Tadkeek — Acceptable-Use Policy (AUP)

Aligned with ISO / IEC 27001:2022 Annex A • Saudi PDPL • applies to all employees, contractors and third-party users

---

1 Purpose

This Policy sets the conditions under which Tadkeek information systems, networks and data may be accessed and used. Its goals are to:

- protect client and candidate information from unauthorised disclosure, alteration or destruction;
- meet legal and contractual requirements (KSA PDPL, SDAIA regulations, client NDAs);
- support ISO 27001 control objectives (A.5–A.8, A.12, A.18).

2 Scope

Applies to **all users** (employees, consultants, interns, temporary and third-party personnel) who access:

- Tadkeek-owned or –managed laptops, mobile devices, servers and cloud services;
- Tadkeek data processed on third-party platforms;
- physical facilities (Riyadh HQ and any remote offices).

3 User Responsibilities

#	You MUST…
3.1	Use only the accounts and privileges that have been formally assigned to you (least-privilege).
3.2	Keep your passwords & MFA tokens secret; change them immediately if you suspect compromise.
3.3	Lock your screen or log out when leaving your workstation unattended (even for a short time).
3.4	Encrypt confidential data before storing it on removable media or sending externally.
3.5	Report **within 30 minutes** any suspected security incident, lost device or policy breach to `communication@tadkeek.com` or the SOC hotline +966-54-218-2925.
3.6	Comply with all applicable laws, including PDPL and copyright regulations.

4 Permitted Use

You may use Tadkeek systems to:

- Perform your assigned job functions (background screening, client communication, research).
- Conduct limited personal tasks (e-banking, family e-mail) **outside core work hours** provided it does **not** interfere with business, consume excessive bandwidth or violate Section 5.

5 Prohibited Use

It is strictly forbidden to:

1. Access, store or transmit content that is illegal, extremist, pornographic or discriminatory.
2. Share client or candidate data with unauthorised persons, including via personal cloud storage or messaging apps (WhatsApp, Telegram, etc.).
3. Disable or bypass security controls: antivirus, EDR, VPN, content filters, logging.
4. Install unlicensed software or make unauthorised configuration changes to company devices.
5. Use Tadkeek e-mail to commit or endorse fraudulent, defamatory or offensive activity.
6. Introduce malware or conduct penetration testing without written authorisation from InfoSec.
7. Remove or destroy company records without approval and documented retention review.

6 Remote & Mobile Working

- Connect **only** via the company VPN; public Wi-Fi must be protected with WPA2/WPA3 and VPN.
- Company data stored on mobile devices must be encrypted and wiped automatically after 10 failed login attempts.
- Do not discuss confidential information in public areas or when unauthorised parties may overhear.

7 Monitoring & Privacy

Tadkeek logs and monitors network traffic, e-mail, file transfers and device health for security and compliance (ISO 27001 A.12.4). Personal use of systems indicates **consent to such monitoring**. Logs are retained for one year and may be provided to authorities where legally required.

8 Sanctions for Non-Compliance

Violations may result in:

- Immediate removal of system access;
- Disciplinary action up to and including termination of employment or contract;
- Civil or criminal liability under KSA law.

9 Policy Maintenance

- Owner: Information Security Manager
- Review cycle: at least **annually** and after any major regulatory or business change.
- Last approved by the Executive Board: **25 May 2025**
- Next scheduled review: **25 May 2026**