

# Information Security and Confidentiality Policy

Critical infrastructure customers trust us with sites, drawings and data. We protect them.

|          |            |         |              |            |                                               |
|----------|------------|---------|--------------|------------|-----------------------------------------------|
| Document | SI-POL-004 | Version | 1.0          | Effective  | October 2026                                  |
| Owner    | Director   | Review  | October 2027 | Applies to | All employees, contractors and subcontractors |

## Our commitments

- Use customer information only for the purpose it was provided, and share it on a need-to-know basis.
- Store drawings and site data on access-controlled systems protected by multi-factor authentication.
- Bind employees and subcontractors to confidentiality obligations.
- Agree personnel, information and site-access security requirements with Defence and critical infrastructure customers at contract stage, and meet them.
- Take no photographs on a customer site without permission, and publish no site images without the customer's approval.
- Report a suspected breach of customer information to the customer promptly, and meet the Notifiable Data Breaches scheme under the Privacy Act 1988 (Cth) where it applies.
- Dispose of records and devices securely.

The Director is accountable for this policy. Every employee and subcontractor is responsible for following it.

This policy is reviewed annually, and after any significant incident or change.

---

Director, SI Critical Systems

---

Date

