

Privacy Policy

1. Purpose

The purpose of this Privacy Policy is to outline how **Ultimate Security Australia Pty Ltd** ("Ultimate Security", "we", "us" or "our") collects, uses, stores, discloses and protects personal information in accordance with the **Privacy Act 1988 (Cth)** and the Australian Privacy Principles (APPs).

We are committed to managing personal information in an open and transparent way and to protecting the privacy and confidentiality of individuals, including employees, contractors, clients, suppliers, website visitors, event attendees and members of the public.

2. Scope

This policy applies to all personal information collected by Ultimate Security in connection with:

- Employment and recruitment;
- Contractor and subcontractor engagement;
- Client and supplier relationships;
- Security operations, including surveillance such as CCTV and body-worn cameras;
- Website or digital interactions;
- Website forms, enquiries and lead-generation activities;
- Trade events, exhibitions and other marketing activities;
- Email marketing and communications;
- Incident reporting and investigations; and
- Any other lawful business activity involving personal information.

This policy applies to all employees and representatives of the organisation.

3. Anonymity and Pseudonymity (APP 2)

Where lawful and practicable, individuals have the option of not identifying themselves or of using a pseudonym when dealing with us. However, in many cases, we may need to identify individuals to provide services or comply with legal obligations. We will inform individuals when identification is required.

4. Types of Personal Information Collected (APP 3)

We may collect the following types of personal information:

- Full name and contact details;
- Date of birth;
- Employment history and qualifications;
- Identification documents (e.g. driver's licence, passport);
- Right-to-work documentation;
- Payroll and banking details;
- Superannuation information;
- Emergency contact details;
- Criminal history or background check information, where required by law or consented to;
- Surveillance recordings, including CCTV and body-worn camera footage;
- Information provided through website enquiry and contact forms;
- Information provided when registering for or attending trade events, exhibitions and other marketing activities;
- Marketing and communication preferences;
- Information relating to enquiries, requests for information and business opportunities; and
- Any other information necessary for lawful business operations.

We only collect sensitive information, such as health, biometric or criminal record information, where required by law or with the individual's consent.

We only collect sensitive information (e.g. health, biometric, criminal record data) where required by law or with the individual's consent.

5. How Information is Collected (APP 3 & 4)

We collect personal information:

- Directly from individuals, including through forms, interviews, correspondence and website enquiries;
- Through recruitment and onboarding processes;
- From referees, background checks or government agencies, where authorised;
- From labour hire providers or subcontractors;
- Through surveillance systems, with appropriate signage and notices;
- Through business interactions and service delivery;
- Through our websites and online forms;
- Through HubSpot and other business, marketing and customer relationship management systems;
- At trade events, exhibitions, conferences and other marketing activities; and
- Through other lawful marketing and business activities.

We collect information by lawful and fair means. If we receive unsolicited personal information, we will assess whether we could have collected it under APP 3. If not, and it is lawful and reasonable to do so, we will destroy or de-identify the information as soon as practicable.

6. Notification of Collection (APP 5)

At or before the time we collect personal information (or as soon as practicable afterwards), we will take reasonable steps to notify individuals of:

- Our identity and contact details;
- The purpose of collection;
- Any third parties to whom we may disclose the information;
- Whether the information is required or authorised by law;
- The consequences of not providing the information;
- How individuals can access or correct their information; and
- How to make a complaint.

Where personal information is collected through our websites, online forms, events or marketing activities, relevant collection notices may also be provided at the point of collection.

7. Purpose of Collection and Use (APP 6)

We collect and use personal information for purposes including:

- Assessing job applications and verifying right to work;
- Managing employment, payroll and superannuation;
- Delivering security and related services;
- Managing client and supplier relationships;
- Responding to enquiries and business opportunities;
- Managing event and exhibition registrations and attendance;
- Providing information about our security services and solutions;
- Managing marketing communications and preferences;
- Ensuring workplace health and safety;
- Complying with legal and regulatory obligations; and
- Investigating incidents and managing risks.

We will only use or disclose personal information for the purpose for which it was collected (primary purpose), or for a related secondary purpose that individuals would reasonably expect, unless consent is provided or required by law.

8. Direct Marketing (APP 7)

We may use personal information for direct marketing purposes where permitted by the Privacy Act.

Our marketing communications may include information about:

- Security solutions and services;
- Events, exhibitions and conferences;
- Company updates and general marketing information; and
- Other products or services relevant to the individual's relationship or enquiries with us.

