IT POLICY DOCUMENT

IT Department
it@walplast.com

Contents

Laptop Policy 2
1.0 Purpose 2
2.0 Scope 2
3.0 Procedures 2
4.0 Laptop Damages: 4
5.0 Returning the Laptop 4
Password Policy: 5
Internet Usage Policy 6
Policy Statement 6
Purpose for Policy 6
Unacceptable Behaviour 6
Monitoring 7
Sanctions 7
Agreement 7
Contact Details: 7

Laptop Policy

1.0 Purpose

Laptop computers provide important functionality, allowing employees to have their computing resource at hand in meetings/workplace, and those who travel on business to be maximally functional and productive while away.

2.0 Scope

These procedures apply to all employees who use Company owned laptop/desktops. These individuals are hereinafter referred to as "owners." Each owner of a Company-owned laptop/desktop is responsible for the security of that machine, regardless of whether the laptop is used in the office, at one's place of residence, or in any other location such as a hotel, conference room or while travelling.

3.0 Procedures

3.1 Requesting a new Laptop

Every department need to submit a formal request to IT department for requesting a laptop along with the approval from department HOD. IT department on receiving the request will issue a laptop within 5 working days. The laptop issues will be solely decided by IT department as per specifications agreed and suggested by IT Team at a company level.

Any special request for a specific laptop/desktop configuration need to be submitted to IT team. On proper evaluation of the request, IT will issue a higher grade/version laptop once request is approved by department HOD and management.

3.2 Using a Laptop

Every owner of the Laptop must use the Laptop only for official purposes in the course of their rightful discharge of their duties and not be used for generating, transmitting, corresponding anything that is unlawful or abusive. This may lead to the owner being subject to disciplinary action and may lead to suspension from work or any other appropriate action as per the Company policy and governing Laws will be taken.

3.3 Laptops in Office

Laptops must be secured in a locked drawer when not in use, i.e. when you are not taking your laptop home or will be out of the office for a while. When in office lock the Laptop working screen so that no other person can use it for any purpose.

3.4 Laptops Out of Office

When an owner takes the laptop out of his/her office, he/she is expected to keep the laptop in hand or sight, or in a secure location; at all times. It is the total responsibility of the owner to handle the Laptop.

During the period when the owner carries the Laptop with them, the same should not be misused for the purpose of transferring the data on to other storage devices. If any owner were found malpractice, he/she would be liable for disciplinary action from the organization.

No external devices to be used to copy data from the Laptop to transmit / transfer to other agencies while on work at their site unless it is absolute necessary Ex. use of DVDs, Pen Drives, Network Drives at other location and CDs.

3.5 Reporting a Theft

If a Company-owned laptop is stolen, its owner is expected to immediately file a theft report with all details as to the time, date, location and any other details that you feel is important with HR/Admin Department. If traveling, the owner must also report the theft to the local law enforcement agency. In case of negligence the management has every right to deduct the equivalent amount from the owners Salary or FNF.

3.6 Keeping the Laptop Secure

The owner of a company-owned laptop must have it checked by the System Administrator every three months (quarterly) so that the latest patches, security holes, upgrade and other software remain current.

3.7 Installation of unauthorized Software/Accessories

The owner shall not install any unauthorized/pirated accessories/software like messengers, chatting software or designing software or any malicious software, which may cause problems to the functioning of the Laptop.

3.8 Ending Employment at the Company

An owner must return the laptop to the Company before their last working date of employment in company to IT Dept. The laptop, laptop bag, mouse, and/or any other asset will be collected from the employee. Failure to turn in the laptop or any other IT Asset may result in withholding payments such as Full &Final settlement until the laptop is returned.

4.0 Laptop Damages:

If there is any kind of damage, the owner will be liable to pay the damage cost to the Company, this will be deducted from his monthly salary or Full and Final Payment.

Any owner violating this would be penalized as per the company policy

5.0 Returning the Laptop

Owner shall return the Laptop to the company in the following situations:

a) Leaving the company
b) Requested to return the Laptop without assigning any reason by the Management.

Failure to turn in the laptop or any other IT Asset may result in withholding payments such as Full &Final settlement until the laptop is returned.

Password Policy:

Individuals are responsible for keeping their passwords secure and confidential. As such, the following principles must be adhered to for creating and safeguarding passwords:

Passwords especially susceptible to brute force attacks

1. Password must be changed immediately upon issuance for the first-use. Initial passwords must be securely transmitted to the individual.
2. It's wise to use, discourage or prohibit the following passwords:
   - Easy-to-guess passwords, especially the phrase "password"
   - A string of numbers or letters like "1234" or "abcd"
   - A string of characters appearing sequentially on the keyboard, like "@#$%^&"
   - A user's given name, the name of a spouse or partner, or other names
   - The user's phone number or license plate number, anybody's birth date, or other information easily obtained about a user (e.g., address or alma mater)
   - The same character typed multiple times like "zzzzzz"
   - Default or suggested passwords, even if they seem strong
   - Usernames or host names used as passwords

3. Passwords must never be written down and left in a location easily accessible or visible to others. This includes both paper and digital formats on untagged (unsupported) devices.
4. Individuals must never leave themselves logged into an application or system where someone else can unknowingly use their account

Strong Pass

A strong password describes a password that is difficult to detect by both humans and computer programs, effectively protecting data from unauthorized access.

A strong password consists of :

1. At least six characters (and the more characters, the stronger the password)
2. A combination of letters, numbers and symbols (@, #, $, %, etc.)
3. Passwords are typically case-sensitive, so a strong password can contains letters in both uppercase and lowercase.
4. Strong passwords also should not contain words that can be found in a dictionary or parts of the user's own name.

Internet Usage Policy

Policy Statement

Use of the internet by employees in company is permitted and encouraged where such use supports the goals and objectives of the business. This document constitutes a wide spread policy for the appropriate use of internet and resources.

Purpose for Policy

The policy outlines the use of the internet whereby employees must ensure that they:

- ✓ use the internet in an acceptable way
- ✓ do not create unnecessary business risk to the company by their misuse of the internet

Unacceptable Behaviour

Individuals are responsible for keeping passwords secure and confidential. As such, the following principles must be adhered to for creating and safeguarding passwords:
In particular the following is deemed unacceptable use or behaviour by employees:

1. Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
2. Using the computer to perpetrate any form of fraud, or software, film or music piracy
3. Using the internet to send offensive or harassing material to other users.
4. Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
5. Hacking into unauthorised areas
6. Publishing defamatory and/or knowingly false material about company, your colleagues and/or our customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format – without authorized permissions to do so
7. Revealing confidential information about company in a personal online posting, upload or transmission - including financial information and information relating to our customers, business plans, policies, staff and/or internal discussions
8. Undertaking deliberate activities that waste staff effort or networked resources

Monitoring

Company accepts that the use of the internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business.

In addition, all of the company's internet-related resources are provided for business purposes. Therefore, the company maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Sanctions

Where it is believed that an employee has failed to comply with this policy, they will face the company's disciplinary procedure. If the employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record.

Agreement

All company employees, contractors or temporary staff who have been granted the right to use the company's internet access are, by default, assumed to have the understanding and acceptance of this policy. There will be no separate signing required.

Contact Details:

In the event a breach or compromise, the incident must be reported to IT Team immediately by an email to it@walplast.com