# YMMOT GUIDELINE PROTECTION OF IDENTIFICATION DATA AND PASSWORDS

## 1. Purpose of the Document

This Guideline governs the rules for the use, protection, management and storage of identification data, login data, passwords, authentication means and access rights within the YMMOT Group.

The document applies to:

- employees.
- managing directors.
- administrators.
- developers.
- external suppliers.
- partners with assigned access.
- users of internal systems.

## 2. Protected Identification Data

Identification data is considered to include, in particular:

- Usernames.
- Logins.
- Passwords.
- PIN codes.
- MFA codes.
- Recovery codes.
- API keys.
- SSH keys.
- Certificates.
- Security tokens.
- Access links.
- System accounts.

## 3. Account Ownership

Each account must be:

- assigned to a specific person.
- registered.
- approved by an authorised person.

Shared accounts are prohibited unless it is a technical or system account approved by the system administrator.

4. Password Requirements

Each password must contain:

- at least 6 characters.
- an uppercase letter.
- a lowercase letter.
- a number.
- a special character.

Recommended length:

- at least 8 characters.

The use of the following is prohibited:

- name of the user.
- company name.
- date of birth.
- simple combinations.
- repeated passwords.

5. Multi-Factor Authentication (MFA)

MFA is required for:

- Microsoft 365.
- Microsoft Entra ID.
- Azure.
- GitHub.
- Web administration.
- Cloud services.
- Email accounts.
- Financial systems.
- Systems containing personal data.

Allowed methods:

- Authenticator.
- FIDO2 security Key.
- Passkeys.

Hardware tokens.

SMS authentication is used only exceptionally and must be approved.

6. Password Management

It is recommended to use an approved Password Manager.

It is prohibited to:

store passwords in Excel.
store passwords in emails.
store passwords in unencrypted documents.
write passwords on paper without security.

7. API and System Keys

API keys and system secrets must be:

stored separately.
encrypted.
recorded.
regularly rotated.

only accessible to the authorised persons.

8. Granting and Revoking Access

Each access must have:

date of assignment.
approving person.
purpose of access.
authorisation level.

Upon termination of cooperation, the following will be performed:

immediate account blocking.

withdrawal of MFA.
cancellation of VPN access.
cancellation of API access.
archiving of audit records

9. Security Incidents

An incident is considered to be:

password disclosure.
device loss.
account compromise.
suspicious login.
unauthorised account use.
authentication data leak.

Every incident is reported immediately to: security@ymmot.eu

10. Audit and Control

YMMOT reserves the right to:

conduct access audits.
check security settings.
check compliance with this policy.
require password changes if compromise is suspected.

11. YMMOT Technical Minimums

All future YMMOT systems require:

MFA.
TLS/SSL encryption.
audit logs.
DEV / TEST / PROD department.
role-based access control (RBAC).
regular backups.
security event monitoring.
central identity management via Microsoft Entra ID.

12. Final Provisions

This Guideline constitutes a binding security standard for all websites, applications, cloud services, AI systems, procurement platforms and internal information systems of the YMMOT Group.

Last updated: jun 2026