# udai.io — Remote Work & BYOD Policy

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

## 1. Purpose

Establish consistent requirements for remote/hybrid work and the use of personally owned devices (BYOD) at udai.io.

## 2. Eligibility & Work Standards

Remote/hybrid eligibility is role-based and manager-approved. Maintain a safe, ergonomic workspace; meet performance, availability, and communication expectations.

## 3. Hours, Availability & Communication

Agree core hours with your manager. Be reachable on approved channels and update status when away. Follow meeting etiquette and documentation best practices.

## 4. Equipment & Expenses

Company issues standard equipment per role. BYOD allowed with MDM enrollment. Reasonable, pre-approved business expenses are reimbursable per the expense policy.

## 5. Security Requirements for Remote/BYOD

Mandatory: device encryption, screen lock, OS/app updates, no shared accounts, VPN/ZTNA for access, no local storage of Restricted data, report loss/theft within 24 hours.

## 6. Data Handling

Store files on approved cloud repositories; avoid personal email or unapproved apps. Use DLP controls where provided. Dispose of physical notes securely.

## 7. Privacy

udai.io may collect limited telemetry on managed devices for security and compliance. BYOD participants consent to MDM policies (e.g., remote wipe of company data container).

## 8. Travel & Cross-Border Access

Follow export controls and data residency restrictions. Use extra caution on public Wi■Fi and in high■risk locations.

## 9. Exceptions & Enforcement

Exceptions require manager + Security approval. Violations may result in loss of remote/BYOD privileges and disciplinary action.

# 10. Revision History

Version 1.0 — Initial publication.