COMPANY LAPTOP POLICY

This policy outlines [Organization Name]’s policy on company laptops and is intended to reduce the risks of data security and laptop damage. Although laptop computers are an important and practical business tool, their portability makes them particularly vulnerable to physical damage or theft. The cost of replacing the hardware and software, as well as the value of the organizational data stored on or accessible through them, is also included in the cost of a data breach.

POLICY

Employees are further reminded that, in addition to the limits and restrictions of laptop usage outlined in this Policy, they must follow any provisions of their individual employment agreements that dictate or restrict any activity in this regard.

Intended Use of Laptops

Company laptops will remain the property of [Organization Name] at all times, and the employee will have no right or interest in it other than to use it during their employment or for such a period as the Company may determine.

Employees must guarantee that the laptop is only used for business purposes and in the proper fulfilment of their responsibilities, not for the purpose of generating, transmitting, or corresponding any content that is in violation of any [Organization Name] policy. Employees who violate this policy will face disciplinary action in accordance with company policy.

[Organization Name] reserves the right to undertake inspections of any computer equipment it owns or administers, including all laptops. Employees may be requested to submit the laptop to the company for an audit.

Procedures for Laptop Physical Security

Each employee who receives a laptop from [Organization Name] is responsible for the device's physical security. All computers purchased on behalf of or for [Organization Name] are considered company property.

To guarantee the physical security of [Organization Name] computers, all employees must take the following steps:

* When not in use, place the laptop in a secure place.
* Do not leave your laptop unattended in your vehicle. If you must leave your laptop in your vehicle for a short amount of time, it must be locked in the trunk.
* If you're using your laptop in a public place, don't leave it unattended.
* Employees are not permitted to take the laptop to any external agency or vendor for repair at any time.
* Employees are expected to notify management in the event of any failure with the laptop software.

During travel:

* Do not place your laptop inside a checked luggage.
* To quickly identify your laptop during security checks or if it is misplaced, attach a name tag or business card to it.
* When you're not in the room, put the laptop in the hotel safe or a closed piece of luggage.

Controls for Data Security

Employees are responsible for ensuring the data on their computers is secure. You must follow the following guidelines in this regard:

* Keep your password private because you are personally responsible for all network and system access under your user ID. Never reveal it to anybody, including family members, friends, or IT personnel.
* Authorized personnel are given corporate laptops for official use. Do not lend or allow others to use your laptop, such as relatives and friends.
* Avoid leaving your laptop logged on and unattended. Before leaving the computer, always turn it off, log out, or use a password-protected screensaver.

Virus Protection

Computer viruses are currently spread primarily through email attachments.

* If you didn't expect to receive an email attachment from that individual, don't open it.
* Any files downloaded to your computer from any source (CD/DVD, USB hard disks and memory sticks, network files, email attachments, or files from the Internet) should always be virus-scanned. If your virus definitions are up to date, virus scans should happen automatically, but if you want to be sure, you can run a manual scan.
* To limit the harm, report any security issues (such as virus infections) as soon as possible to your manager.
* Contact your manager immediately if you receive a virus warning notice on your computer, or if you suspect a virus (e.g., strange file activity). If you fear your computer is infected, don't send any files or data over the network.

Unauthorized Software/Content Use

* Employees must guarantee that they do not download, install, or use any illegal software.
* Software packages that allow the computer to be ‘remotely controlled' (e.g. PCAnywhere) and 'hacking tools' (e.g. network sniffers and password crackers) are explicitly prohibited on Company equipment unless they have been explicitly pre-authorized by the management for the advancement of the [Organization Name]’s legitimate business purposes.
* All software or other programs downloaded onto the [Organization Name] provided laptop, whether or not in accordance with the [Organization Name]'s business needs shall immediately become the sole and exclusive property of the [Organization Name], and can only be used in accordance with the [Organization Name]'s directions in this regard.
* Any programs or software that were pre-installed on the laptop when it was turned over to the [Organization Name] cannot be changed or removed in any way, whether permanently or temporarily, except in compliance with the [Organization Name]'s instructions.
* Unsuitable content such as pornographic, racist, defamatory, or harassing files, images, videos, or email messages that may cause offence or embarrassment to the Company, its employees, or any third party will not be tolerated.

**Policy Violations**

Violations of this policy may result in disciplinary action, which could include dismissal. If an employee's laptop is stolen or damaged as a result of negligence, the employee is accountable for the expense of repair or replacement.