INFORMATION SECURITY POLICY

Policy Statement

Maintaining the integrity of information stored in systems of **Motisons Commodities Private Limited** is a responsibility shared by all users of those systems. All Information Technology (IT) computing resource users are responsible for protecting Company's information, and are expected to be familiar with and comply with this policy. Violations of this policy may result in disciplinary action up to and including dismissal or expulsion.

Reason for Policy/Purpose

Information is a vital Company's asset and requires protection from unauthorized access, modification, disclosure or destruction. This policy sets forth requirements and a guideline for incorporation of information security practices into daily usage of Company's IT computing resources.

Who Needs to Know This Policy

Staff and Management

INFORMATION SECURITY POLICY

Policy/Procedures

Users of Company's IT computing resources are responsible for protecting the information processed, stored, or transmitted over or on those resources, and for incorporating the following practices into their daily usage of such resources.

A. Physical Security of IT Computing Resources

Company's technology assets require physical security measures to protect theft and loss of information. Further, if a computer is stolen it can take hundreds or even thousands of hours to re-create the information lost with the hardware. Users of IT resources should:

- ✓ Always use a security cable or locking device with laptop computers;
- ✓ Lock office doors when leaving;
- ✓ Never remove asset tags from equipment;
- ✓ Lock away laptops, PDAs or computer peripherals overnight in accordance with the Laptop Computer and Small Electronic Device Theft Policy;
- ✓ Configure a password-protected screen saver;
- ✓ Logout of the system when finished working; and
- ✓ Utilize a power-on password.

B. Passwords

Passwords are an integral part of overall security. To minimize the risk of a password being compromised and data being lost due to unauthorized access, employ the following:
- ✓ Do not use familiar names;
- ✓ Avoid using commonly known facts about yourself;
- ✓ Do not use words found in the dictionary;
- ✓ Use at least eight (8) characters;

- ✓ Utilize both letters and numbers;
- ✓ Use special characters if possible;
- ✓ Use upper-case and lower-case letters if possible;
- ✓ Combine misspelled words;
- ✓ Do not share your password with anyone;
- ✓ Never write down your password in an area where it can be linked to your specific computer or account;
- ✓ Do not store your password in a computer file;
- ✓ When receiving technical assistance, enter your password instead of telling it to the technology staff member; and
- ✓ If you ever receive a telephone call from someone claiming to need your password, report it immediately.

C. Securing Your PC

It is important to maintain Company's computers up-to-date with the latest electronic security measures to prevent viruses and worms from spreading from one machine to another, and to minimize the opportunity for hackers to damage or steal data. Accordingly, IT computing resource users should employ the following:

- ✓ Keep anti-virus software up to date.
- ✓ Keep systems patched.
- ✓ Use a personal firewall (recommended).

D. Confidentiality

All members of the Company's community are obligated to respect and in many cases to protect confidential data, and to follow the Data Classification Security Policy. The Company's strongly discourages storage of any confidential or sensitive data on any computer or network-attached device that has not been explicitly approved by Company's information security personnel. As such, IT computing resource users shall adhere to the following:

- ✓ Employ adequate encryption technology for sensitive or critical information

- ✓ Notify the management if sensitive or critical Company's information is lost or disclosed to unauthorized parties, if any unauthorized use of Company's systems has taken place, or if there is suspicion of such loss, disclosure or unauthorized use.

- ✓ DO NOT post Company's material such as software, internal memos, or other non-public information on any publicly-accessible computer unless first approved by the appropriate authority.

- ✓ DO NOT place Company's sensitive or critical information in any computer unless the persons who have access to that computer have a legitimate need-to-know the information involved.

- ✓ DO NOT save fixed passwords in web browsers or e-mail clients when using a Company's system. This may allow unauthorized users to access critical or sensitive information such that contained in Banner or the Enterprise Accounting System.

- ✓ DO NOT distribute internal critical or sensitive Company's communications to external entities that are not affiliated with the Company's. Only distribute to internal entities on a need to know basis.

✓ DO NOT establish Internet or other external network connections that could allow non-Company's users to gain access to Company's systems with critical or sensitive information unless prior approval has been received by the appropriate authority.

✓ DO NOT discuss information security-related incidents with individuals outside of the Company's, or with those inside the Company's who do not have a need-to-know.

E. Availability

Company's systems and IT computing resources are expected to be available and ready for usage. Accordingly, resource users are expected to limit usage of these resources to reasonable levels and should assist in making resources available as follows:

✓ Update system patches for IT computing resources that transmit, process or store critical or sensitive information.

✓ DO NOT probe security mechanisms at either the Company's or other sites unless authorized to do so by the Chief Security Office.

✓ DO NOT cause intentional harm to Company's -owned IT computing resources. This includes intentionally down loading from any source.

F. Integrity

Integrity means ensuring the soundness or completeness of information during its transmission, storage, generation, and/or handling. Information that is modified may be erroneous and could lead to poor business decisions. In order to maximize integrity, IT computing resource users shall adhere to the following:

✓ Screen all non-text files downloaded from the Internet with anti-virus software prior to usage to minimize the risk of corruption, modification or loss of data.

✓ Notify the Management immediately if passwords or other system access control mechanisms are lost, stolen or disclosed, or are suspected of being lost, stolen or disclosed.

✓ Forward information pertaining to security-related problems to the Chief Security Officer immediately. DO NOT personally redistribute system vulnerability information.

✓ Review information obtained from the Internet with caution. Before using free Internet-supplied information for business decision-making purposes corroborate and confirm the information by consulting other reliable sources.

✓ Secure personal computers via a locking feature such as a password-protected screen saver when walking away. Public computers with no critical or sensitive information, such as those in the library or in labs, are excluded.

For Motisons Commodities Private Limited

Authorised Signatory