YMMOT STAKEHOLDER/STAKEUP GOVERNANCE FRAMEWORK

1, Purpose of the Document

This document sets out the basic governance and stakeholder architecture of the YMMOT group for:

- Homepage.
- AI systems.
- Procurement platforms.
- Enterprise applications.
- E-Government solutions.
- EU integration projects.

2, Main Stakeholder Groups

Internal stakeholders

- YMMOT management.
- Supervisory Board.
- Executives.
- Developers.
- Team.
- Security team.
- Legal department.
- Economic department.
- Procurement department.

External stakeholders

- Clients.
- Public institutions.
- Suppliers.
- Technology partners.
- Cloud providers.
- Regulators.
- EU entities.

3, Governance Layers

Strategic layer

- Group direction.
- AI governance.
- Security strategy.
- EU compliance.

Operational layer

Systems management.
Administration.
Monitoring.
Incident management.
Access management.

Legal layer

Master compliance policy. (whole group)
Information security policy.
Data retention policy
Data classification policy
Incident response plan
Business continuity plan
AI governance framework
NIS2 compliance framework
RoPA register of processing activities
GDPR.
General Business Terms and Conditions.
DPA.
SLA.
Compliance.
Audit.

4, Stakeup Principle

StakeUp represents the internal principle of YMMOT:

centralisation of management.

separation of risks.

layering of powers.

access control.

protection of the parent structure.

separation of jurisdictions.

auditability of systems.

5. Security Principles

YMMOT implements:

MFA.
Least privilege model.
System segmentation.
Audit logs.
Incident monitoring.
DEV / TEST / PROD department.
Cloud security.

API security.
Aata governance.

6. Future Extensions

This document forms the basis for:

AI governance framework.
Cybersecurity framework.
Procurement governance.
EU data governance.
Enterprise security architecture.
Digital trust framework.

Last updated: jun 2026