

Contents

1. PURPOSE AND INTRODUCTION	2
1.1 Introduction	2
1.2 Purpose	2
2. SCOPE	2
3. POLICY STATEMENT	3
4. WHAT IS PERSONAL INFORMATION AND SENSITIVE INFORMATION?	3
4.1 Personal Information	3
4.2 Sensitive Information	3
5. HANDLING PERSONAL INFORMATION	3
5.1 What Information Do We Collect?	3
5.2 How We Collect Personal Information	4
5.3 Why We Collect and Use Personal Information	5
5.4 When We Disclose Personal Information	5
6. ACCESS AND CORRECTION OF PERSONAL INFORMATION	7
7. REPORTING A DATA BREACH, LODGING A COMPLAINT OR SEEKING FURTHER INFORMATION	8
8. TRAINING AND AWARENESS	8
9. RESPONSIBILITIES	9
10. CONSEQUENCES OF NON-COMPLIANCE WITH THIS POLICY	9
11. RELATED POLICIES AND DOCUMENTS	10
12. POLICY REVIEW	10
13. DEFINITIONS AND INTERPRETATION	10
14. DOCUMENT HISTORY	11
15. APPROVAL	11

MSS SECURITY GROUP OF COMPANIES		Privacy Policy
---------------------------------------	--	----------------

1. PURPOSE AND INTRODUCTION

1.1 Introduction

The **MSS Security Group** recognises that protecting the privacy of individuals is fundamental to our role as a trusted provider of security, protective, medical, emergency, and corporate services. In the course of our operations, we handle a broad range of **Personal Information** relating to our **Personnel**, **Personnel** of our subcontractors, **Clients**, customers, and other stakeholders.

This policy outlines our commitment to managing Personal Information transparently, lawfully and ethically and forms part of our broader information governance and data protection framework. It reflects our legal obligations under the **Privacy Act** and the **Australian Privacy Principles** (APPs) and supports our intention to foster a culture of privacy awareness, accountability, and continuous improvement across the **MSS Security Group**.

(Note: Terms in **bold** with Capitalised first letters are defined in Section 13).

1.2 Purpose

The purpose of this policy is to

- articulate the **MSS Security Group's** commitment to the lawful and ethical handling of **Personal Information**;
- explain how we collect, hold, use and disclose **Personal Information**;
- support compliance with the **Privacy Act**, the **Australian Privacy Principles** and relevant contractual obligations;
- ensure consistent and accountable privacy practices across the organisation; and
- clarify the rights of individuals and the responsibilities of our **Personnel** when dealing with **Personal Information**.

2. SCOPE

This policy applies to:

- the MSS Security Group of Companies (referred to in this policy as the **MSS Security Group**) which includes MSS Security Pty Ltd (ABN 29 100 573 966), MSS Strategic Medical and Rescue Pty Ltd (ABN 48 155 387 152), Habitat Security Pty Ltd (ABN 48 610 045 189), and any related entities of these entities;
- all **Personnel** of the **MSS Security Group**, who handle or have access to **Personal Information** in the course of their work or duties; and

Approved: June 2025 Reviewed on: June 2025 Version: 3.0		Page 2 of 11
This document when printed is an UNCONTROLLED document.		

MSS SECURITY GROUP OF COMPANIES		Privacy Policy
---------------------------------------	--	----------------

- any other individuals whose **Personal Information** is collected, held, or managed by the **MSS Security Group**, including **Clients**, customers, contractors, suppliers, and members of the public.

3. POLICY STATEMENT

The **MSS Security Group** is committed to safeguarding **Personal Information** through a culture of integrity, compliance, and continuous improvement. We recognise that privacy is not only a legal requirement, but also a reflection of our values and the expectations of those we serve.

This policy sets a clear standard for how we manage **Personal Information** across all parts of our organisation. It forms part of our broader information governance and risk management approach and is supported by practical controls, training, and leadership accountability.

To achieve this, we will:

- comply with our obligations under the **Privacy Act** and the **Australian Privacy Principles**;
- investigate concerns about our collection, use, storage or disclosure of **Personal Information**; and
- take appropriate action where **Personal Information** is not handled properly.

4. WHAT IS PERSONAL INFORMATION AND SENSITIVE INFORMATION?

4.1 Personal Information

Personal Information means Information or an opinion (whether true or not, and whether recorded in material form or not) about an identified individual, or an individual who is reasonably identifiable. This includes names, contact details, identification numbers, employment data, and any other information defined as personal information under the **Privacy Act**.

