Electronic communication and security policy

1. Introduction

TMI-SSP's electronic communication and information systems have become an integral part of company operation. On the one hand it provides an efficient and effective communications tool and on the other hand it provides access to company information which is vital for the quality of work produced, and the access to accurate and timely information, for operations as diverse as sales, and the credit control function. The operation of TMI-SSP is therefore dependent upon the systems used and information maintained electronically form part of company assets.

This policy describes the reasonable steps that need to be taken to ensure the security of critical information as well as TMI-SSP's standards and guidelines with regard to the use of the system. The policy furthermore explains TMI-SSP's right to access to and disclosure of usage of the system's used by TMI-SSP's employees and other users.

2. Scope and framework

This policy applies to all users of TMI-SSP's System and applies to all company information, and includes any electronically generated and stored information, and all handwritten, typed, printed, faxed, e-mailed or scanned information.

The policy provisions as contained in this policy document, and as amended from time to time, are by reference incorporated in TMI-SSP's service conditions.

3. Use of TMI-SSP's electronic communications system

3.1 Personal use of the system

3.1.1 As TMI-SSP provides the System's to assist employees in the performance of their jobs, usage of the System's should be restricted to company-related business only. Incidental and occasional personal use of the System's permitted but any personal usage will be subject to the same access and disclosure principles applicable to System usage, as described below. For example, employees should not use the TMI-SSP's e-mail for gossip, or for transmitting personal information of self or others, or for soliciting or proselytizing non-job-related commercial ventures, religious or personal causes.

3.1.2 TMI-SSP cannot protect the confidentiality of any private information stored on its infrastructure.

3.2 Content of communications

3.2.1 Each employee is responsible for the content of all text, audio or images that they place or send over the System. No e-mail or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else or someone from another company. All messages communicated on the System should contain the employee's name.

3.2.2 Any messages or information sent by an employee to another individual outside of TMI-SSP via an electronic network (e.g. bulletin board online service or Internet) are statements that reflect on TMI-SSP. While some users include personal "disclaimers" in electronic messages, there is still a connection to TMI-SSP, and the statements may be tied to TMI-SSP. Electronic communications should be carefully screened and so as not to harm TMI-SSP's image and should for instance not contain emotional responses to business correspondence or work situations.

3.2.3 All communications sent by employees via TMI-SSP's e-mail/Internet system must comply with this and other company policies and may not disclose any confidential or proprietary company information.

3.3 Generally unacceptable usages of the System

The System may not be used for:

3.3.1 Transmitting, retrieving or storage of any communications that may be seen as insulting, disruptive, or offensive by other persons, or harmful to morale, discriminatory or harassing in nature or materials that are obscene or sexually explicit. Examples of unacceptable transmissions include messages containing abusive, profane or offensive language, explicit messages, cartoons, or jokes, unwelcome propositions or love letters; ethnic or racial slurs, or any other message that can be construed to be harassment or disparagement of others based on, inter alia, their sex, race, sexual orientation, disability, physical attributes, age, national origin, or religious or political beliefs;

3.3.2 Any purpose which is illegal or against company policy or contrary to TMI-SSP's best interest. The System should not be used in such a manner that it damages Fleet Street Publications' public image;

3.3.3 Solicitation or any use of the System for personal gain.

3.4 Software and Hardware

3.4.1 No user may bring any hardware or software for use on TMI-SSP systems without the specific written permission of management and all downloaded software must be registered to TMI-SSP. No downloading of any unauthorized software is allowed as this may be illegal and may transmit computer viruses through the System.

3.4.2 No user may remove any hardware or software from the premises without written authorisation specific for each item.

3.4.3 All users should immediately follow any electronic instructions, (e.g. to log out) provided by TMI-SSP's security protection systems, and to follow all such instructions immediately and comprehensively.

3.5 Copyright Issues

Copyrighted materials belonging to entities other than TMI-SSP may not be transmitted by employees on the System. All employees obtaining access to other companies' or individuals' materials must respect all copyright and may not copy, retrieve, modify or forward copyrighted materials, except with permission, or as a single copy to reference only. Failure to observe copyright or license agreement may result in disciplinary action up to and including termination and in certain instances criminal prosecution.

3.6 Passwords and Security

3.6.1 All users are issued with an individual password, which will provide the access to the systems, appropriate to the user's role.

3.6.2 User access is given for the purposes of the user performing a defined role, and no attempt should be made by the user to gain any additional access to the information systems.

3.6.3 The password should be kept secret and not given to any other user.

3.6.4 Any contravention of policy while using the password will be deemed to be a contravention by that user.

3.6.5 Users should ensure that they log out when moving away from their desk for any purpose.

3.7 Confidentiality of information

3.7.1 The electronic and paper systems contain information about the business and its operations, its customers, products, supplier information, and its managers and employees.

3.7.2 This information is classified as confidential and sensitive information and may not be accessed unless for work related to the user role, and no other information may be accessed without written explicit and specific management permission.

3.7.3 Users who come into possession of such information may not disclose this to any other person without written explicit and specific management permission.

3.7.4 No user may make any statement to any form of external media – including placing information on the internet – without the written explicit and specific management permission.

4. Access to and disclosure of an individual’s use of TMI-SSP’s electronic communications system

4.1 Management’s right to access, monitor and disclose information

4.1.1 Although TMI-SSP respects the privacy of its employees and other users of its System’s, restriction of this right is unavoidable in the context of the employee’s work-related conduct or the use of TMI-SSP’s provided equipment, supplies or System. The System’s have been installed by TMI-SSP to facilitate business communications and to provide in TMI-SSP’s operational needs.

4.1.2 TMI-SSP is obliged to manage and protect its System’s. Management has been tasked with the responsibility to monitor the Systems and usage to ensure compliance with this policy and may, without further notice to the user/employee, intercept, inspect, monitor or refuse to make a communication available or to pass it on to its intended receiver, all communication in the exercise of its responsibility.

4.1.3 Although each employee has an individual password to access this system, the System belongs to TMI-SSP and the facilities belonging to and controlled by TMI-SSP (telephones, electronic mail, fax machines, modems, computers, network tools and application including Internet access facilities, web browsers), and the content of e-mail communications and Internet usage should be accessible at all times by TMI-SSP’s management for any business purpose. All System passwords and encryption keys must be available to management, and employees may not use passwords that are not known to your supervisor or install encryption programs without turning over encryption keys to your supervisor.

4.1.4 The System may be subject to periodic unannounced inspection, and should be treated like other shared filing systems. TMI-SSP also routinely monitors usage patterns for its e-mail/Internet communications. The reasons for the inspection and monitoring are many, including cost analysis/allocation and the management of TMI-SSP's gateway to the Internet.

4.1.5 All messages created, sent, or retrieved over the System and all other searches, transmissions or downloads are Company records which remain the property of TMI-SSP and should not be considered public information. TMI-SSP reserves the right to access, monitor and disclose without the employee's permission, where necessary, all System usage (including messages and files on TMI-SSP's e-mail/Internet system). Employees should not assume that electronic communications are private or confidential.

4.2 Password and Encryption Key Security and Integrity

Employees (other than management in the circumstances mentioned above) are prohibited from the unauthorised use of the password and encryption keys of other employees to gain access to the other employee's e-mail messages.

5. Violations

Any alleged contraventions of this policy will be investigated by management, and all users are required to report any contravention of the policy which comes to their attention. Appropriate disciplinary action will be taken against any user found to have contravened the system and this may lead to dismissal, or termination of a contractor contract. If necessary, TMI-SSP also reserves the right to advise appropriate legal officials of any illegal violations.

ELECTRONIC COMMUNICATION AND SECURITY POLICY Signature

I, ____, hereby confirm that I have received this memorandum and that I acknowledge the contents thereof.

Signature ________________________________ Date _____________________________