Asset Management Policy

1. Assets

Business assets include:

- hardware - including electronic storage media, ICT equipment;
- software - including applications, services, IT systems, software patches;
- data and information - including data sets and documents; and
- other Intellectual Property.

Use of assets covers processes to:

- acquire, transport, store, manage, maintain and dispose of assets; and specifically
- design, operate, maintain or support, decommission and dispose of hardware, services and systems used by the organisation.

2. Custodian

An asset held by MENU is owned by the organisation, or is owned by a 3rd party, and the organisation is responsible for handling it appropriately on behalf of the owner.

Each business asset held by MENU has a named custodian who is the member of staff who is held accountable for the security of that asset.

The member of staff that creates or first acquires an asset automatically becomes the custodian.

MENU Technologies AG · Dammstrasse 19 · 6301 Zug, Switzerland · +41 41 723 2041 · hello@menu.app

A manager with a legitimate interest in an asset may change the custodian of that asset, provided that they have the agreement of the line managers of the current and proposed new custodians.

3. Asset classification and marking

MENU business assets must be classified <Confidential> or <Sensitive> and where possible each must carry a marking to show the classification level.

The classification of an asset determines how the asset is be handled, including how it should be protected and who should be allowed access to it.

For the classification levels, associated labels and access rules please refer to the MENU Asset Classification Policy.

4. Handling classified assets

The custodian of <Confidential> and <Sensitive> assets must ensure that a non-disclosure agreement is in place before disclosing the asset to a third party.

<Sensitive> assets must never be left unattended in any place where unauthorised persons might gain access to them.

The asset custodian must ensure that classified material is removed from systems and hardware devices when they are decommissioned or disposed of.

5. Storage services

A member of staff must seek permission from their line manager to use a 3rd party service to store or transfer MENU's data assets.

The manager must only grant permission for use of services approved by Security Management.

6. Removable media

MENU does not allow removable media, such as USB sticks, CDs or DVDs to store or transfer data.

7. Mobile devices

A mobile device is a portable end-user device (EUD), including a laptop, tablet, mobile phone or smartphone, which may be owned by MENU or the employee, or a supplier.

The line manager must approve the use of mobile devices for business purposes (privately or business owned) before they may be used.

The End User Device (EUD) Policy[1] describes how a mobile device must be configured and used for Bring Your Own Devices (BYODs).

When configuring, using and decommissioning an EUD, you must conform to the EUD Policy.

---

[1] **Registration of personal mobile devices for business use**
Employees when using personal devices for business use will register the device with MENU's system administrator, who is under the direct supervision of the CTO.

Personal mobile devices can only be used for the following business purposes:
- Email access
- Business internet access
- Business telephone calls

Each employee who utilises personal mobile devices agrees:
- Not to download or transfer business or personal sensitive information to the device. Sensitive information includes any type of business and customer data, intellectual property, other employee details or any other business related data.
- Not to use the registered mobile device as the sole repository for MENU information. Any business information stored on mobile devices should be backed up.
- To make every reasonable effort to ensure that MENU's information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected.
- To maintain the device with current operating software and current security software.
- Not to share the device with other individuals to protect the business data access through the device.
- To abide by MENU's internet policy for appropriate use and access of internet sites.
- To notify MENU immediately in the event of loss or theft of the registered device.
- Not to connect USB memory sticks from an untrusted or unknown source to MENU's equipment.

All employees who have a registered personal mobile device for business use acknowledge that the business:
- Owns all intellectual property created on the device.
- Can access all data held on the device, including personal data.
- Will regularly back-up data held on the device.
- Will delete all data held on the device in the event of loss or theft of the device.
- Has first right to buy the device where the employee wants to sell the device.
- Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data.
- Has the right to deregister the device for business use at any time.

Keeping mobile devices secure
The following must be observed when handling mobile computing devices:
- Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away.
- Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended.
- Mobile devices should be carried as hand luggage when travelling by aircraft.

8. Sensitive physical assets

<Sensitive> physical assets must only be stored in a safe or specialised storage facility. The safe custodian must limit access to a small number of named staff, under the authority of a MENU board member.

Only members of staff to whom access has been specifically granted in the associated name list are allowed to access <Sensitive> assets.

No <Sensitive> asset must be used, transferred or transported unless an associated risk assessment has been performed, and the associated risks have been accepted by the asset custodian and Security Management.

9. Disposal of Media

When no longer required media must be disposed securely by following documented procedures (Data Disposal Policy). These procedures minimise the risk of confidential information leakage to unauthorised parties.