DATA PROTECTION POLICY

I. INTRODUCTION

In conducting business, the Company needs to gather and use certain information about individuals. This can include information on customers, suppliers, business contacts, employees and other people in the course of business who may have a relationship with the Company.

This policy helps protect the Company from very real and destructive data security risks. Additionally, this policy helps the Company and its subsidiaries comply with data protection laws. Each employee is responsible for knowing the procedures in this policy, complying with this policy and taking common sense measures to ensure that sensitive information is secured, protected and used only for proper purposes.

II. POLICY SCOPE

This policy applies to everyone who works for or with the Company, each of its subsidiaries, its partners and contractors. Each person has the responsibility to ensure that data is collected, handled and stored appropriately. Data must be handled, processed and disposed of in compliance with this policy and all applicable laws.

In the course of business, the Company handles a great deal of confidential and sensitive information. This policy applies to all data that the Company holds and handles relating to individuals as well as customers, suppliers and partners – including company information as well as information classified as personal data as described in IV below.

III. DATA POLICY IN GENERAL

a. DATA STORAGE

These rules apply to the storage of data no matter where or how it is kept. How to best protect data depends on how it is stored. Whether data is stored electronically or physically, on paper, disks or other medium, steps must be taken to protect the information and prevent it from being improperly deleted, misused or disseminated to unauthorized persons.

Confidential or sensitive information should never be left out or unattended where it can be seen by unauthorized persons. If data is printed on paper, the paper should be kept in a secure area where any unauthorized persons cannot access or view it. When possible, sensitive data should be kept in locked drawer of filing cabinet. All employees must take care when printing sensitive data. Paper and printouts should never be left where an unauthorized person can see them, including being left on the printer in an unsecured area. Anyone who prints a document containing sensitive information has the absolute responsibility to retrieve the document immediately to ensure it stays private.

Wherever data is electronically stored, it must be protected from unauthorized access, accidental deletion, and malicious hacking. All sensitive and confidential data must be password protected or have access restricted to authorized personnel only, without exception. Access to password protected information should never be given to unauthorized persons, nor should authorized employees share passwords to protected information. Any data stored on removable devices (i.e. CD/DVD or flash drive) should be kept locked away and secured

when not in use. Sensitive data should only be stored on designated drives and servers and should only be uploaded to approved cloud computing services. Any server that contains personal data should be kept in a secure location, away from the general population office space. Any server containing personal data must also be compliant with the rules in the policy. Personal data should never be kept or saved on individual computers or laptops unless the device is properly encrypted and secured by IT for this purpose. Personal data must never be stored on mobile devices, including tablets or smart phones. All Company servers and computers containing data should be protected by proper security software and firewall protections approved by IT.

b. Keeping the data accurate

All personal data used and kept by the Company should be up to date and accurate. Personal data should be held in as few places as possible to ensure that updates to the accuracy of the data are most effective. Employees should take every opportunity to ensure that personal data is accurate and up to date. As soon as inaccuracies are discovered, the data should be updated.

Any personal data that is redundant, trivial or outdated should be deleted. Personal data storages should be frequently monitored and cleaned out, updated and corrected, whenever necessary.

IV. PERSONAL DATA

Personal data is defined as “any information relating to an identified or identifiable natural person.” This can include information such as IP addresses, vehicle identification numbers, phone

numbers, email addresses, etc. Personal data is therefore, any information that directly identifies, or could lead to the discovery of, an individual. Personal data carries stricter regulation because of the possible damage it can do to an individual if the personal data is misused or abused. Processing personal data is any operation or set of operations which is performed on personal data or sets of personal data. Any time the Company is handling personal data, it must comply with the following procedures. If misused or mishandled, personal data can be at a risk of loss, corruption or theft.

- Any employee working with personal data should ensure the security of that data.
- Only where it is necessary should personal data be printed.
- If a document containing personal data is printed, it must be kept secure, such as in a locked office, filing cabinet or drawer and away from view of unauthorized persons.
- If personal data is being used electronically, employees should always lock their computer screens when they are away from their computer and use password protected files.
- No unnecessary personal data should ever be saved to a computer, cloud or server.
- All personal data transferred electronically must be encrypted.

a. Permissible Reasons to Retain Personal Data

All personal data retained about an individual must be accompanied by (i) a legal reason to do so, or (ii) the unequivocal, clear and unambiguous consent of the individual. Without consent of the individual, the Company must have one of the following reasons for retaining and processing the data; (1) necessary for the performance of, or entry into a contract with a particular data subject, (2) necessary for compliance with a legal obligation,

(3) necessary to protect the vital interests of the data subject or of another natural person, (4) necessary for the performance of a task in the public interest or in the exercise of official authority vested in the Company or (5) necessary for the purposes of legitimate interest pursued by the Company or a third party.

b. Rights of individuals

Each individual who has personal data processed or retained by the Company has the following rights in relation to his or her data; (1) each individual has the right to be informed by the Company when the personal data is being used and processed, (2) each individual has the right to access the data being used, free of cost, upon request at any time, (3) each individual has the right to request that his or her data be deleted from all computers, servers and backups, (4) each individual has the right to change or correct any data that is inaccurate or incorrect, (5) each individual has the right to restrict the processing or retention of his or her data.

c. Retention of personal data

In addition to needing to be accurate and available to the subject, the data must also be kept for only as long as truly necessary to accomplish whatever reason the data was being used for in the first place. Any employee or department in possession of and using personal data is responsible for making sure the data is kept accurately and for only as long as necessary.

V. DISCLOSURE

Under certain circumstances, the Company may be required to disclose sensitive, confidential or personal data, such as to law enforcement agencies or pursuant to other legal process, without consent of the person to whom the data pertains. Any questions regarding whether personal data must be disclosed to a government agency or other process of law should contact the Data Protection Officer for the applicable country or the law department.

VI. DATA PROTECTION OFFICER

The Company has appointed a Data Protection Officer ("DPO") to monitor and oversee the Company's compliance with this policy. In additional, each subsidiary subject to data privacy laws will also have a designated DPO for the same purpose. Questions on how to store data, what data should be stored or anything else related to data retention should be directed to the DPO.

VII. REPORTING VIOLATIONS

Each employee has the responsibility to ensure that the data being used by the Company is protected, accurate and kept up to date. Any violations of this policy could have serious consequences for the Company, its employees or its partners and customers. All Employees are expected to abide by and assist in upholding this policy. Any known or suspected violations of this policy should be immediately remedied and, if significant, reported to the Data Protection Officer.