CONTROLLED

Vilcom Networks Limited IT Asset Management & Disposal Policy	Document No.	Policy/31
	Version No.	1.0
	Classification	Restricted
	Date	03.07.2025

Policy for IT Asset Management& Disposal

1.Purpose

This policy provides guidelines for the management, assignment, and protection of IT assets within Vilcom Networks Limited. It ensures that all IT assets, including laptops, desktops, mobile devices, and peripherals, are properly tracked, secured, and maintained. The policy also outlines procedures for reporting and handling asset damage, theft, and loss. All information assets and equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.

2. Scope

This policy applies to all employees, contractors, and third-party users who are assigned IT assets by Vilcom Networks Limited. It covers the management of assets from assignment to return and addresses procedures in the case of damage, loss, or theft.

3. Asset Assignment Policy

3.1. Asset Allocation and Registration

- IT assets will be assigned to employees based on departmental needs and job responsibilities.
- Each asset will be registered in the Inventory Management System and assigned a unique identifier (serial number, model, etc.).
- Employees upon accessing the asset portal, they acknowledge receipt and responsibility for the assigned equipment in the asset management portal as stated this document.

3.2. Responsibilities of the Employee

- Employees must use assigned assets solely for work-related purposes. Employees are responsible for the safekeeping, maintenance, and security of the assigned equipment.
- Any transfer of the asset to another employee or department requires approval from IT.

- Using personal laptops for work may expose company data to security risks. All work-related tasks should be conducted on the assigned company laptop, except in the following cases:

  Work Emergencies - If the company laptop is unavailable, employees may temporarily use a personal laptop with IT or management approval, ensuring security protocols are followed.

  Remote Work -Employees may use a personal laptop with IT approval when working remotely, ensuring secure work practices.

3.3. Security of Assets off premises.

- Whenever IT assets are used outside the office including issued and temporary assigned shall adhere to this policy for the purposes of safety of the asset and information security as highlighted in clause 3.2 above.

3.4. Returning Assets

- Upon resignation, termination, or internal transfer, employees are required to return all IT assets to the IT department.
- An Exit Checklist will be completed, including asset inspection and acknowledgment of return.

4. Asset Damage Policy

4.1. Reporting Damage

- Employees must immediately report any damage, loss, or malfunction of assigned IT assets to the IT Department.
- A Damage report must be submitted detailing the nature of the damage and how it occurred.

4.2. Assessing Liability

- If damage is caused by negligence (e.g., dropping the device, spilling liquids, misuse), the employee may be held financially liable for repair or replacement costs.
- The IT department will evaluate the damage and decide whether the asset can be repaired or needs to be replaced.

- Repeated Negligence to those employees who repeatedly damage assets due to carelessness or misuse may face disciplinary action and be required to contribute to the replacement costs.

4.3. Damage Not Caused by Negligence

- If the damage is due to normal wear and tear or technical malfunction, the IT department will manage the repair or replacement without charging the employee.

4.4. Preventative Maintenance

- Employees must ensure that devices are regularly updated with security patches and antivirus software.
- The IT department will provide regular checks and updates for all assets as part of the maintenance process.

5. Asset Theft or Loss Policy

5.1. Reporting Theft or Loss

- In the event of theft or loss, the employee must report the incident immediately to IT and to the local authorities (police).
- A police report (or police abstract) must be filed within 24 hours of the incident and submitted to IT for record-keeping.

5.2. Liability for Theft or Loss

- If the theft or loss occurs due to employee negligence, the employee may be held financially responsible for the asset's replacement.
- If theft occurs under reasonable circumstances (e.g., burglary or forceful entry), the company will work with the employee and the authorities to investigate and resolve the issue.

Vilcom Networks Limited IT Asset Management & Disposal Policy	Document No.	Policy/31
	Version No.	1.0
	Classification	Restricted
	Date	03.07.2025

6. Asset Return and Disposal

6.1. End-of-Life Equipment Disposal

- When IT assets reach the end of their useful life, they must be returned to the IT department for proper disposal or recycling in accordance with environmental regulations and best practices.
- Sensitive data will be completely wiped from the device using secure data destruction methods before disposal.

6.2. Data Wiping and Disposal Standards

- IT will perform data wiping using available tools to ensure no data is recoverable before assets are recycled or disposed of.

7. Compliance and Monitoring

- Non-compliance with this policy may result in disciplinary actions and could involve the employee paying for asset repairs or replacement if negligence is proven.
- Periodic Audits will be conducted to ensure compliance with the asset management process, including random checks of asset locations and usage.