FACILWORK INFORMATION SECURITY POLICY

Version 1.0 – June 2026

1. Purpose

Facilwork is committed to protecting customer, seller, marketplace, and business data through appropriate technical and organizational security measures.

2. Access Control

Access to systems is restricted to authorized personnel. Role-Based Access Control (RBAC) and the Principle of Least Privilege are applied. Multi-Factor Authentication is used where available.

3. Password Management

Strong password requirements are enforced. Credentials must be protected and are stored using secure cryptographic methods.

4. Infrastructure Security

Infrastructure is hosted on AWS cloud services. Network access is controlled through security groups, firewalls, encrypted communications, monitoring, and logging.

5. Data Encryption

Data is protected in transit using TLS/HTTPS and protected at rest where supported by storage and infrastructure services.

6. Endpoint Security

Company-managed devices are protected with antivirus and endpoint security solutions and kept up to date with security patches.

7. Vulnerability Management

Facilwork performs regular patching, dependency reviews, monitoring, and remediation of identified vulnerabilities.

8. Incident Response

Documented procedures exist for identifying, reporting, investigating, containing, remediating, and communicating security incidents.

9. Data Protection

Personal data is processed according to GDPR principles. Access is limited to authorized personnel and retained only as necessary.

10. Data Deletion

Customer data is deleted or anonymized according to contractual obligations and applicable legal requirements.

11. Employee Responsibilities

Employees and contractors must follow security procedures and maintain confidentiality of information.

12. Contact Information

Privacy Contact: privacy@facilwork.app Security Contact: security@facilwork.app