VMS
Fleet Management Ltd

Signed:

Name: Martin James

Position: Managing Director

Date: 15th March 2019

Intranet Usage Policy

Intranet Usage Policy

The Intranet policy states that all information on the intranet is the company's property; all employees who use the intranet are required to follow this policy, all other relevant company policies, adhere to the staff handbook and the VMS privacy policy and all applicable laws. Employees assume all responsibility for their accounts, this includes passwords, violation of privacy and prohibits unauthorised access to other's files.

All information on the intranet is the company's property. The appropriate department must approve initiation of intranet pages and modifications to pages. Generally, the process is initiated through the information technology (IT) department.

All employees who use the intranet are required to follow this policy, all other relevant company policies (e.g. bullying and harassment, discrimination), and all applicable laws (e.g. copyright).

Employees assume all responsibility for their accounts. Passwords or access codes must not be shared with others. Employees may only use data, software programs, e-mail, or computer facilities for which they have authorisation and for an authorised company purpose. Employees may not conceal their identity in any electronic communication.

If an employee suspects that someone may have discovered or guessed their password, they must contact the systems administrator to change it immediately. The intranet must not be used to communicate confidential information. It is not permitted to post confidential information on any intranet page.

The intranet must be used only for company-related business and not for other commercial purposes. For example, employees may not post unauthorised advertisements for products, services, charities, or meetings. Employees may not post "chain letters" and may not use the intranet connection to run a business. Any use of the intranet to facilitate illegal activity, such as gambling, is prohibited and will dealt with as a serious matter in accordance with the company handbook.

At times, employees may use the e-mail account to send an occasional personal e-mail, but such use is to be kept to a minimum. Further, the company will not forward such personal e-mail when you leave.

Employees may only post company-owned information, or information that is legally permissible to copy and distribute, on printed and/or electronic media.

Employees shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users except as authorised. They may not misrepresent other users on the network. Employees may not circumvent login procedures on any computer system.

The disruption or misuse of company communications, hardware, or software; the harassment of intranet users; and the unauthorised access to communications or facilities are prohibited. For example, activities such as "spamming" the network (randomly sending e-mail messages to large numbers of recipients) or sending "e-mail bombs" (overloading addresses with e-mail messages) is strictly prohibited. Similarly, use of the intranet to develop programs that harass, or stalk others is strictly prohibited. Use of the intranet to infiltrate a computer system and/or damage the software components of a computer system is also strictly prohibited.

All intranet information must be written in courteous, respectful, and professional language. Use of discriminatory, insulting, abusive, threatening, offensive, disrespectful, demeaning, or sexually suggestive language is strictly prohibited. Similarly, accessing or storing discriminatory, derogatory, racial, or sexually oriented material is strictly prohibited.

All material(s) placed on the intranet must conform to the company's graphic standards policy. For example, all intranet pages must include the company name at the top of the page and a link to the company's home page.

When the intranet is used for collaborative work, employees must use the company standard word-processing software to edit, read, and circulate the document.

The systems administrator may examine usage, e-mails, Web pages, hard drives, files, and any other facilities in order to diagnose or solve problems or investigate possible violation of company policy. The systems administrator may examine, edit, and/or remove any material that, in the company's judgment, violates company policies. By using the intranet, employees consent to review of their use of the intranet. Employees should not have any expectation of privacy with respect to their use of the intranet. All intranet conferences and bulletin boards may be monitored.

If any investigation of intranet use reveals possible evidence of criminal, illegal, or other prohibited activity, system personnel may provide the results to law enforcement officials.

Employees are expected to report any violations of this policy. Employees who believe they have been harassed or otherwise discriminated against should report such complaints to HR following the grievance procedure within the staff handbook. Reports of violations will be investigated. Employees are expected to cooperate with the investigation. False information provided in the course of an investigation may lead to disciplinary action.

Employees who violate this policy and misuse the intranet are subject to disciplinary action in accordance with staff handbook and disciplinary policy and procedure and possible civil or criminal action.

Approval for this policy

This policy was approved by Martin James, the Managing Director.