Document ID: SS-SEC-PROC-001

Document Title: Classified Document Handling Procedure

Version: 1.0

Status: Approved

Date: 12 August 2025

Parent Document: SS-SEC-POL-001 Defence Security Policy

1. Introduction

1.1 Purpose

This document provides detailed, mandatory procedures for the handling of classified and sensitive information at Synthetic Systems. The purpose is to ensure that all such information is correctly marked, stored, transmitted, and destroyed in a manner that protects its confidentiality, integrity, and availability. These procedures are critical to meeting our contractual and national security obligations.

1.2 Scope

This procedure applies to all Synthetic Systems personnel (employees and contractors) who generate, receive, or handle information classified as OFFICIAL, PROTECTED, or SECRET, in both electronic and physical formats. It is a subordinate procedure to the overarching *SS-SEC-POL-001 Defence Security Policy*.

1.3 Principles

The following core principles, derived from *SS-SEC-POL-001*, govern the handling of all classified information:

- **Need-to-Know:** Access to classified information is strictly limited to personnel whose duties require such access.
- **Individual Responsibility:** Every person handling classified information is personally responsible for safeguarding it.
- **Proportionality:** Security measures applied will be proportionate to the classification level of the information.

2. Information Classification and Marking

Correctly marking documents is the first step in ensuring they receive the appropriate level of protection. All documents created or received by Synthetic Systems must be

assessed and marked according to the Australian Government's security classification system.

2.1 Marking Requirements

Markings must be clearly visible. For physical documents, markings shall be in uppercase, bold text, and placed at the top and bottom center of every page.

- **OFFICIAL:**
  - **Description:** Used for the majority of government business information. The compromise of this information could cause limited damage to national interests, organisations, or individuals.
  - **Marking: OFFICIAL**
  - **Additional Markings:** May include dissemination limiting markers (DLMs) such as **SENSITIVE** or **SENSITIVE:LEGAL**.
- **PROTECTED:**
  - **Description:** Used for information that, if compromised, could cause serious damage to national interests, organisations, or individuals. This includes information related to defence capabilities, intelligence, or law enforcement.
  - **Marking: PROTECTED**
  - **Header/Footer:** Every page must be marked **PROTECTED** at the top and bottom.
  - **Cover Sheet:** A blue **PROTECTED** cover sheet must be used for physical documents when not in a secure container.
  - **Watermark:** Electronic documents should have a "PROTECTED" watermark applied where technically feasible.
- **SECRET:**
  - **Description:** Used for information that, if compromised, could cause exceptionally grave damage to the national interest. This is the highest classification level handled at Synthetic Systems.
  - **Marking: SECRET**
  - **Header/Footer:** Every page must be marked **SECRET** at the top and bottom.
  - **Cover Sheet:** A red **SECRET** cover sheet must be used for physical documents when not in a secure container.
  - **Copy and Page Numbering:** Each copy of a SECRET document must be numbered, and each page must be marked with its page number and the total number of pages (e.g., Page 3 of 15).
  - **Register:** All SECRET documents must be recorded in the company's central SECRET Document Register, managed by the Company Security Officer.

3. Storage and Handling

Secure storage is paramount to preventing unauthorised access. The level of protection must match the classification.

3.1 Storage of Physical Documents

- **OFFICIAL:** Documents should be stored in locked cabinets or drawers when not in use, particularly if they contain sensitive information. Clean desk practices are encouraged.
- **PROTECTED:** Must be stored in a Class C secure container approved by the Security Construction and Equipment Committee (SCEC). The container must be located within a secure area with controlled access. Combination locks must be changed annually or when a person with knowledge of the combination departs the company.
- **SECRET:** Must be stored in a Class B secure container (or higher) approved by SCEC. The container must be located within a designated secure zone with stringent access controls. Two-person integrity checks are required for accessing and securing SECRET material where practical.

3.2 Storage of Electronic Information

- **General Requirement:** All classified electronic information must be stored on company-approved IT systems that have been accredited to hold information up to the required classification level.
- **Networks:** As mandated by the Defence Security Committee (DSC) in *SS-SEC-POL-001*, classified information must only be stored and processed on networks accredited for that classification level. SECRET material must be stored on a dedicated, air-gapped network.
- **Removable Media:** USB drives, hard drives, or other removable media used for classified information must be marked with the highest classification of the data they contain and stored in a secure container appropriate for that level.

4. Transmission and Transportation

4.1 Electronic Transmission

- **Prohibition:** The transmission of any classified information (PROTECTED or SECRET) over unapproved networks, including the public internet or internal corporate email systems not accredited for that level, is strictly prohibited. This is a critical directive from the Defence Security Committee (DSC) referenced in *SS-SEC-POL-001*.
- **Approved Methods:**
    - **PROTECTED:** Can be transmitted using Defence-approved encrypted networks or using an approved cryptographic device (e.g., a secure fax or IP

encryptor).
    - **SECRET:** Can only be transmitted over networks specifically accredited to the SECRET level.

4.2 Physical Transmission

- **Internal:** When carried within Synthetic Systems facilities, classified documents must be concealed in an appropriately marked folder or envelope.
- **External (Australia):**
    - **PROTECTED:** Must be double-enveloped. The inner envelope must be marked with the classification. The outer envelope should show no classification marking but must be addressed to a specific, authorised individual. It must be sent via a registered courier service with tracking.
    - **SECRET:** Must be transported by authorised personnel with the appropriate security clearance, using a Defence-approved courier service or escorted by cleared staff. A transit note must be completed and logged in the SECRET Document Register.

5. Destruction

When classified information is no longer required, it must be destroyed in a manner that makes reconstruction impossible.

5.1 Approved Destruction Methods

- **Paper-based Products:**
    - **OFFICIAL:** Can be destroyed using a standard office cross-cut shredder.
    - **PROTECTED/SECRET:** Must be destroyed using a SCEC-approved Class A or Class B shredder. The destruction of SECRET material must be witnessed by a second cleared person and recorded in the SECRET Document Register.
- **Electronic Media:**
    - Hard drives, USB sticks, and other media must be destroyed using a SCEC-approved degausser or physical destruction device. Simply deleting files is insufficient. All electronic media destruction must be formally recorded.

6. Incident Reporting

Any suspected or actual compromise of classified information, including loss, theft, or unauthorised disclosure, must be reported immediately to the Company Security Officer. Failure to report a security incident is a serious breach of company policy.