold the principles of this Policy and urges them to adopt similar policies within their own businesses. It is mandatory for all users to adhere to the provisions of this policy.

4. Policy Statement

- The Company will protect all its stakeholders' interests by ensuring confidentiality, Integrity and continuous availability of information and information systems under its control which includes, but is not limited to electronic, print information etc., on servers, workstations, laptops, networking and communication devices, tapes, CDs, and information printed or written on paper or transmitted by any medium.
- The Company is committed to comply with all legal, regulatory, and contractual security obligations as may be applicable in cyberspace.
- The Company shall evaluate the business risk in information security perspective, prevent and reduce the risks to the maximum possible extent to avoid any undesired effects on business and Customers.
- The Company shall protect all Information from unauthorized access, use, disclosure, modification, disposal, or impairment whether intentional or unintentional, through appropriate technical and organizational security measures.
- The Company is committed to provide a virus free network and all Information processing systems will be auto updated with latest security patches from the manufacturer and loaded with an approved antivirus system.
- The Company shall provide framework to manage and handle security breaches, violations and business disruptions.
- The Company shall ensure continuity of critical operations in line with business and contractual requirements.
- A comprehensive backup procedure will be implemented to protect the business transactions. Backup tapes are to be verified by restoring the data for integrity as per SOP.
- Only authorized and licensed software will be allowed to be installed on corporate systems.
- Company network will be always protected from the Internet through a firewall.
- All third-party partners dealing with the Company who use IT information assets will be asked to sign a non-Disclosure agreement (NDA)
- All servers to be located in a secured area with restricted access.
- All information assets used in production will have either warranty or a support contract from the authorized vendor/ partner.
- All changes in the information processing system will be managed through the change control process.

5. Policy Compliance and Dissemination

a) It is the responsibility of all employees to adhere to the policy and the management has all rights to take disciplinary action in case of its violation.
b) Employees while operating from remote/outside organization network should strictly connect via VPN for accessing Applications and Corporate Network.
c) All employees should implement appropriate controls to ensure compliance with this policy by their users.
d) IT Department will ensure resolution of all incidents related to the security aspects of this policy by their users.
e) Users should not install any network/security device on the network without consultation with the Implementing Department.
f) The IT Department should ensure that training and awareness programs on use of IT resources are organized at regular intervals. To ensure security awareness amongst Employee to enable them to meet their security obligations. IT Department should ensure proper dissemination of this policy. IT Department may use newsletters, banners, bulletin boards, corporate Websites and Intranet etc. to increase awareness about this policy amongst their users.
g) Orientation programs for new recruits should include a session on this policy.

6. Monitoring and Review

The Company shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy. The Company for security related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on devices under intimation to the user. This includes items such as files, e-mails, and Internet history etc. Monitoring and review of this policy is governed by IT department. A periodic reporting mechanism to ensure the compliance of this policy should be established by the IT Department.

The Managing Director in consultation with the IT- Head is authorized to make modifications to this policy as and when deemed necessary and appropriate to ensure the ends of the policy being served.

7. Reporting and Remedy

Any questions or concerns on matters concerning Cyber Security shall be reported to IT- Head, Corporate. The Company assures through this policy that any Cyber Security Matters resulting from or caused by the Company's business activities shall be appropriately and adequately remedied in a time-bound manner.

* * *

This policy was approved by the Board of Directors on 21 June, 2023.