

Network Assets Security Policy

Document Classification:	Protected
Document Ref.	ISMS-NW-001-02-Asset Security Policy-V2-Draft
Version:	2
Dated:	09/02/2023
Document Author:	Network Administrator
Document Owner:	Network Administrator

Revision History

Version	Date	Revision Author	Summary of Changes
1	13/07/2020	Network Administrator	Prepared the first version document
1.1	11/08/2022	Network Administrator	1. Asset upgrade details table added 2. Also getting signature when employee relieving from organisation
2	09/02/2023	Network Engineer	Consolidated the below mentioned two policies into one: 1. ISMS-NW-001-02-Asset Security Policy-V1.1-Final 2. ISMS-NW-001-29-Network Asset Safety Policy-V1-Final

Approved By

Name	Position	Date
Manivel Rajendran	Chief Technology Officer	29/08/2022
Kamalavel Rajendran	Chief Executive Officer	09/02/2023

Table of Contents

Sl. No.	Title	Page Number
1	Purpose	3
2	Procedures for Assets Physical Security	3
2.1	During Travel	3
3	Guidelines	3
4	Policy Violation	4
4.1	Natural Issue	4
4.2	Issue because of Negligence	5
4.3	Unidentified	5
5	Details and Declaration	5

List of Tables

Sl. No.	Title	Page Number
1	Table 1 - Asset Upgrade Details	6

1. Purpose

This policy addresses the actions to be taken by all Employees/Interns of Mallow Technologies Pvt. Ltd., who have any company issued assets like Laptop/iMac/Mobile Devices/Accessories etc.,

2. Procedures for Assets Physical Security

Each employee is responsible for the assets provided to them by Mallow Technologies Private Limited. All assets are acquired on behalf of Mallow Technologies Private Limited. The company is the sole owner of all assets.

All Employees/Interns must take the following actions to ensure the physical security of the company assets.

- When not in use, all electronic assets must be locked with a password. The user should be cautious while entering the password in a public space to avoid shoulder surfing (the practice of spying by looking over the victim's shoulder).
- Store the electronic assets in a locked cabinet or desk when not in use, outside of the office premises.
- Do not leave your electronic assets in your vehicle. If it is necessary to leave the assets in your vehicle for a very short period, the assets must be locked inside the vehicle.
- When using electronic assets in public areas, do not leave them unattended for any length of time.
- Electronic assets can be damaged by factors like any liquid, extreme dust, extreme temperatures, etc. It's everyone's responsibility to protect the assets from these factors.

2.1 During travel

- Do not pack your electronic assets in checked luggage.
- Attach a name tag or business card to your electronic device and carrying bags for easy identification during security checks or if it is lost.
- Store the electronic assets in a hotel room safely or lock them in a suitcase/locker when you are not in the room.

3. Guidelines

Here, are the guidelines to ensure the safety of the assets

- Shut down your system as you close the work for the day. And, please shut down the system in case you are planning for a long leave. This indeed increases the performance of the system and the battery.

- The password policy implemented in the systems includes a validity of 90 days. If the system is left to sleep for a long time, you may not be able to log in to the system with the existing password if it has expired. Restart the system daily to reset the password at a defined interval.
- Please ensure that the electrical power supply you are working on is stable enough with proper grounding to safeguard your system. Also, please check that the power socket is appropriately inserted. Some sockets may not be tight enough, creating friction in passing the electricity through them.
- If you feel like your system is getting overheated, then please keep it in Sleep Mode for a couple of minutes then resume working. But if you feel like you have to do this frequently then please contact the Network team.
- Please ensure that you use your system on a flat surface to ensure proper airflow. Please avoid keeping the system on flexible surfaces like beds, pillows or cushions to prevent air block.
- Don't place the water bottle near the laptop, the liquid may spill on the laptop. Please ensure the bag you use for your laptop and the workplace you use to keep your laptop is neat and clean and is away from eatables, which usually attract insects and ants. Also, we recommend cleaning your laptop at least twice weekly with Laptop cleaning gel to prevent it from getting affected.
- Most of the devices we use are under warranty/AMC period. So we urge you to let the network team know about the issues in relation with the system or testing device as earlier as possible. This will make it easier for us to address the issue effectively under the said warranty itself, if possible.

4. Policy Violations:

Any damage or theft of company assets results in this policy violation. Any violation of the policy has to be updated to the company immediately.

If the company found that assets are damaged/stolen due to negligence, the Employee/Intern will be responsible for the cost of repairing/replacing the same. These policy violations might affect your employment based on the severity of the negligence.

Asset damage has been categorised into three types. Depending on the damage category, repairing or replacement costs will be applied.

4.1 Natural Issue

Any hardware(Motherboard, SSD, Speaker, Mic, Keyboard, Screen, Charger, Battery, etc.) issues which occur due to the life span of the assets, belongs to this category.

For this category of issues, Mallow will manage the repair or replacement of the system.

4.2 Issue because of Negligence

The following types of issues are included in this category.

- Liquid damage
- Damage due to power fluctuation
- Physical damage
- Any hardware(Motherboard, SSD, Speaker, Mic, Keyboard, Screen, Charger, Battery, etc.) issues due to the user's Negligence

For this category of issues, the employee has to bear the repairing or replacing cost. However, the Network team will evaluate the issue before making the final decision. The final decision lies with the Network team.

4.3 Unidentified

In case of any issue that is not listed in any of the above two categories (Issue because of Negligence or Natural Issue) occurs, then the final decision will be based on the type of issue and our policy. The Network team will consider a specific set of checkpoints before making a decision.

5. Details and Declaration

Please sign below to indicate receipt of the Asset, agree to the policy and to authorise the deduction of the respective amount if the assets are damaged/lost/stolen.

Make: Configuration:

Model: Serial No.:

Asset Tag:

Monitor : Yes / No

Data Card : Yes / No

KeyBoard : Yes / No

Mouse : Yes / No

Employee's/Intern's Full Name:

Designation:

Employee's/Intern's Signature:

Date:

Asset Upgrade Details:

Asset Info	Asset Tag	Serial No	Issue Date	Employee Sign	Return date	Receiver Sign

Table 1

Employee Exit Date:

Employee Signature:

Asset In-charge Signature: