

Security & Compliance Pack

The answers your IT, InfoSec and procurement teams ask for, in one document. This is the public summary; the full audit reports, Data Processing Agreement and sub-processor list are available under NDA.

Duress — workplace safety technology: hardware, software and 24/7 accredited monitoring.

Last updated 17 September 2026

At a glance

Certification / accreditation	Scope
ISO/IEC 27001:2022	Information security management system — global
SOC 2 Type II	Report available under NDA
Vanta continuous controls monitoring	Ongoing, automated control monitoring
ASIAL Grade A1	Australian monitoring centre
BS 5979 / NSI Gold	UK monitoring centre
ULC	Canada monitoring centre
EN 50518	EU monitoring centre standard

Certifications & attestations

ISO/IEC 27001:2022 certified.

Independent third-party audited information security management system. Certificate provided in the full pack; annual surveillance audits.

SOC 2 Type II.

SOC 2 Type II and ISO 27001 audit reports are available under NDA — email security@duress.com to request.

Continuous controls monitoring via Vanta.

Security controls are monitored continuously and automatically, not just at audit time.

Encryption

AES-256 in transit and at rest.

All customer data is encrypted with AES-256 in transit (TLS 1.3) and at rest. TLS 1.2 minimum on all endpoints. Per-tenant encryption keys — no shared crypto material between customers.

Mutual TLS for devices.

Device-to-platform communications use mutual TLS where supported.

Data residency

Data stays in your region.

AU customers on AWS Sydney. UK on AWS London. NZ on AWS Auckland. US on AWS Virginia. Multi-AZ deployment. No cross-region replication of customer data without explicit consent.

Backups.

Daily backups, encrypted at rest, held in-region.

Access & identity

Single sign-on through your IdP.

SAML 2.0, OpenID Connect and OAuth2. Works with Azure AD / Entra, Okta, Google Workspace and Ping. Just-in-time and SCIM 2.0 provisioning.

Role-based access & audit.

Group-based role assignment (RBAC), a full audit log of administrative and operational activity, and remote device wipe.

Privacy & data protection

Region-appropriate privacy frameworks.

Adherence to GDPR, the Australian Privacy Act 1988, PIPEDA and UK GDPR as applicable to your region.

Data subject rights & controls.

DPIA support, a subject-access-request workflow, and per-tenant data retention controls. A Data Processing Agreement (DPA) is available, and the Data Protection Officer is contactable in the full pack.

AI usage — transparent

We tell you where AI assists.

Where AI assists (audio detection, fatigue flagging, content drafting) we tell you, name the model class, and document the human-review step. No customer data is used for training, and there is no silent training on your data.

Monitoring centres

Accredited 24/7 response, per region.

Australia: ASIAL Grade A1. United Kingdom: BS 5979 / NSI Gold. Canada: ULC. European Union: EN 50518. Average alert pickup is measured in seconds, every alert.

Vulnerability disclosure

Report it to us.

Found a vulnerability? Email security@duress.com. We aim to acknowledge within 24 hours.

Requesting the full pack

The following are available under NDA — email security@duress.com:

- SOC 2 Type II report and the ISO 27001 certificate
- Data Processing Agreement (DPA)
- Current sub-processor list
- Completed common InfoSec questionnaire (CAIQ / SIG-style)

Duress Pty Ltd · security@duress.com · duress.com/security