Introduction and background

The **DC GEOMATICS** RPAS security processes and procedures, as required under the South African Civil Aviation Regulations, Part 101, are applicable to remotely piloted aircraft systems (RPAS) within civil aviation operations. The measures contained herein are approved security measures to be followed by all personnel involved in RPAS operations and of RPAS under **DC GEOMATICS** operational control and the secure storage thereof.

The main objective of the DC Geomatics Security manual is to ensure the protection of the RPAS from unlawful interference through the application of security controls laid down in Part 101 of the South African Civil Aviation Regulations, 2011 as well as its associated Technical Standards (SA-CATS-101).

Premises, staff and access control and control of permits

- Considering the size and capability of the RPAS, adequate physical barriers, such as fences, security gates and doors shall be installed to protect the RPA and Remote Pilot Station from an act of unlawful interference.

- Physical barriers shall be of such nature that unauthorised access will be detected and prevented. This will include the following:
- All RPAS Storage unit/s and areas shall be closed and locked or guarded when not in use.
- All RPAS Storage unit/s and areas shall be equipped with intrusion detection devices. Where intrusion detection devises are not installed other means of protection against intrusion shall be used.
- Access to RPAS Storage unit/s and areas shall be restricted to authorized persons with an operational need.
- Access control shall be exercised at specific access control points, there being no other means of access into the premises other than through that point or points.
- Each access control point shall be staffed, or effectively monitored or secured.
- The outer perimeter shall be clearly defined through physical barriers.
- The inner perimeter shall be clearly defined through physical barriers.
- Staff authorized to have unescorted access to controlled areas shall be issued with passes/permits.
- Visitors shall at all times be escorted if required to enter RPAS Storage areas.
- A permit control process shall be implemented to approve and control the issuance, use and recovery of passes/permits.

Visitors

- The identity of visitors shall be recorded and where visitors are required to enter security sensitive areas such as RPAS Storage areas, such visitor will always remain under escort by an authorised representative.

- Visitors requiring access to RPAS Storage areas shall, commensurate with the level of threat, be subject to search as to prevent the introduction of explosives, incendiary devices or any other prohibited or harmful articles which may be used to commit acts of unlawful interference.

- Parcels, bags or containers brought into security-controlled areas by visitors shall either be prevented from taking such parcels, bags, containers into security-controlled areas or such items shall be accounted for on exit.

Unauthorised Access

- Where an unauthorised person has gained access to an RPAS Storage unit/s and/or area, such RPAS Storage unit/s and area shall be viewed as being unsecure. In this event such RPAS Storage unit/s and area shall first be subjected to appropriate security controls including a security search prior to be deemed as secure.
- In any event of unauthorised access to an RPAS Storage unit/s and/or area, appropriate steps shall be taken without delay to prevent further breaches to the security system.
- Where an unauthorised person is detected in an RPAS Storage area the following actions shall be taken:
- The person should be challenged. If it is regarded as not safe, the assistance of the security personnel and/or police must be sought.
- The identity of the person should be established.
- The applicable area of the RPAS Storage unit/s and/or area shall be regarded as contaminated/unsecured.
- The area, including all products/articles stored in the area shall be subjected to security controls (which may include a thorough search/inspection) as to confirm that the RPA and Remote Pilot Station stored in that area is secure.
- The SACAA shall be notified of the incident within 48 hours.

Electronic Security Systems

- Intruder detection systems shall be tested at least once every 30 days. Where Passive detectors are installed, such detectors should regularly be inspected for signs of tampering or damage. The inspection should further include verifying that the coverage areas of Passive detectors are not obstructed.
- Where security lights are installed, such lights should regularly be inspected for operation, signs of tampering or damage. The inspection should further include verifying that the coverage areas of security lights are not obstructed.

I the undersigned hereby accept the assignment as responsible person for the satellite station.

Signed at Worcester on this 05 day of June the year 2025

Satellite station name: Techno Survey Solutions cc

Responsible person: Rudy van Breda

Signature: _____