Data Classification Policy

1. Purpose

The pupose of data classification policy is to establish a process for classifying and handling data assets based on its level of sensitivity, value and criticality to MENU and its Customers. As such, these procedures help asset custodians to ensure that assets are identified, marked, handled and who should get access to it so as to safeguard the information security of such assets.

2. Classification levels

MENU assets must be classified “Confidential” or “Sensitive” and where possible each must carry a marking to show the classification level. If an asset is not marked it is deemed not to require protection.

The classification levels, associated labels and access rules are summarised in Table 1.

Classification	*Marking*	*Access to asset*
«**Confidential**»	**Confidential**	MENU asset that must be held confidential to MENU, but may be accessed by 3rd parties under suitable contract.
	MENU: «Internal use only»	A Confidential asset that must only be accessed by members of staff.
	«**Personal**»	A Confidential asset that contains non-sensitive PII, which must only be accessed by members of staff.

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

«**Sensitive**»	«**MENU Directors eyes only**»	A «Sensitive» MENU asset that must only be accessed by the Directors of MENU.
«**Sensitive Personal**»	«**Sensitive Personal: MENU Directors eyes only**»	A MENU asset that contains sensitive PII that must only be accessed by the Directors of MENU.

A MENU asset must assert copyright when disclosed outside of the organisation.

3. Classifying an asset

The custodian of an asset must assign a classification to the asset that is appropriate to the confidentiality or sensitivity of the asset or its contents.

3rd-party assets, including software, such as applications, must be classified «Confidential» or higher.

When classifying an asset, special care needs to be taken with the increased risk and sensitivity:

- when the asset contains Personally Identifiable Information (PII);
- through aggregation of data; and
- with certain types of data processing, including pattern finding and when data could be linked.

In such cases it may become necessary to increase the classification level.

Classification alone is only guidance. The custodian must protect the asset appropriately, and ensure that the asset is handled appropriately after considering the risks to that asset.

The asset custodian must make staff and users aware of specific contractual conditions that may apply to the handling of specific assets.

The creator of a document or data set must assign an appropriate classification as soon as the document is generated, according to the expected content, and making allowance for the likely increase of information in the asset over time.

A document is any object generated in GSuite, or equivalent. A data set is a file, directory, database or data repository.

The classification marking of a document must be displayed clearly in the document when it is displayed on a screen, and when the document is printed to physical form.

The creator of the document must add the markings to the document as soon as possible. An editor of a document must increase the classification level when changes to the document increase the sensitivity of its contents.

A user must not reduce the classification of a document without consulting the asset custodian.

4. Personally Identifiable Information (PII)

An asset that contains personal information must be treated with special care, and must be handled in compliance with the relevant data protection regulations.

An asset that contains Personally Identifiable Information (PII) must be classified either «Confidential» or «Sensitive», appropriate to the sensitivity of its contents.

Where possible the asset must be marked with, as appropriate:

- «**Personal**»

  or

- «**Sensitive Personal: MENU Directors eyes only**»

«Sensitive PII» is defined in GDPR, and could create significant risks to a person's fundamental rights and freedoms, for example, by putting them at risk of unlawful discrimination.

«Sensitive PII» includes information about:

- race or ethnic origin;
- religion;
- politics or trade union membership;
- genetics or health;
- biometrics (where used for ID purposes); or
- sex life, sexual orientation.

Staff must also classify and handle financial and PII as «Sensitive».

An asset containing sensitive PII must only be accessed by members of staff that are identified in the list of names associated with the classification, and marked on the asset whenever possible.

Other assets that contain PII must only be accessed by members of staff.

The custodian must agree special arrangements with the Security Management for access to an asset that contains PII outside of the MENU. The Security Management may refuse access on ground of compliance.

5. Asset register

The MENU Asset Register identifies all important, sensitive or critical business assets and summarises the associated data required for risk assessment, data and information management, and disaster recovery.

For each asset in the register Asset Register specifies:

- the asset type;
- the designated custodian;
- its classification & labels, and criticality;
- its storage location, retention period and format; and
- backup provisions and disposal method.

The Asset Register must specify when an asset is judged to be mission critical, such that its compromise would seriously threaten the business or its operations.

The custodian of a «Sensitive» asset is accountable for ensuring that the asset is recorded accurately and sufficiently in the Asset Register.

Whenever an asset has been designated «Sensitive», the custodian must inform Security Management as soon as possible after an asset has been classified, or re-classified. Security Management must then record the asset and its classification in the Asset Register, and the custodian must assist to ensure that other fields in the Asset Register are completed.

A document, dataset of other items of information that has no classification and does not contain PII does not need a formal owner or to be recorded within the asset register.

An asset custodian may use their discretion on whether to record a Confidential asset in the Asset Register.

6. Personal data

The responsible manager must trigger an Assessment of the need for a Privacy Impact Assessment (APIA) whenever an asset is labelled «Personal», or when they suspect that an asset might contain PII.

Security Management must then conduct a Privacy Impact Assessment (PIA) for each asset that contains PII, and may in turn require an Information Assurance (IA) risk assessment.

The owner of an asset that is labelled «Personal» is accountable for ensuring that the asset is recorded accurately and sufficiently in the Processing Register.

The custodian of an asset that contains PII must consult the Data Protection Officer (DPO) for guidance, before any PII is transferred to a third party.

The custodian must demonstrate to the DPO that a Personal Data Handling Agreement is in place before the asset may be disclosed, transferred to, or processed by, a third party. The custodian of such an asset must ensure that the asset is managed in compliance with GDPR, and other relevant data protection legislation, throughout its whole life cycle until destruction.