4.2 Sensitive Information

Sensitive Information is a subset of **Personal Information** that is afforded additional protections under the **Privacy Act** due to its potentially harmful or intrusive nature. It includes information or opinions about an individual's racial or ethnic origin, political opinions or memberships, religious or philosophical beliefs, trade union or professional memberships, sexual orientation or practices, criminal record, health or disability information, and genetic or biometric data.

5. HANDLING PERSONAL INFORMATION

5.1 What Information Do We Collect?

Approved: June 2025 Reviewed on: June 2025 Version: 3.0		Page 3 of 11
This document when printed is an UNCONTROLLED document.		

The **MSS Security Group** collects **Personal Information** where necessary to operate our business, meet contractual, legal and regulatory obligations, and deliver security, emergency, medical and support services. Although we primarily engage with corporate and government clients, we collect **Personal Information** from individuals in the following contexts:

- subcontractor **Personnel** and sole traders – such as their names, contact details, security licence numbers, qualifications, identification documents, proof of right to work, emergency contacts, and the results of security or compliance checks (such as police, criminal, and working with children checks);
- **Client** and supplier representatives – including names, roles, and business contact information such as email addresses and phone numbers;
- visitors to our sites or client locations, including access records, sign-in logs, and surveillance footage (such as CCTV); and
- individuals interacting with our websites or portals – limited information collected via **Cookies** and analytics tools.

In the context of our medical and emergency services operations, we may also collect health or other Sensitive Information, including:

- medical history or incident-related health data (for example, in connection with workplace injuries, emergency response, or medical services);
- fitness for duty or vaccination records (for example, for remote or high-risk sites); and
- Information necessary to provide care or comply with occupational health and safety obligations.

Where required, we may also collect **Sensitive Information** for security vetting or licensing purposes (such as criminal record checks). Such information is collected only where lawful and reasonably necessary and is subject to additional protections.

We also collect **Personal Information** from our own employees and job applicants. Where this information relates directly to the employment relationship, it is generally exempt from the **Privacy Act** and managed in accordance with applicable workplace laws.

5.2 How We Collect Personal Information

We collect **Personal Information** through lawful and fair means, including:

- directly from individuals (for example subcontractors and their employees, site visitors, medical service recipients, job applicants);
- from recruitment firms, service providers or **Clients**, or government agencies;

- from access control and security systems, such as CCTV and sign-in platforms;
- through onboarding or compliance processes (for example, licence validation or work health declarations); and
- from our websites or systems, including **Cookies** or analytics tools.

This policy outlines the circumstances in which we collect **Personal Information** and how it is handled. Where required or appropriate, we may also provide additional notices at the time of collection to supplement this policy.

If we receive unsolicited **Personal Information** that we are not permitted to retain, we will take reasonable steps to destroy or de-identify it in accordance with the **Privacy Act**.

5.3 Why We Collect and Use Personal Information

We collect and use **Personal Information** to:

- engage, screen, and manage subcontractors, sole traders, and consultants;
- deliver our contracted security, emergency response, and medical services;
- maintain records of licensing, clearances, training, and access compliance;
- manage operational relationships with **Clients** and suppliers;
- monitor and control access to secure or high-risk sites;
- investigate incidents, manage safety and compliance obligations, and resolve complaints; and
- comply with relevant laws, regulations, and **Client** contractual requirements.

In the course of providing medical and emergency services, we may collect health-related information in order to provide appropriate care, assess fitness for duty, or meet work health and safety and regulatory obligations.

We do not use **Personal Information** for direct marketing purposes.

5.4 When We Disclose Personal Information

We may disclose **Personal Information** to third parties where reasonably necessary to support our operations, comply with legal obligations, or fulfil contractual requirements. This may include:

- other **MSS Security Group** entities, where operationally required;

- **Clients** or site controllers (for example for onboarding, clearances, incident reporting or access purposes);
- third-party service providers, including background screening providers, training organisations, payroll processors, IT service providers, and legal or regulatory advisers; and
- government bodies, law enforcement agencies, emergency services, or regulators, where authorised or required by law.

We do not sell **Personal Information** under any circumstances. We will never provide **Personal Information** to third parties for marketing or unrelated commercial purposes.

Where we disclose **Personal Information** to third parties, we take reasonable steps to ensure those parties handle it in accordance with the **Privacy Act** and this policy.

