

# Company Equipment

## Risks

- Damage / Deterioration or Loss due to carelessness or negligence of a user.
- Unauthorized use of computers.
- Unauthorized access to Company Information.
- Installation of unlicensed Software.
- Installation of virus infected software which can damage data files, programs of the company.

## General Policies

Employees and 3<sup>rd</sup> parties within the scope of this policy are accountable for the protection and proper use and handling of all physical company assets to which they have access. They must:

- Exercise due diligence in the use of the computer. As in any other equipment, computers require regular maintenance. The user shall allow authorized IT personnel to inspect and maintain the computers, from time to time.
- Use physical assets only for legitimate company business purposes.
- Protect company assets from use or access by unauthorized people.
- Secure company assets from accidental or intentional loss, theft or damage
- Report immediately to management any suspicious activity, unauthorized persons, theft, and emergencies.

Information Asset: it is the responsibility of every employee to protect the information assets of by exercising appropriate care in the use of the company's information assets so that confidentiality, integrity and availability of these assets are maintained. In the course of your employment you will become aware of business information relating to the business or affairs of the company including but not limited to new product details, trade secrets, client and customer information, marketing strategies and financial arrangements between the Company and its staff and clients. In accepting employment you are required to treat this confidential information as the sole property of the Company and you accept that the information is confidential to the company and to users of the Confidential Information authorized by the Company. Accordingly, you will not directly or indirectly divulge to any person or use the Confidential Information for your own or another's benefit. Where the company considers data highly sensitive, encryption software may be used. IT may be contacted for advice on security or encryption software.

## **Other Policies**

### **Issuance and Withdrawal of Computer**

The company reserves the right to withdraw the issue of a computer at any time and for any reason. In particular, where a staff member is deemed to frequently breach guidelines, a computer will be recalled from that staff member.

For laptop users, if you have been advised by the IT or your supervisor that you need to return your computer, the computer needs to be fully powered down, do not leave it in suspend mode or hibernation. You will be advised if you need to return your computer accessories as well.

### **Authorized Use**

Computers are issued to employees of Tilson and are only to be used by the employee that the computer has been assigned to. Computers are not for the use of friends or family members.

### **Proper use of computers**

Computers are delicate electronic equipment requiring due care. Whenever possible do not leave in high or low temperatures, strong sunlight, or where the computer may be subject to harsh vibration or the risk of impact through falls, etc. Computers are to be maintained in a clean and workable state at all times.

- Keep physical hazards (liquids, dust, etc) away from your computer.
- Be aware of software “viruses”. Accept software from reliable sources only. do not download software from the internet. Make use of “anti-virus” software on your computer.
- Be sure that your PC has a Power-On Password and screen saver password (at least 15 minutes idle)
- Always use good password practices such as combination of alphabet and numbers.
- Regularly back up your critical data for data disaster recovery.

### **Reporting Stolen, Lost or Damaged Computers and Associated Equipment**

Any person issued with a company computer is obliged to report the incident as soon as they become aware that their computer has been lost, stolen, misplaced or damaged.

Report the matter to the following people:

- Police (if stolen)
- Your immediate supervisor
- Director of Department

If your computer has been stolen you will be required to contact the CFO or IT for information about your computer (i.e. Serial number, make and model). You will need to report the following to the CFO or President:

- Copy of the Police Report of Case Number
- What items have been stolen (i.e. Laptop, computer bag, power cord, etc.)
- Description of the event (i.e. time and location)

### **Loss of a Company Owned Computer from a Vehicle**

Where a company computer has been lost or stolen from a motor vehicle, (whether the vehicle is company owned), a replacement computer will not automatically be re-issued.

Approval to replace a computer lost or stolen from a motor vehicle must be gained from the appropriate supervisor. Replacement conditions stated in the following section, Damage or Loss due to Carelessness also apply.

Leaving a company owned computer and computer accessories (power cord and computer car charger) in view in an unattended vehicle, for any period, in any location, is strictly forbidden.

If your computer is not with you during a sales call or with you while driving, it must then be placed in your computer bag and stored in the trunk of your vehicle and no where else inside of your vehicle. If your computer is stolen from inside your vehicle (not from the trunk) then you will be required to refund the company the insurance excess or replacement cost of the computer, whichever is the lesser amount.

### **Damage or Loss Due to Carelessness**

Where a computer has been lost, stolen or damaged due to carelessness and only if this is the first incident of loss or damage to a company computer for that staff member, the computer may be replaced / repaired at the company expense with charges allocated to the appropriate individual's budget once approved by the Senior Director of Information Technology.

Any further loss or damage to a company issued computer or any associated equipment, will require the staff member concerned to refund to the company either the cost of the repairs require, payment of the insurance excess or replacement cost of the computer, whichever is the lesser amount.

### **Damage or Loss Due to Negligence**

Where a company computer and/or associated equipment has been lost, stolen or damaged due to negligence, the staff member concerned will be required to refund to the company either the cost of the repairs required, payment of the insurance excess or replacement cost of the computer, whichever is the lesser amount.

A replacement computer will not automatically be re-issued in cases of negligence. Replacement approval must be gained from the Senior Director of Information Technology.