Access Control Policy

Pronounced80 Solutions Limited

Freeing business from the tyranny of legacy software

Version 1.0 | Effective: May 2026 | Review: Annual

1. Purpose

To control access to information and systems on a least-privilege, need-to-know basis.

2. Scope

All systems, cloud services and data used by Pronounced80 Solutions Limited and its personnel.

3. User Access

- Unique, named accounts; no shared credentials.
- Strong passwords managed via an approved password manager.
- Multi-factor authentication enabled where supported (mandatory for email, cloud admin, source control, identity provider).

4. Privileged Access

- Admin access granted only where required for role.
- Production / client environment access is logged and reviewed.
- Just-in-time elevation preferred where supported by the platform.

5. Joiners, Movers, Leavers

- Access provisioned on documented authorisation.
- Access reviewed on role change.
- Access revoked promptly on departure or end of engagement.

6. Client Systems

- Access only with written authorisation and within agreed scope.
- Use of client-issued credentials where required; otherwise federated/SSO where available.
- No long-lived credentials stored outside approved secret stores.

7. Remote Access

- Performed from managed/approved devices over encrypted channels (TLS, VPN where required by client).

8. Reviews

- Periodic access reviews of cloud, source control, identity and email.
- Audit logs retained per provider defaults.

9. Enforcement

Breaches of this policy may result in disciplinary action, contract review or legal action.