Training & Advisory Services Ltd.	**PERSONNEL POLICY**
Reference: HR007 Version: 1.0	Number of Pages 6
TITLE: **DATA & INFORMATION SECURITY**	
Authorised by: **Russell Prince** Chief Executive	Effective Date: 01/03/2016 Supersedes: 14/05/2012

Contents

Introduction / Purpose

It is important to the company to ensure that our data is secure against loss and/or damage. This Policy states the company's position with regard to information security and ensures that we:

(a) Prevent loss or corruption of data due to computer 'viruses'.

(b) Maintain security over confidential or sensitive company data, to ensure that access is only available within the company to authorised employees.

(c) Avoid the introduction of unauthorised programs and files to the network which can have a detrimental effect on resources, or the introduction of material which is inappropriate in the workplace.

Full compliance with this policy is mandatory and of the utmost importance. Failure to comply with this Policy could result in disciplinary action, which may ultimately lead to termination of employment.

General

(1) Never leave sensitive documents lying around unattended. At the end of the working day clear your desk of any confidential material. Whenever possible lock desks and filing cabinets.

(2) Do not supply outsiders with company documentation, except when authorised to do so by your Manager.

(3) If sending confidential information by fax make sure that no unauthorised person at either end can gain access to the document. In such cases, notify the recipient in advance by telephone.

(4) Always ensure that important or key computer files are held on the file server as these are automatically backed up each evening. Company files should not be held on the hard disks (C:\ drive) of individual PCs.

Computer Software - Acquisition & Installation

(1) All software must be acquired and installed under the control of the IT Consultant. The company will carry out checks and monitoring of systems from time to time to identify if any unauthorised or illegal software is being used. These checks will be occasional and random. In carrying out these checks the company recognises the need to respect the privacy of its employees.

(2) Copies of program software must never be taken.

(3) Never install illegal copies, in particular of pirate software.

(4) Do not transfer software programs from a private PC to a company PC.

(5) If computer files do need to be introduced to our network for business purposes, either from floppy disks or from compact disks (CDs) then contact the Computer Department to arrange the most suitable method of transfer.

(6) Demonstration programs are a major source of computer viruses. Think carefully before you decide to use these, and always ensure that they are first checked for viruses by the Computer Department, and installed in a temporary demonstration area on the server.

(7) Viruses are frequently transmitted via computer games or screen savers, and these are not permitted. **It will be considered a disciplinary matter to install computer games or screen savers (not supplied with the PC) on company computers.**

(8) Programs should not be downloaded from the Internet or e-mailed to company PCs.

Controls Regarding Access to Data

To control access to data, all users are issued with an individual user identification (I.D.) which must be accompanied by a password, specific to the user, and entered before any access to the system is allowed.

Passwords which are totally under the control of the user are therefore a very important control and should be managed as follows:-

(1) Choose words which cannot easily be guessed and which should not have any readily identifiable connection with their owner, nor be written down and left in an easily accessible place.

(2) They should be at least six characters in length and can comprise alphabetic characters and numbers.

(3) Keep a personal and private record of chosen words to ensure that no-one else can gain access to information which is specific to, and the responsibility of, individual users.

(4) Do not disclose your password to others and when using it on the system make sure that you are not overlooked by anyone who might be interested in learning it.

(5) Users will be required to change passwords after specific periods, normally once every 3 months. Passwords already used should be avoided as these may already be known by unauthorised users or ex-employees.

(6) Always activate the screen saver with password security to ensure that if you are away from your PC nobody can access or modify your data.

Protective Measures Against Computer Viruses

Viruses introduced through any individual PC or workstation put our entire company information system at risk.

We have installed appropriate anti-virus software, which is updated automatically on a regular basis via the file servers to individual PCs. Even so, new viruses are being created daily and we cannot rely totally on the installed software. Therefore:-

(1) If our anti-virus software does detect a problem do not take any action to eliminate such software infections on your own. Discuss any measures to be taken with the Computer Consulant, and do not deploy any other anti-virus programs if not under their control and supervision.

(2) If you detect unknown programs within your area of responsibility avoid running them until you are sure of their origin.

