Document ID: SS-SEC-POL-001

Document Title: Defence Security Policy

Version: 1.0

Status: Approved

Date: 12 August 2025

Parent Document: SS-CORP-PLAN-001 Corporate Plan 2025-2028

1. Introduction

1.1 Purpose

This Defence Security Policy establishes the overarching security framework, principles, and governance for Synthetic Systems. Its purpose is to protect the company's people, information, and assets from a range of security threats, ensuring we meet our contractual, legal, and ethical obligations as a trusted partner in Australia's defence industry. This policy provides the foundation for a resilient and security-conscious culture that enables our business objectives and supports national security interests.

1.2 Scope

This policy and its supporting procedures apply to all Synthetic Systems personnel, including permanent employees, temporary staff, contractors, consultants, and third-party vendors who access company information or assets. It covers all business activities, company-owned or managed facilities, and information technology (IT) and operational technology (OT) systems. Compliance with this policy is mandatory for all individuals and entities within its scope.

1.3 Policy Statement

Synthetic Systems is unequivocally committed to implementing and maintaining a comprehensive security framework that aligns with the Australian Government's Defence Security Principles Framework (DSPF). We will foster a proactive security culture where every individual understands their role in safeguarding our capabilities. Our approach to security will be risk-based, integrated into all aspects of our business, and continuously improved to counter evolving threats. The implementation of this policy is a key enabler of our corporate strategy, directly supporting our ability to deliver secure and resilient communication solutions to the Australian Defence

Force and our allies.

2. Security Principles

Synthetic Systems adopts the Australian Government's Defence Security Principles to guide its security planning, decision-making, and culture.

- **Principle 1: Security is everyone's responsibility.** We will ensure all personnel are aware of their security obligations and are empowered to identify and report security concerns without fear of reprisal. Security is a collective effort integral to our daily operations.
- **Principle 2: Security risk management is essential.** We will systematically identify, assess, and treat security risks to our people, information, and assets. Our risk management processes will be integrated into our corporate governance and business planning to ensure decisions are risk-informed.
- **Principle 3: Security measures must be proportionate to the risks.** We will implement security controls that are commensurate with the value of the assets we are protecting and the level of threat. We will avoid measures that are excessive or unduly impede our core business of innovation and delivery.
- **Principle 4: Information is secured based on its classification and business criticality.** We will apply robust controls to protect the confidentiality, integrity, and availability of all information, with specific measures applied to sensitive and classified data in accordance with government and contractual requirements. The "Need-to-Know" principle will be strictly enforced.
- **Principle 5: Physical security measures will protect our people and assets.** We will maintain a secure and controlled physical environment for our facilities, preventing unauthorised access, damage, or interference to company assets and Defence projects.
- **Principle 6: Personnel security measures will establish and maintain a trusted workforce.** We will implement rigorous pre-employment screening, ongoing vetting, and security awareness training to ensure our personnel are suitable to hold positions of trust and to access sensitive or classified information.
- **Principle 7: Cyber security measures will defend against and respond to cyber threats.** We will maintain a robust cyber security posture to protect our digital infrastructure and information from compromise, ensuring the resilience of the systems that underpin our product suite and corporate functions.

3. Governance and Accountability

3.1 Defence Security Committee (DSC)

The Defence Security Committee (DSC) is hereby formally established as the primary governance body for security matters within Synthetic Systems. The DSC is chartered by the CEO and has the full authority to oversee the implementation and continuous improvement of the company's security program in line with this policy.

3.1.1 Authority and Mandate

The DSC is authorised by the CEO to:

- Endorse all subordinate security policies, standards, and procedures.
- Oversee the company-wide security risk management program.
- Approve and monitor the allocation of resources for security initiatives.
- Direct the investigation of and response to major security incidents.
- Review and report on the company's security performance to the CEO and the Executive team.

3.1.2 Composition and Meetings

The DSC will be chaired by the Head of Operations. Core members will include representatives from Information Technology, Human Resources, and Engineering. The committee will meet quarterly, or more frequently if required by emerging security matters.

3.2 Key Security Roles

- **Chief Executive Officer (CEO):** The CEO holds ultimate accountability for security within Synthetic Systems and for the successful execution of the Corporate Plan.
- **Head of Operations:** As Chair of the DSC, the Head of Operations is responsible for the operational implementation of this policy and its supporting frameworks.
- **Managers and Team Leaders:** Are responsible for ensuring this policy is implemented within their respective teams and for fostering a positive security culture.
- **All Personnel:** Are responsible for understanding and complying with this policy and reporting all security incidents and concerns.

4. Key Security Programs

4.1 Information Security Management System (ISMS)

In direct support of this policy, and as a primary corporate objective outlined in the *SS-CORP-PLAN-001 Corporate Plan 2025-2028*, Synthetic Systems is committed to developing and maintaining an Information Security Management System (ISMS).

A key strategic driver for the implementation of this policy is the company's goal to achieve **ISO 27001 certification**. This initiative, overseen by the Head of Operations through the Defence Security Committee (DSC), is critical for demonstrating our commitment to protecting sensitive information and is a prerequisite for deeper integration into the defence supply chain. The ISMS will govern all aspects of information security, including classification, handling, storage, and disposal of sensitive and classified data.

4.2 Personnel Security

Synthetic Systems will implement a personnel security program that meets the requirements of the Defence Industry Security Program (DISP). This includes:

- Pre-employment screening and police checks for all new hires.
- Facilitating and managing Australian Government Security Vetting Agency (AGSVA) clearances for eligible staff.
- Mandatory security induction and annual refresher training for all personnel.
- Formal processes for managing security during employee onboarding, role changes, and separation.

4.3 Physical Security

We will ensure our facilities are protected by a layered security model, including:

- Access control systems to restrict entry to authorised personnel.
- Alarm systems and surveillance to monitor and respond to unauthorised access.
- Secure zones for the handling and storage of classified information and sensitive project hardware.
- Visitor management and escort procedures.

4.4 Cyber Security

Our cyber security program will align with recognised standards such as the Australian Signals Directorate's (ASD) Essential Eight. The program will focus on:

- Network security and segregation.
- Endpoint protection for all servers and workstations.
- A robust incident response plan to detect, contain, and eradicate cyber threats.
- Regular vulnerability assessments and penetration testing.

5. Policy Compliance and Review

Compliance with this policy is a condition of employment for all personnel. Non-compliance may result in disciplinary action, up to and including termination of employment or contract.

The Defence Security Committee (DSC) will review this policy biennially, or in response to significant changes in the company's risk environment, strategic direction, or relevant government security requirements.

6. Related Documents

- SS-CORP-PLAN-001 Corporate Plan 2025-2028