YMMOT LIABILITY FOR VIOLATION OF SAFETY AND SECURITY RULES

1. Purpose of the Document

This document regulates the responsibilities of persons who have access to the systems, data, documents, applications, cloud services or other information assets of the YMMOT Group.

It applies to:

- managing directors.
- employees.
- external cooperators.
- suppliers.
- developers.
- administrators.
- consultants.
- persons with assigned access.

2. Obligation to Comply with the Rules

Each authorised person is obliged to comply with:

- YMMOT internal guidelines.
- Personal data protection rules.
- Security policies.
- Access management rules.
- Rules for the use of information systems.
- European Union legislation.
- The legislation of the relevant country of operation.

3. Violations mainly mean

Security breaches

- sharing login details.
- bypassing security measures
- unauthorised account creation.
- unauthorised provision of access.
- use of unauthorised software.
- intentional weakening of system security.

Data protection violations

unauthorised processing of personal data.
unauthorised copying of data.
unauthorised export of data.
disclosure of confidential information.
failure to cooperate in a security incident.

Organisational violations

breach of confidentiality.
failure to comply with the instructions of the system administrator.
failure to report a security incident.
failure to provide truthful information during the investigation of the incident.

4. Violation Measures

Depending on the severity, YMMOT may take one or more of the following measures:

Technical Measures

Changing passwords.
Resetting authentication data.
Blocking the account.
Removing privileges.
Disconnecting the device from the network.
Blocking remote access.

Organisational measures

written warning.
temporary restriction of access.
user retraining.
increased supervision of user activity.

Contractual measures

termination of cooperation.
withdrawal from the contract.
suspension of service provision.
withdrawal of the supplier's authorisations.

5. Compensation for Damages

A person responsible for a breach of obligations may be liable for damage caused to:

YMMOT.
Clients.
Business partners.
Data subjects.
Third parties.

Compensation for damages may include:

direct property damage.
costs of restoring systems.
costs of investigating the incident.
costs of legal defence.
costs arising from regulatory proceedings.

6. Legal Actions

In the event of a serious or intentional violation, YMMOT reserves the right to:

file civil claims.
claim damages.
file an administrative complaint.
file a criminal complaint.
cooperate with public authorities.
exercise other legal remedies.

7. Responsibility of Managers

People performing management or administrative functions have an increased level of responsibility for:

access management.
data protection.
security settings.
supervision of compliance with internal rules.

8. Individual Assessment

Each breach is assessed individually according to:

the extent of the incident.
intent or negligence.
the damage caused.
the impact on systems.
the impact on personal data.
the impact on clients and partners

9. Final Provisions

Revocation of access, termination of cooperation, compensation for damages or legal action may be applied separately or simultaneously depending on the severity of the violation.

This document forms part of the YMMOT Group security and compliance framework for homepage, applications, AI systems, procurement platforms, cloud services and internal information systems.

Last updated: jun 2026