YMMOT GUIDELINE REPORTING AND RESOLUTION OF SECURITY INCIDENTS

1. Purpose of the Document

This Guideline governs the procedure for identifying, reporting, recording, investigating and resolving security incidents within the YMMOT group.

It applies to:

- employees.
- executives.
- administrators.
- developers.
- external suppliers.
- users of YMMOT systems.

2. Reporting Obligation

Every security incident must be reported immediately to: security@ymmot.eu

If the incident concerns personal data, it must also be reported to: privacy@ymmot.eu

The report must be made without undue delay after the discovery or suspicion arises.

3. What is considered a security incident

A security incident is considered to be:

Cyber incidents

- unauthorised access to a system.
- an attempt to break into an account.
- an attack on a website.
- DDoS attack.
- malware.
- ransomware.
- phishing.
- email account compromise.
- cloud environment compromise.

Personal data incidents

- data loss.
- unauthorised disclosure of data.
- unauthorised modification of data.
- personal data leakage.
- unauthorised copying of data.

Access incidents

- password disclosure.
- loss of MFA device.
- account sharing.
- misuse of privileges.

Physical incidents

- loss of laptop.
- loss of mobile device.
- theft of device.
- loss of access card.
- unauthorised entry into premises.

4. Report Content

The reporter shall state, where possible:

- name of the reporter.
- date and time of the incident.
- date of detection of the incident.
- description of the incident.
- affected system.
- affected persons.
- extent of damage.
- measures taken.

5. Incident Categorisation

Low severity

- no impact on operations.
- no data leak.
- local problem.

Medium severity

- limited operations.
- suspected compromise.
- partial impact on services.

High severity

data leak.
system compromise.
large-scale outage.
legal or financial consequences.

Critical severity

large-scale cyberattack.
infrastructure compromise.
mass data leak.
threat to the functioning of the organisation.

6. Incident Resolution Procedure

After receiving the notification, the following will be performed:

Phase 1 – Records
incident registration.
allocation of an identifier.
determination of the responsible person.

Phase 2 – Analysis
verification of the facts.
identification of the cause.
identification of the scope of the impact.

Phase 3 – Measures
damage limitation.
system isolation.
access blocking.
restoration of operation.

Phase 4 – Closure
final report.
recommendations.
preventive measures.

7. GDPR Incidents

If the incident constitutes a breach of personal data protection, a separate assessment will be carried out under the GDPR.

If necessary, the following will be ensured:

recording of the incident.
notification to the supervisory authority.
notification to the data subjects.
adoption of corrective measures.

8. Duty to Cooperate

Any person with access to YMMOT systems is obliged to:

cooperate with the investigation.
provide truthful information.
maintain the confidentiality of the investigation.
implement the security measures imposed.

9. Incident Records

YMMOT maintains a central incident register containing:

incident number.
date of occurrence.
date of notification.
incident category.
actions taken.
date of closure.

10. Liability

Intentional concealment of an incident or violation of this policy may result in:

withdrawal of privileges.
disciplinary action.
termination of employment.
compensation for damages.
legal action.

11. Final Provisions

This guideline constitutes a binding framework for the management of security incidents within the homepage, applications, cloud services, AI systems, procurement platforms and other information systems of the YMMOT Group.

Last updated: jun 2026