udai.io — Information Security & Acceptable Use Policy

Version: 1.0 | Effective Date: 2025-09-19 | Owner: People & Operations

1. Purpose

Define security standards that protect the confidentiality, integrity, and availability of udai.io systems and data.

2. Scope & Roles

Applies to all users, devices, vendors, and cloud services. Security roles: System Owners, Data Owners, Security Team, End Users.

3. Data Classification

• Public • Internal • Confidential • Restricted. Handle data according to its classification; default to the higher sensitivity when in doubt.

4. Access Control

Least privilege; role-based access; MFA on all externally accessible systems; unique accounts; no shared passwords; quarterly access reviews.

5. Authentication & Passwords

Use SSO and MFA wherever supported. Passwords must be strong and unique; store only in approved password managers. Never share credentials.

6. Device & Endpoint Security

All laptops and mobile devices must be enrolled in MDM, use full-disk encryption, auto-lock, and up-to-date OS/patches. Antivirus/EDR required.

7. Network & Cloud Security

Use VPN/ZTNA for remote access. Restrict inbound access; segment environments; encrypt data in transit (TLS1.2+). Apply infrastructure as code and security baseline hardening.

8. Secure Development

Follow secure coding standards, code review, SAST/DAST, dependency scanning, and secrets management. Separate dev/test/prod; require approvals for deployments.

9. Logging & Monitoring

Centralize logs; enable security alerts for auth, privilege escalation, data exfiltration. Retain logs per legal/contractual requirements.

10. Incident Response

Report incidents immediately to Security. Severity levels (SEV-1 to SEV-4). Use triage, containment, eradication, recovery, and post-incident review. Notify customers/regulators as required.

11. Acceptable Use

Company resources are for business use. Prohibited: unlawful content, harassment, circumventing security, unauthorized software, mining crypto, excessive personal use that impacts work.

12. Third Parties & Vendors

Perform security due diligence; require DPAs and minimum security controls; review SOC 2/ISO 27001 reports as applicable.

13. Backup & Business Continuity

Protect critical systems with regular backups, tested restores, and documented RTO/RPO. Maintain and test DR plans.

14. Enforcement & Exceptions

Non-compliance may lead to disciplinary action. Exceptions require risk acceptance by Security and executive approval; time-bound with compensating controls.

15. Revision History

Version 1.0 — Initial publication.