5.5 How We Protect and Store Personal Information

The **MSS Security Group** takes reasonable steps to protect **Personal Information** from misuse, interference, loss, unauthorised access, modification, or disclosure. We implement a range of physical, technical, and administrative safeguards to maintain the confidentiality, integrity, and availability of **Personal Information** we hold.

We store **Personal Information** in both paper-based and electronic formats, including in systems hosted at secure data centres. We take reasonable steps to ensure that those data centres store **Personal Information** in Australia.

Access to **Personal Information** is limited to those who require it to carry out legitimate business functions. Physical records are held at secure **MSS Security Group** premises with controlled access. Electronic data is protected by system access controls and other safeguards.

We provide training to our **Personnel** on their privacy obligations and take appropriate action to address any potential or actual misuse of **Personal Information**.

We retain **Personal Information** only for as long as necessary to fulfil the purpose for which it was collected, or as required by law. When no longer required, we securely destroy or de-identify **Personal Information** in accordance with internal procedures and legal obligations.

5.6 Use of Cookies and Website Analytics

A **Cookie** is a small text file placed on a user's device when visiting a website. **Cookies** help websites recognise the device and store information about preferences or previous activity. **Cookies** themselves do not directly identify individuals but can associate limited technical data with a specific device.

When a user visits our websites or social media pages and consents to the use of **Cookies**, a **Cookie** is saved to their device. These **Cookies** may collect information such as:

- Internet Protocol (IP) addresses;
- browser type and device characteristics;
- pages visited and time spent on the site;
- referring website addresses;
- application activity logs and error logs.

This information helps the **MSS Security Group** understand how users interact with its website, identify peak usage periods, and improve navigation, content, and functionality.

Users may choose to disable **Cookies** by adjusting their browser settings. However, disabling **Cookies** may affect their ability to access certain features or services on the website.

The **MSS Security Group** may also use analytics tools (such as Google Analytics) that rely on **Cookies** to track usage patterns and generate reports. These tools collect non-identifiable information and do not allow the **MSS Security Group** to identify individual users. Further information is available at: <https://policies.google.com/technologies/partner-sites>

The **MSS Security Group** does not use **Cookies** for advertising, profiling, or automated decision-making and does not use **Cookie** data to identify individuals.

6. ACCESS AND CORRECTION OF PERSONAL INFORMATION

Individuals may contact the **MSS Security Group** to access the **Personal Information** it holds about them or to request that it be corrected. The **MSS Security Group** will take reasonable steps to assist with such requests in accordance with the **Privacy Act** and the **Australian Privacy Principles**.

An individual may:

- request access to their **Personal Information**, subject to verification of identity and any applicable legal exemptions;
- request correction if their **Personal Information** is inaccurate, incomplete, out-of-date, irrelevant, or misleading;
- request deletion of **Personal Information** where it is no longer required and the **MSS Security Group** is not legally required to retain it; and
- be provided with written reasons if access or correction is refused, along with information about how to lodge a complaint.

Requests should be submitted to privacy@msssecurity.com.au. The **MSS Security Group** may require identification to verify the request.

MSS SECURITY GROUP OF COMPANIES		
		Privacy Policy

The **MSS Security Group** does not charge a fee to make a request. However, a reasonable administrative fee may be charged where providing access requires significant time or resources.

The **MSS Security Group** aims to respond to all access and correction requests within 30 days of receipt.

7. REPORTING A DATA BREACH, LODGING A COMPLAINT OR SEEKING FURTHER INFORMATION

The **MSS Security Group** encourages individuals to raise concerns or seek clarification regarding how their **Personal Information** is handled. Individuals may contact the **MSS Security Group** in relation to any of the following:

- to report a suspected data breach, including unauthorised access, disclosure, or loss of **Personal Information**;
- to lodge a privacy complaint about how **Personal Information** has been collected, used, stored, or disclosed;
- to request an update or correction to previously provided **Personal Information**; and
- to seek further information about this policy or the MSS Security Group's privacy practices.

Enquiries should be directed by email to privacy@msssecurity.com.au.

Individuals may choose to remain anonymous or use a pseudonym when making a report or enquiry. However, this may limit the **MSS Security Group's** ability to respond or investigate the matter fully.

The **MSS Security Group** will aim to respond within 30 days of receiving a complaint or request.

If an individual is not satisfied with the response, they may contact the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au to lodge a complaint.

