YMMOT GUIDELINE ACCE PERMISSIONS

1, Purpose of the Document

This guideline regulates the rules for assigning, recording, managing, controlling and revoking access rights within the information systems, cloud services, web applications and IT infrastructure of the YMMOT

2, Basic Principles

Access is assigned according to the principle:

"Need to Know"

The user has access only to the data and functionalities that the user absolutely needs to perform their job.

"Least Privilege"

The user is given only the minimum range of permissions necessary to perform their tasks.

"Separation of Duties"

Critical processes must be divided between multiple people so that one person cannot independently perform the entire process without control.

3, Access Categories

A. Public user

Access:

- publicly available information.
- homepage.
- public documents.

With no possibility of:

- administration.
- data entry.
- system changes.

B Registered user

Access:

- own profile.
- own data.
- assigned functionalities.

With no access to:

- other users' data.
- system settings.

C. Clerk

Access:

- management of assigned agendas.
- client management.
- process management.

With no possibility of:

- changing security settings.
- system configurations.

D. Administrator

Access:

- user management.
- authorisation management.
- operational settings.

With no automatic access to:

- financial data.

legal documents.
higher-level audit records.

E. Global Administrator

Access:

entire technological infrastructure.
cloud services.
security configurations.
system settings.

Access is subject to:

increased control.
MFA.
audit logs.

4, Authorisation Assignment

Each authorisation must include:

unser name.
account identification.
scope of authorisation.
date of assignment.
approving person.
purpose of access.

Accesses are assigned solely based on the approval of the authorised person.

5, Authorisation records

YMMOT keeps records of:

user accounts.
administrator accounts.
service accounts.
API accounts.
external accesses.
temporary accesses.

6, Temporary Access

Temporary authorisations:

must have a specified expiration date.
are automatically deactivated upon expiration.
are subject to record keeping.

7, External Parties

External contractors can only gain access if:

- they have an approved Access Agreement.
- they have a signed confidentiality agreement.
- they use MFA.
- the scope of access has been defined.

8, Withdrawal of Authorisations

Access is immediately withdrawn upon:

- termination of employment.
- termination of contractual relationship.
- change of job classification.
- security incident.
- decision of YMMOT management.

9, Access Audit

At least once a year, the following is performed:

- active account check,
- administrator privileges check,
- external access check,
- inactive account check.

10, Central Identity Management

YMMOT uses or plans to use centralized identity management through:

- Microsoft Entra ID.
- Microsoft 365.
- Cloud-based security tools.
- Internal authentication systems.

11, Final Provisions

All access to YMMOT systems must be auditable, recorded and granted exclusively in accordance with this Guideline.

Last updated: jun 2026