Document ID: SS-SITE-SEC-PROC-001

Document Title: Site Security Procedure

Version: 1.0

Status: Approved

Date: 12 August 2025

1. Introduction

1.1 Purpose

The purpose of this document is to define the procedures for maintaining the physical security of all Synthetic Systems facilities. These procedures are designed to protect personnel, prevent unauthorized access, and safeguard company and customer assets in accordance with the principles established in the *SS-SEC-POL-001 Defence Security Policy*.

1.2 Scope

This procedure applies to all Synthetic Systems personnel (employees and contractors), visitors, and assets located at company facilities. It covers access control, vehicle management, and security checks.

2. References

- **SS-SEC-POL-001:** Defence Security Policy

3. Access Control

3.1 General Access

All personnel must wear their company-issued access control card (ACC) and photo identification visibly at all times while on site. Access to the facility is restricted to authorized personnel and officially escorted visitors only. Tailgating through access-controlled doors is strictly prohibited.

3.2 Secure Zones

Access to designated Secure Zones (e.g., server rooms, development labs, classified storage areas) is strictly limited by specific access permissions programmed onto an individual's ACC. Access is granted based on the principle of "Need-to-Know" and requires formal approval from the relevant asset owner or department head.

4. Vehicle Access and Parking

4.1 Personal Vehicles

Personnel may park their personal vehicles in the general parking area. For security purposes, all vehicles are subject to search upon entering or leaving company premises. Synthetic Systems assumes no liability for theft or damage to personal vehicles parked on site. Personnel must not leave their company-issued ACC or other security items visible within their parked vehicle.

4.2 Company Vehicles

Company vehicles must be parked in the designated fleet parking area. The keys for all company vehicles must be logged and stored in the secure key press located at reception when not in use.

4.3 Deliveries and Commercial Vehicles

All delivery and commercial vehicles must report to the designated receiving area. Drivers must remain with their vehicles unless escorted by a member of Synthetic Systems staff. Unscheduled deliveries will be refused entry.

5. End-of-Day Security Checks and Lock-Up

A comprehensive security check of the facility must be conducted at the close of business each day. The last person to leave a department or work area is responsible for ensuring that area is secure.

5.1 Lock-Up Checklist

The designated closing personnel or security guard must complete the following checks:

- **Windows and Doors:** Confirm all external windows and doors are closed and securely locked.
- **Secure Containers:** Verify that all safes, security containers, and classified document cabinets are locked.
- **Clear Desk Policy:** Ensure all desks are clear of sensitive or classified information. Any unsecured sensitive materials must be secured in an appropriate container.
- **Equipment:** Power down all non-essential electronic equipment.
- **Alarm System:** Arm the building's security alarm system.

5.2 Closing Register

Upon completion of the lock-up checklist, the designated closer must sign and date the End-of-Day Closing Register located at the main reception desk.

6. Security Incident Reporting

The timely reporting of security incidents is critical to maintaining a secure environment.

6.1 What to Report

A physical security incident is any event that has compromised, or has the potential to compromise, the security of the facility or the safety of personnel. Examples include, but are not limited to:

- A lost or stolen access control card (ACC).
- Discovery of an unlocked external door or window after hours.
- Sighting of an unauthorized or unescorted person within the facility.
- Evidence of forced entry or tampering with security hardware.
- Any act of theft or vandalism.

6.2 Immediate Actions

In the event of an active or life-threatening situation, personnel should immediately contact emergency services (000).

6.3 Reporting Procedure

All non-emergency physical security incidents must be reported immediately to the Head of Operations.

The Head of Operations is responsible for conducting an initial assessment of the incident and, if deemed necessary, formally reporting the incident to the **Defence Security Committee (DSC)**. As established in SS-SEC-POL-001, the DSC is the primary governance body for security matters and will direct the formal investigation and response to all significant security incidents. The report to the DSC must be made within 24 hours of the incident's discovery.

7. Document Control

This is a controlled document. The official version is maintained by the Head of Operations. Any printed copies are considered uncontrolled. This document shall be reviewed biennially or as required by changes to the parent policy.