# Asset Tracking Policy

1. Introduction........................................................................................................................3

1.1 Linked policies........................................................................................................3

2. Definitions..........................................................................................................................3

2.1 Material asset.........................................................................................................4

2.2 Material asset in use ..............................................................................................4

2.3 Material asset in storage ........................................................................................4

2.4 Material asset in waiting .........................................................................................4

2.5 Skilled user.............................................................................................................5

2.6 Unskilled user.........................................................................................................5

2.7 Data Breach Policy Owner .....................................................................................5

3. Policy.................................................................................................................................5

3.1 Labelling of material assets....................................................................................5

3.2 Asset inventory.......................................................................................................5

3.3 Updating the asset inventory..................................................................................6

3.4 Asset review...........................................................................................................7

3.5 Discrepancies uncovered in the asset review.........................................................7

3.6 Completing the asset review ..................................................................................7

**1. Introduction**

Ufix recognises that as a business they need to be careful with their data, such data includes client documents, staff data, administrative username, and passwords. All of which must be also kept as a back up in a data centre such as a remote back up server which is highly secured.

All of our assets are kept in a way that a user taking out an asset must comply with the following:

• All equipment be held in a locked rack: Equipment includes assets such as laptops and keys for rooms.

• That the rack be always locked unless a verified engineer is working on site and is physically present at the rack.

• CCTV must continuously monitor the rack and covers the surrounding area of our equipment is located.

This policy does not ignore the fact however, that there may be entities in or out of Ufix that may use said assets for malicious intent to use against Ufix.

**1.1 Linked policies**

This policy has links to, but does not set out here, policies with respect to:

• The security of the data centre environments in which we operate and related access controls. This can be linked to many environments in the company such as the disciplinary aspect.

• Secure disposal of assets.

**2. Definitions**

**2.1 Material Asset**

A material asset is identified by Ufix as a means of transportation (cars), the ability to book a room for conferencing, laptops or any means of communication.

**2.2 Material asset in use**

This is a sub class of material asset. All the conditions applying to the definition of a material asset apply to this sub class. A material asset is deemed to be in use when it is electronically active i.e the tracking of cars using the navigation system installed on the vehicle

**2.3 Material asset in storage**

This is a sub class of material asset. All the conditions applying to the definition of a material asset apply to this sub class.

A material asset is deemed in storage where it has previously been a material asset in use and, therefore is in a state where it is available and deemed in an appropriate state for reuse.

Such an asset will normally be identifiable by criteria such as:

• Being electrically powered or cabled.

• Having evidence of wear and tear associated with prior use.

• Being held in a storage drawer within the environment.

• Being in an unsealed box, anti-static envelope, or similar container.

**2.4 Material asset in waiting**

This is a sub class of material asset. All of the conditions applying to the definition of a material asset apply to this sub class.

That is, a material asset in waiting will contain no confidential data, material assets in waiting can be identified as a spare part which will be used to fix an asset in storage.

Such an asset will normally be identifiable by criteria such as:

• Not being electrically powered or cabled.

• Having no evidence of wear and tear associated with prior use.

• being held in a storage drawer within the environment.

• being in a supplier sealed box, anti-static envelope, or similar container.

Please note that the material in waiting must be in pristine condition which allows the engineers to install the appropriate software to the devices/vehicles.

**2.5 Skilled user**

Ufix has deemed a skilled to be any individual with the competence to manipulate material assets. A skilled user would, for example, would be capable of exchanging material assets, having use to disciplinary’s/staff data. Ufix has used managers and administration as the example for such skilled users.

**2.6 Unskilled user**

The definition of unskilled users includes, for examples, customer advisors who are capable of identifying individuals who have taken out assets and understanding the system but not having the capability of validating themselves.

**2.7 Data Breach Policy Owner**

Ufix recognises that there must be a person responsible for the management of staff data and the administrative system and therefore have appointed this to the IT security manager

**3. Policy**

**3.1 Labelling of material assets**

We will require that all material assets in use and all material assets in storage in any data centre shall be identifiable by a unique, vendor supplied, serial number. This serial number shall be permanently fixed to the material asset by a means that makes attempt to tamper evident.

**3.2 Asset inventory**

An inventory must be created to keep track of said assets, independently of the supplier. A separate inventory must be in use to show the assets on loan at one time. This can be done through the means of a database and must be kept in a permanent form. The database, on demand, should be able to produce a report of the assets in the company and could be exported to PDF for managements use.

As a minimum, for the purposes of this policy, the asset inventory must include, for each material asset in use and each material asset in storage:

• Supplier.

• Serial number.

• Part number or name so that an unskilled user can identify a product for returning and retrieving the products.

Any asset that is broken or at the end of life must be reported and known to the company for replacement/maintenance of the products.

**3.3 Updating the asset inventory**

The separate database data set must be used to represent the following information:

• An asset that has been taken out of use.

• The time and date in which this is done.

• A new asset being introduced into the company.

There may be policies that deal with secure disposal of material assets in storage and related topics. However, this policy is only concerned with tracking the inventory. Updating the information of the

**3.4 Asset review**

A yearly report must be undertaken by the head of IT security management and reviewed by a separate entity from Ufix, this means if there are any discrepancies in the inventory, that it can be investigated by an entity not related to the company, yet they don’t have the ability to make changes to said inventory.

**3.5 Discrepancies uncovered in the asset review**

It is possible that the asset review will reveal discrepancies between the material assets in use or material assets in storage and those recorded on the asset inventory. For example, an asset may have been taken out for a longer period but yet not recorded for said time.

**3.6 Completing the asset review**

Once the asset review has been completed (assuming all discrepancies are deemed valid and the asset inventory duly updated) the following information will be recorded:

• Date of review.

• Name of the reviewing party.

• The employee identifications of the reviewing party.

• Discrepancies, along with the validation of said assets with not being recorded.

The review will then be countersigned by a manager of Ufix who will review all the material and will document it to the system. POLICY DOCUMENT ENDS