# Information Security Policy

## Pronounced80 Solutions Limited

*Freeing business from the tyranny of legacy software*

Version 1.0 | Effective: May 2026 | Review: Annual

Owner: Director (acting as Information Security Lead)

## 1. Purpose

To protect the confidentiality, integrity and availability of information handled by Pronounced80 Solutions Limited and our clients.

## 2. Scope

Applies to all personnel, contractors, devices, systems and information assets used in the delivery of our services.

## 3. Principles

- Least privilege and need-to-know access.
- Defence in depth and secure-by-default.
- Risk-based decision making.
- Compliance with UK GDPR, the Data Protection Act 2018, and applicable contractual obligations.

## 4. Roles and Responsibilities

- **Director / Information Security Lead:** owns this policy, risk register, incident response and supplier assurance.
- **All personnel:** must follow this policy and report security concerns promptly.

## 5. Asset and Information Management

- Information is classified as Public, Internal, Confidential or Client Confidential.
- Client data is handled per contract and stored only in approved systems.

## 6. Access Control

- Unique accounts, strong authentication and MFA where supported.
- Access reviewed periodically and revoked promptly on role change/exit.
- See Access Control Policy.

## 7. Endpoint and Device Security

- Disk encryption, screen lock, automatic updates, endpoint protection.
- See Mobile Device Policy and BYOD Policy.

## 8. Cryptography

- TLS for data in transit; encryption at rest using platform-native services (e.g. Azure Storage Service Encryption, AWS KMS).
- Secrets managed in approved secret stores; no secrets in source control.

## 9. Cloud and Supplier Security

- Use of reputable cloud providers (Microsoft Azure, AWS, Microsoft 365).
- Supplier assessment and contractual security/data protection terms.

## 10. Vulnerability and Patch Management

- Operating systems, browsers and tooling kept current.
- Dependencies monitored; critical issues remediated promptly.

## 11. Logging and Monitoring

- Use of provider-native logging (Azure / AWS / Microsoft 365) for relevant activity and security events.

## 12. Secure Development

- Source control with review, secret scanning, dependency scanning and least-privilege deployment credentials.

## 13. Incident Management

- Documented process for detect, log, triage, contain, resolve, review.
- Notification to affected clients without undue delay (see DPP, BCP).

## 14. Business Continuity

- See Business Continuity Plan and Disaster Recovery Plan.

## 15. Training and Awareness

- Security and data protection awareness undertaken at onboarding and refreshed at least annually.

## 16. Compliance and Review

- Reviewed at least annually or after significant change/incident.