8. TRAINING AND AWARENESS

The **MSS Security Group** supports a culture of privacy awareness and provides guidance to Personnel to help them understand their obligations when handling **Personal Information**. Where appropriate, the **MSS Security Group** provides training and awareness activities to support compliance with this policy. These may include:

- mandatory privacy training for new starters especially if their roles involve regular access to **Personal Information**;

Approved: June 2025 Reviewed on: June 2025 Version: 3.0		Page 8 of 11
This document when printed is an UNCONTROLLED document.		

MSS SECURITY GROUP OF COMPANIES		
		Privacy Policy

- targeted training following a change in role where the individual's responsibilities include handling **Personal Information**;
- privacy-related communications or updates in response to policy changes, new legal obligations, or identified risks; and
- support and coaching following incidents, audits or complaints;

Personnel who regularly handle **Personal Information** are expected to understand and apply the principles set out in this policy. Additional support is available from the **MSS Security Group** Privacy Officer or relevant specialist teams where clarification is required.

9. RESPONSIBILITIES

The **MSS Security Group** assigns responsibility for privacy compliance across different levels of the organisation to ensure that **Personal Information** is handled appropriately:

- **Directors and Senior Leadership Personnel** are responsible for promoting a culture of privacy awareness and supporting governance and oversight of privacy obligations.
- **Specialist and Support Functions**, including Legal, IT and People and Culture teams, and the Privacy Officer, provide advice, training, and systems support to manage privacy risks and compliance.
- **Managers and Supervisors** are expected to support their teams in understanding and applying this policy and to escalate any concerns or breaches.
- **All Personnel** are responsible for handling **Personal Information** in accordance with this policy and for completing any training relevant to their role.

10. CONSEQUENCES OF NON-COMPLIANCE WITH THIS POLICY

The **MSS Security Group** takes compliance with this policy seriously. Any breach of this policy may result in disciplinary action, which may include:

- coaching or informal counselling;
- formal warnings;
- suspension or termination of employment or engagement; or
- referral to regulatory or enforcement authorities, where appropriate.

All breaches or suspected breaches will be investigated in accordance with the **MSS Security Group's** applicable disciplinary and grievance procedures, and in line with the principles of procedural fairness.

Approved: June 2025 Reviewed on: June 2025 Version: 3.0		Page 9 of 11
This document when printed is an UNCONTROLLED document.		

MSS SECURITY GROUP OF COMPANIES		Privacy Policy
---------------------------------------	--	----------------

11. RELATED POLICIES AND DOCUMENTS

This policy should be read in conjunction with related policies, procedures and protocols which are available on the **MSS Security Group** Intranet. These include:

- Acceptable Use of Information Technology Policy;
- Artificial Intelligence Policy;
- Corporate Social Responsibility Statement;
- Data Retention Policy;
- Employee Code of Ethics (set out in the Employee Standing Instructions);
- Grievance Policy;
- Information Handling and Classification Policy;
- Information Security Policy; and
- Information Security Incident Response Policy.

12. POLICY REVIEW

The **MSS Security Group** will periodically review this policy and update it as relevant and necessary to ensure it remains effective and appropriate.

13. DEFINITIONS AND INTERPRETATION

In this policy, unless the context otherwise required:

Australian Privacy Principles (APP) means the binding principles set out in Schedule 1 of the **Privacy Act**; they regulate how most Australian public and private sector organisations, including the **MSS Security Group**, must handle **Personal Information** covering its collection, use, disclosure, storage, and access;

Client means any external organisation or individual that engages **MSS Security Group** to provide services under a contract, agreement, or other commercial arrangement;

Cookies are as defined in section 5.6 of this policy;

MSS Security Group is as defined in section 2 of this policy;

Personal Information is as defined in section 4.1 of this policy;

Personnel includes the officers, employees, agents, contractors and authorised third parties of an entity;

Approved: June 2025 Reviewed on: June 2025 Version: 3.0		Page 10 of 11
This document when printed is an UNCONTROLLED document.		

MSS SECURITY GROUP OF COMPANIES		
		Privacy Policy

Privacy Act means the *Privacy Act 1988* (Cth); and

Sensitive Information is as defined in section 4.2 of this policy.

14. DOCUMENT HISTORY

Version	Date	Author	Reason
1.0	Unspecified	Legal Department	Implementation of policy
2.0	March 2014	Legal Department	Updated to comply with new legislation
3.0	June 2025	Legal Department	Legal review and update

15. APPROVAL

Date	Name	Position	Signature
June 2025	Geoff Alcock	Managing Director	