(3) Discontinue use of a system if any suspicion of virus arises, i.e.:-

(a) If you detect unauthorised attempts to gain write access to your programs;

(b) If files grow in length with no explanation;

(c) If the system becomes extremely slow for no apparent reason;

(d) If programs run more slowly than usual, or if errors start occurring in previously trouble-free programs;

(e) If file attributes change without any corresponding processing having taken place;

(f) Problems or inconsistencies with screen displays.

Internet Policy

The company Policy on the Internet is as follows:

(1) Employees/Guests/Learners are allowed to use the Internet for limited private use, but this must not be carried out during working hours and downloading of material for private use is not permitted.

(2) Software must not be downloaded or distributed to others

(3) Sites offering sexually oriented material, or racist or other offensive material, gambling or on-line games should not be accessed.

(4) It is forbidden to use the internet for carrying out business on a private or freelance basis.

(5) Employees must not allow anyone else to use the Internet installed on their PC unless authorised by their manager to do so.

(6) Employees should not divulge power on passwords, screen saver passwords, or network passwords to anyone without their manager's permission.

(7) Employees/Guests/Learners should be aware that all Web sites accessed from their PC or devices are logged, and they can be questioned about this at any time.

(8) Misuse of the Internet could lead to disciplinary action: in serious cases this could mean dismissal.

(9) Internet sites that are cost related or have cost implication terms of access must not be subscribed to without prior authority.

(10) The Company retains the copyright to any material posted to the World Wide Web by any employee in the course of his or her duties. It is inappropriate to reveal confidential information. Any employee releasing protected information via e-mail or the internet (whether or not inadvertent) will be subject to disciplinary investigations under the normal disciplinary procedure.

1 Guidelines on the use of E-mail

Although e-mail is a useful and efficient medium for internal and external communication, misuse of the system can have serious repercussions.

Employees may use e-mail for some limited private use but this must be kept to a minimum. Excessive personal use during working hours and transmission of large files (such as those containing photographs) is not permitted. Employees have no expectation of privacy and should avoid communicating any personally sensitive information in this way. It is the responsibility of each employee to ensure that this

technology is used for proper business purposes and in a manner that does not compromise the Company or any of its employees.

The company's e-mail system should not be used for sending e-mails of a sexually explicit nature, or discriminatory material. Do not send messages or attach files whose content is of an obscene, pornographic, lewd or distasteful nature. Sending or the possible storage of such material may be an offence under section 43 of the Obscene Publications Act 1984. A single act infringing this regulation may lead to summary dismissal and prosecution.

If an employee sends an e-mail in work which constitutes harassment, the employer can be held vicariously liable for this. In addition, under current legislation, harassment is a criminal offence as well as a civil wrong and could result in legal proceedings. You should be aware that e-mails which some may consider humorous could offend others and be held to be material causing harassment, as could unwanted communications or explicit language.

Staff are warned not to indulge in certain activities via the Company's e-mail facilities such as:

(1) Posting information that insults or harasses others on the basis of their sex, marital status, race, colour, nationality, age, disability or religion.

(2) Downloading or distributing copyright information.

(3) Posting confidential information about their employer, its customers or suppliers.

(4) Engaging in on-line gambling.

(5) Do not send or forward any e-mails or attachments which are defamatory (those which attack the reputation or good name of a company or individual).

(6) All negotiation and commitments made via e-mail should be carefully checked and authorised. Care must be taken to ensure that contractual arrangements are not made without express intention to do so.

In considering the dangers of misuse please remember that:

(1) E-mails can be read by third parties.

(2) E-mails can be used in evidence.

(3) E-mails can create binding contracts.

(4) All statements made should be factually correct and non-defamatory of others.

(5) **E-mail and Internet misuse can amount to gross misconduct and lead to summary dismissal.**

2 General Points:

The Company reserves the right to intercept any e-mail for monitoring purposes, preventing or detecting crime, investigating or detecting the unauthorised use of the Company's telecommunications system or ascertaining compliance with the Company's practice or procedures.

The company reserves the right to take disciplinary action regarding any material considered inappropriate in the workplace.

The company reserves the right to check an employee's computer in the case of absence from work.

It is vitally important that the guidelines above are followed to avoid any misuse.

These guidelines also apply to faxes, letters and any other written material.

If during the performance of their work any employee encounters obscene or inappropriate material, unauthorised software or the misuse of company information systems this should be reported directly to the Human Resources department.