Security Policy

1. Introduction

At 308 One Pty Ltd, hereafter referred to as "308", we uphold the highest standards of cybersecurity governance and practice. Our cybersecurity strategy aligns with both the Australian Signals Directorate (ASD) Essential Eight at Maturity Level Two and ISO/IEC 27001. We are actively reconciling our policies and controls against these frameworks as part of our commitment to security excellence and in preparation for formal audit and certification.

This policy outlines the cybersecurity measures 308 has in place to protect our website visitors, potential customers, partners, and other stakeholders who engage with us. Our goal is to ensure a secure and transparent interaction while maintaining the confidentiality, integrity, and availability of information shared with us.

2. Governance & Compliance

308 is dedicated to a robust cybersecurity governance framework, incorporating:

- ASD Essential Eight – Maturity Level Three: Implementing best-practice mitigation strategies against cyber threats.
- ISO/IEC 27001 Compliance: Establishing and maintaining an Information Security Management System (ISMS) to systematically manage security risks.
- Continuous Improvement: Regular review and enhancement of security controls through risk assessments, vulnerability management, and third-party audits.

3. Website Security Measures

We have implemented stringent security measures to protect website visitors and their data:

- Data Encryption: All data transmitted between visitors and 308's website is secured using TLS 1.3 encryption, ensuring confidentiality and protection against interception.
- Secure Authentication & Access Controls: Role-based access and multifactor authentication (MFA) are enforced for all administrative access to our website backend.
- Proactive Threat Detection: Continuous monitoring, intrusion detection, and automated threat response mechanisms are in place.
- Website Integrity Assurance: Regular security audits, penetration testing, and vulnerability patching are conducted to prevent unauthorised access and exploitation.

- Content Security Policy (CSP): Preventing malicious script injections and clickjacking attacks.
- Strict Cookie & Privacy Policies: Transparent handling of visitor data, aligned with UK GDPR and international best practices.

4. Engagement & Data Protection Standards

To ensure a secure and trustworthy relationship between 308 and our stakeholders, we implement the following security measures:

- NDA/MNDA Policy:
  - Non-Disclosure Agreements (NDAs) and Mutual Non-Disclosure Agreements (MNDAs) are mandated early in engagements with potential partners, customers, or prospects.
  - NDAs/MNDAs are securely stored in an encrypted cloud drive, with a local air-gapped backup on a physically secured device.
- Access to Sensitive Information:
  - Sensitive business discussions and proprietary data sharing are conducted only through secure, vetted communication channels.
  - Requests for proprietary information are subject to verification and pre-approved security checks.
- Third-Party Risk Management:
  - All third-party vendors and service providers undergo cybersecurity risk assessments to ensure compliance with our security standards.
  - Vendor access to sensitive data is minimised and subject to stringent contractual and technical controls.

5. Incident Response & Reporting

We operate a comprehensive incident response framework to ensure rapid identification and mitigation of cybersecurity incidents:

- Automated Monitoring & Threat Notifications: 308 employs a plethora of security notifications to detect and respond to threats, overseen by our Chief Security Officer (CSO).
- Incident Reporting Protocols:
  - Visitors who suspect a security issue related to our website can report it to contact@308id.com
  - A dedicated Responsible Disclosure Policy encourages ethical reporting of vulnerabilities.
- Breach Notification Procedures: Should an incident affect visitor data, we comply with all UK GDPR notification obligations and will inform affected parties promptly.

6. Visitor Responsibilities & Secure Interaction Guidelines

To help us maintain a secure online environment, visitors should:

- Avoid sharing confidential or sensitive information via unencrypted email or unsecured channels.

- Verify the legitimacy of any requests for information claiming to be from 308 before responding.
- Use strong, unique passwords for accounts related to 308 services and enable MFA where applicable.
- Report any suspicious activity related to 308's website or communications.

7. Continuous Improvement & Contact Information

We continuously update and refine our cybersecurity policies in line with emerging threats, regulatory changes, and best practices. If you have any questions or require further information, please contact our cybersecurity team at ping@308.com.

By engaging with 308's website and digital services, you acknowledge our cybersecurity policy and agree to adhere to the security practices outlined above.

Version: 1.6 | Effective Date: 11/08/2026

308 One Pty Ltd
Level 1, 63-73 Ann Street
Surry Hills NSW 2010, Australia
Email: tap@into308.com
Phone: 1300 711 380