Evidence Management Policy

Purpose:

This policy outlines the procedures for the collection, handling, storage, and presentation of evidence in a lawful, ethical, and professional manner. Our goal is to ensure the integrity and admissibility of evidence collected during investigations and compliance with applicable laws in Victoria, Australia.

---

1. Scope

This policy applies to all employees, contractors, and agents of **Night Hawk Intelligence** involved in the collection, management, and use of evidence during investigations.

---

2. Legal Compliance

All evidence must be collected, handled, and presented in accordance with:

- The *Evidence Act 2008 (Vic)*
- The *Surveillance Devices Act 1999 (Vic)*
- The *Privacy Act 1988 (Cth)* and Australian Privacy Principles (APPs)
- Any other applicable Commonwealth or state laws

Failure to comply with these laws may result in evidence being inadmissible in court or penalties for unlawful practices.

---

3. Collection of Evidence

3.1 Lawful Methods

Evidence must be collected lawfully, ensuring compliance with the *Surveillance Devices Act 1999 (Vic)*. This includes:

- Obtaining proper consent where required.
- Using surveillance devices (e.g., cameras, audio recording devices) only in accordance with the law.
- Avoiding actions that could constitute trespass or breach of confidence.

3.2 Ethical Practices

- Evidence must not be fabricated, altered, or obtained through deceitful or illegal means.
- Investigators must act professionally and respect the privacy and rights of individuals during evidence collection.

3.3 Chain of Custody

To maintain the integrity of evidence, a clear chain of custody must be established and documented. This includes:

- Recording when, where, and how evidence was obtained.
- Documenting the handling and transfer of evidence, including dates, times, and personnel involved.

---

4. Handling and Storage of Evidence

4.1 Secure Storage

All physical and digital evidence must be securely stored to prevent loss, damage, or unauthorised access. This includes:

- Locking physical evidence in secure storage facilities.
- Encrypting digital evidence and storing it on secure, password-protected systems.

4.2 Access Control

Access to evidence is restricted to authorised personnel. A log must be maintained to track who accesses evidence, the purpose of access, and the date/time of access.

4.3 Preservation

Evidence must be preserved in its original form to avoid contamination or deterioration. For digital evidence, metadata must be maintained.

---

5. Presentation of Evidence

5.1 Accuracy and Objectivity

When presenting evidence in reports, affidavits, or court proceedings:

- Ensure all evidence is presented accurately and without bias.
- Clearly distinguish between facts, interpretations, and opinions.

5.2 Compliance with Legal Standards

Ensure evidence meets the requirements of admissibility under the *Evidence Act 2008 (Vic)*, including relevance, authenticity, and reliability.

---

6. Disposal of Evidence

When evidence is no longer required, it must be disposed of securely and in accordance with legal and regulatory requirements. This may include:

- Shredding physical documents.
- Permanently deleting digital files.

A record of evidence disposal must be maintained, including the date, method, and authorisation of disposal.

---

7. Training and Awareness

All employees, contractors, and agents must receive training on:

- Relevant laws governing evidence collection and handling.
- Ethical practices for investigations.
- This Evidence Policy and its application.

---

8. Monitoring and Review

This policy will be reviewed annually or as required to ensure ongoing compliance with legal and regulatory changes.

---

9. Contact

For questions or concerns regarding this Evidence Policy, contact:

Night Hawk Intelligence
support@nhi.net.au
0481 331 974

Night Hawk Intelligence is committed to maintaining the highest standards in the handling of evidence to ensure its integrity, admissibility, and compliance with the law.