Data Security Procedures

This policy outlines the standards which Fox Moving & Storage requires all users of its electronic communications systems and equipment to follow. All Users are responsible for the success of this policy and must ensure that they have read and understood the policy.

The rules below apply regardless of whether data is stored electronically, on paper or on other media.

The Company provides access to staff and other users of its electronic communications systems for the primary purpose of enabling the Company to operate efficiently. The Systems and the data held within the Systems are the property of the Company.

Compliance with the policy will be monitored on a regular basis - any non-compliance will be dealt with in accordance with the disciplinary procedure. In serious cases non-compliance may be treated as gross misconduct leading to summary dismissal.

What is Covered by the Policy
This Policy covers the use of all the electronic communication systems ("the Systems") belonging to the Company including computer equipment, email, internet connection, telephones, mobile devices, fax machines, copiers, scanners, CCTV, electronic key fobs and cards (collectively "the equipment"), USBs, DVDs, CDs.

Who is Covered by the Policy
- all individuals working for the Company at all levels and grades (including those on temporary contracts) ("Employees");
- third parties who have access to the Company's electronic communication systems including but not limited to contractors and sub-contractors.

Email and other forms of direct and/or instant communication
Users should only use email where it is the appropriate means of communication bearing in mind the content and recipient of the email.

Users should draft and consider email communication as identical to a letter or fax and address and copy correspondence only to relevant individuals.

Internet Use
Users should not use the Systems to access any web page or download any files (whether documents, images or other format) which:
- are defamatory, threatening or intimidatory or which could be classed as harassment;
- contain obscene, profane or abusive language;
- contain pornographic material (i.e. writings, pictures, films video clips of a sexually explicit or graphic nature);
- contain offensive or derogatory images, regarding sex, race, religion, colour, origin, age, physical or mental disability, medical condition or sexual orientation;
- infringe third party's rights (including intellectual property rights) or are otherwise unlawful or inappropriate;
- involve any form of online gambling.

Users should not:

- upload to any website (whether a personal email account or otherwise) any documents, text, information, images or pictures which belong to the Company unless specifically authorised to do so;
- use the Systems to post messages in an internet chat room, on any internet message board or to set up or log text or information on a blog unless specifically authorised to do so;
- install unauthorised software or hardware, including modems and wireless access unless they have explicit management approval.

Users are reminded that music, video, text and other content on the internet are copyright works and should not download or email such content to others unless certain that the owner of such works has authorised this.

Personal Use of Systems

The Company permits the incidental personal use of the Systems provided that;

- use must be minimal and take place substantially out of normal working hours (i.e. during a worker's usual lunch hour, before or after standard work hours);
- it does not interfere in any way with the User carrying out his or her duties on behalf of the Company;
- it does not commit the Company to any marginal costs;
- it complies with the Company's policies including this policy.

Equipment Security

Users are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this Policy.

All suspicious emails should be reported to the IT Department as soon as reasonably practicable and no action taken whatsoever (including the deletion of the same) unless specifically authorised by the IT Department.

The Company reserves the right to block access to attachments to emails for the purpose of effective use of the Systems and for compliance with this Policy.

Users should be aware at all times that the System contains information which is confidential to the Company's functions, operations and/or which is subject to data protection legislation. Such information must be treated with extreme care.

Working from Home

No customer files or other information may be taken off site without the approval of senior management.

When working from home, employees must be aware of the increased risk of a security breach and must ensure that all documentation is stored securely and that any laptop or PC is password protected and turned off when not in use.

Data Security Procedures

IT equipment provided to the employee to support working from home is for the exclusive use of that employee alone. The employee is not permitted to allow family members or friends to use IT equipment provided to them.

While working from home employees will remain subject to all confidentiality clauses contained within their contract of employment.

Use of Laptops

- company provided laptops must only be used in connection with the business activities they are assigned and / or authorised; access to company laptops is forbidden for non-authorised personnel;
- every user is responsible for the preservation and correct use of the laptops they have been assigned;
- special care must be taken for protecting laptops, tablets and other portable assets from being stolen; active laptops and tablets must be secured if left unattended;
- users shall maintain the assets assigned to them clean and free of accidents or improper use. They shall not drink or eat near the equipment;
- when travelling by plane, portable equipment like laptops and tablets must remain in possession of the user as hand luggage;
- losses, theft, damages, tampering or other incident related to assets that compromises security must be reported as soon as possible to the IT Department;
- any asset requiring disposal must be returned to the IT Department.