Where applicable, we will:

- Obtain consent where required before sending marketing communications;
- Provide a simple means to opt out of receiving further marketing;
- Comply with opt-out requests promptly and free of charge; and
- Inform individuals of the source of their personal information upon request, unless unreasonable or impracticable.

Individuals may also be provided with the ability to manage their communication preferences, including selecting or unsubscribing from relevant marketing categories.

9. Cookies and Similar Technologies

Our websites may use cookies and similar technologies to support website functionality, understand website usage, measure marketing activities and improve our digital services.

Technologies used across our websites may include:

- Google Tag Manager;
- Google Analytics 4;
- Google Ads and conversion/remarketing technologies;
- HubSpot;
- Webflow;
- Google Fonts; and
- Amazon CloudFront.

These technologies may collect information such as IP addresses, browser and device information, website activity, interactions and other usage information.

Non-essential analytics and advertising technologies may be activated when a visitor accesses our website. Individuals may manage or disable cookies and similar technologies through their browser or device settings, noting that doing so may affect website functionality.

10. Cross-Border Disclosure (APP 8)

We generally store personal information in Australia. However, certain website analytics, marketing, advertising and technology services may involve processing, access or disclosure of personal information outside Australia.

Our technology and service providers may include:

- HubSpot – CRM records are hosted in HubSpot's Sydney region; however, HubSpot analytics and usage data, support and security access, and certain sub-processors may involve processing outside Australia, including the United States;
- Google Analytics 4 – may process information through Google's United States and global infrastructure;
- Google Ads – may process information in countries where Google or its sub-processors operate facilities;
- Google Fonts – uses Google's global infrastructure;
- Webflow – may involve processing through infrastructure outside Australia; and
- Amazon CloudFront – uses global content delivery infrastructure.

Where personal information is disclosed to overseas recipients, we will take reasonable steps to ensure that the disclosure and handling of personal information is undertaken in accordance with applicable privacy obligations. Where practicable, we will inform individuals of relevant overseas recipients or countries.

11. Government Identifiers (APP 9)

We will not adopt, use or disclose government-related identifiers (e.g. Tax File Numbers, Medicare numbers, driver's licence numbers) as our own identifiers unless required or authorised by law.

12. Data Quality (APP 10)

We take reasonable steps to ensure that the personal information we collect, use or disclose is accurate, up to date, complete and relevant for the purposes for which it is collected. Individuals are encouraged to notify us of any changes to their personal information.

13. Storage and Security (APP 11)

We take reasonable steps to protect personal information from:

- Misuse, interference and loss; and
- Unauthorised access, modification or disclosure.

Security measures include:

- Secure electronic systems and encrypted storage;
- Password protection and access controls;
- Locked physical storage;
- Staff training in data protection; and
- Regular review of security practices.

When personal information is no longer required and retention is not legally required, we will securely destroy or de-identify it.

14. Access to Personal Information (APP 12)

Individuals may request access to their personal information by contacting our Privacy Officer. We will respond within a reasonable time and provide access unless an exception applies. If access is refused, we will provide written reasons and information on how to lodge a complaint.

15. Correction of Personal Information (APP 13)

Individuals may request correction of their personal information if it is inaccurate, out of date, incomplete, irrelevant or misleading. We will take reasonable steps to correct the information and notify any third parties where appropriate.

16. Data Breaches

In the event of a data breach involving personal information that is likely to result in serious harm, we will:

- Assess the nature and scope of the breach;
- Take immediate steps to contain the breach; and
- Notify affected individuals and the Office of the Australian Information Commissioner (OAIC) as required under the Notifiable Data Breaches (NDB) scheme.

17. Complaints

If you believe your privacy has been breached, you may lodge a complaint in writing to our Privacy Officer:

Privacy Officer

Ultimate Security Australia Pty Ltd

compliance@ultimatesecurity.com.au

+61 2 9311 1111

Level 2, 111 Parramatta Road, Concord, NSW 2137

We will investigate complaints promptly and confidentially. If you are not satisfied with our response, you may contact the OAIC.

Office of the Australian Information Commissioner (OAIC)

Website: www.oaic.gov.au

Phone: 1300 363 992

18. Responsibilities

All employees, contractors and representatives must:

- Handle personal information responsibly;
- Maintain confidentiality; and
- Comply with this policy and relevant legislation.

Breaches of this policy may result in disciplinary action.



Ying Loong Lee

Chief Operating Officer

28 September 2026