# TECH-TRENDS LTD INFORMATION COMMUNICATIONS TECHNOLOGY SECURITY POLICY

## Purpose

This policy is designed to emphasise the importance that Tech-Trends Ltd places upon security of its property, confidential information and electronic systems including any computer and any accessory or peripheral device connected to or networked with any such computer, in this policy referred to as the company's "property".

The company's property should be used for the business interests of the company and must not be used in any way contrary to those interests. The company will take active steps to protect its property, including taking legal action. Any copying, distribution or abuse of any company property other than for the company's legitimate business purposes is strictly prohibited.

This policy is also designed to protect the company's electronic security systems and therefore to ensure the security of its computer equipment and software and physical property including its premises. It covers all aspects of the company's security or electronic equipment that it is designed to protect including but not limited to entry codes, electronic codes in security fobs, electronic keys and alarm systems as well as the company's computer equipment and networks.

The company will afford access to its confidential information to enable employees to carry out their duties, but such confidential information is valuable and loss or misuse of it could cause substantial damage to the company.

This policy is non-contractual in effect and does not form part of normal terms and conditions of employment. The company reserves the right to change the terms of this policy from time to time and to introduce a replacement procedure as may be required.

## Definition and scope

This policy applies to all employees, agency workers, independent contractors or any other worker afforded access to Tech-Trends Ltd property, referred to in this policy as "employees".

This policy should be read in conjunction with the Tech-Trends Ltd suit of policy documents.

For the purposes of this policy computer equipment shall mean any hardware and/or software that uses or comprises electronic or computer code or circuitry, including but not limited to telephones, televisions, CCTV systems, DVD's, video recorders or sound recording equipment where such equipment is capable of being connected to a computer by digital or other interface.

Tech-Trends Ltd will take steps to use password protection and/or other security means including monitoring to protect its property. Employees are given access to the company's information and property, including its computer equipment, for the purpose of carrying out their duties for the company and for that purpose only. Any loss sustained by the company as a result of a breach of this protocol, whether intentional or unintentional, will give rise to disciplinary action and all employees are asked to take great care with electronic security systems and to report immediately the loss and/or failure of any electronic or other security measure or equipment to their line manager or other appropriate person immediately.

The policy sets out rules in relation to the use of the company's property.

# Principles

Employees must not, under any circumstances:

- Use any device (including any flash drive, memory or mirroring device) in combination with the company's property unless specific authorisation has been given for that particular purpose;
- Use any computer, photocopier, scanner or any other copying device for the purpose of copying information onto any medium other than in the company's business interests;
- Download or upload any computer software, data, code or information belonging to the company;
- Introduce any recording medium such as a CD, DVD or flash drive to the company's computers unless it has been checked and approved by a person in authority within the company;
- Use the company's property or any property in any way that will increase the likelihood of damage arising from the introduction of unscreened software or hardware that may expose that property to viruses, spyware or adware of any kind;
- use the company's property to:
    - harass;
    - discriminate;
    - bully;
    - defame;
    - or otherwise act offensively;

  Toward any person whether or not an employee of the company, directly or indirectly and inside or outside working hours.

Any breach of this policy or unlawful act carried out using the company's computer equipment will give rise to an investigation that will be likely to give rise to disciplinary proceedings and may, in serious cases, result in dismissal and/or entail disclosure of any facts or information to the police or other enforcing authority.

Tech-Trends Ltd also reserves the right to take legal action in the civil courts to recover losses sustained or about to be sustained as a result of any breach of this policy including any potential breach.

# Passwords and electronic systems security

Under no circumstances without specific authorisation should any employee:

- Share any password or other electronic security information with any other person other than an authorised employee or director of the company;
- Copy or upload any of the company's security information, software, confidential information or personal data;
- Use any of their own or any third party's software and/or hardware including but not limited to any flash drive, memory stick, external hard drive or

recording media in combination with the company's computer equipment or systems;

- Use any other employee's security information, passwords, electronic identity including username or any means by which any such employee accesses the company's equipment, property and/or information;
- Abuse any electronic time recording and/or entry or exit systems or any information for the purpose of creating a false record or otherwise;
- Give or allow to be given or lent to or otherwise shared with any third party any of the company's computer or electronic equipment, including any passes, electronic keys or fobs;
- Upload and/or e-mail or otherwise transmit any data belonging to the company other than in relation to normal working practices;
- Download and/or access any unauthorised information and/or website including video-streaming and/or downloading music or other copyright data;
- Copy upload or e-mail any software licensed to the company to any unlicensed user in breach of the terms of the company's licences which, it should be presumed, are for use on the company's computer equipment only;
- Copy upload or e-mail any of the company's confidential business information stored electronically for any purpose other than for business purposes and then only strictly in accordance with the terms of this policy and any other of the company's policies including but not limited to the data protection policy;
- Enter or attempt to enter any restricted part of the company's computer equipment which they do not have authority to enter by any means whatever including the use of another's security clearance and/or passwords or otherwise compromise the integrity of the company's computer equipment.

Any deliberate destruction of any computer equipment other than in the course of the proper disposal of the same with full and proper authority will, if proven upon investigation, be treated as an act of gross misconduct.

Signed: 

Name: Paul Palmer

Position: Director

Date: 15 August 2011