Passwords

The IT Manager will maintain a list of administrative access codes. Employees set up their own passwords. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained.

User passwords will expire every 90 days. Users will receive a notification 14 days prior to this date reminding them to change it.

Clear Desk Policy

- employees are required to ensure that all sensitive / confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period;
- computer workstations / laptops must be locked when workspace is unoccupied; workstations must be shut completely down at the end of the work day;
- any restricted or sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
- filing cabinets containing restricted or sensitive information must be kept closed and secure;
- upon disposal, restricted and / or sensitive documents should be shredded in the official shredder bins;
- all printers should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up;
- documents, once scanned, should be disposed of by shredding if no longer required.

Data Security Procedures

Credit / Debit Card Policy
Customer's credit / debit card details must not be stored on our Systems or in any other records. All credit card transactions will be processed on our own system. If information is provided to us in writing, the document will be securely destroyed immediately after we have used the details for collecting payment.

Card details given over the 'phone must be processed as soon as received and notes taken must be destroyed immediately.

Visitors
All visitors must report to reception on entering and leaving the building and must always be escorted for duration of visit, especially to sensitive/non-public areas.

Mobile 'Phones
Where a mobile 'phone has been issued by the company, it is for business use only and at all times will remain the property of the Company. The User(s) will be responsible for its safekeeping, proper use, condition and eventual return to the Company and will also be responsible for any cost of repair or replacement other than fair wear and tear. If a replacement is required, the Company will organise this.

Employees accessing emails using their personal mobile 'phones should have the appropriate secure systems in place to ensure that should their phone be lost or stolen the data cannot be accessed. The IT Department must be informed immediately.

Data Breach
Any personal data breach must be report to the IT Manager, as soon as possible after the breach being identified. This can be done via email, 'phone, text or verbally.

Monitoring & Compliance
The Company reserves the right to monitor telephone, email, voicemail, web and other communications traffic and to retrieve the contents of email or telephone messages or check searches which have been made on the internet for the following purposes (this list is non-exhaustive).

- to monitor whether the use of the Systems is legitimate and in accordance with this policy or other policies of the Company;
- to retrieve messages lost due to computer failure or any other reason;
- to assist in the investigation of any acts which may be in breach of this policy or other policies of the Company;
- to comply with any legal obligation; or monitoring emails and telephone messages during your absences from the Company.

Monitoring is carried out to ensure compliance with these policies and any other policies of the Company and will only be carried out to the extent and as permitted or required by law. Users should be aware that any personal use of the Systems may also be monitored and where evidence of misuse is found, as a result of such monitoring or otherwise, the Company may undertake a more detailed investigation. In accordance with our disciplinary procedure, this may involve the examination and disclosure of monitoring records to those nominated to

undertake the investigation and any witnesses or managers involved in the disciplinary procedure. If necessary such information may be handed to the police in connection with a criminal investigation.

Misuse or abuse of the Systems in breach of this Policy will be dealt with in accordance with our disciplinary procedure. Serious breaches will amount to gross misconduct which can lead to summary dismissal. Misuse can, in certain circumstances, constitute a criminal offence.

Abuse of the personal use Policy may result in withdrawal of the privilege.

Telephone numbers and internet sites may be blocked at the discretion of the Company.

Enforcement
The Company's IT Manager has overall responsibility for this policy including:

- day-to-day responsibility for overseeing and implementing action;
- responsibility for monitoring and reviewing the operation of the Policy and any recommendations for charges;

Managers have a specific responsibility to ensure workers understand this policy and adhere to it at all times.

I confirm that I have read and understood the terms of these procedures and that it forms part of the terms and conditions of my employment. I specially understand that Information security incidents must be reported immediately to the IT Manager or other senior manager in his / her absence.

Name : _____

Position : _____

Signature : _____

Date : _____