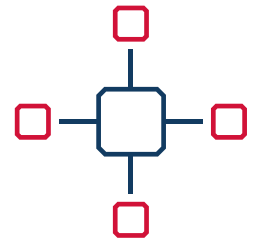# Pegasus:
Complete Covert Intelligence
Manage all areas of covert policing with one modular system

Pegasus makes it easy to handle and disseminate information, evidence and intelligence obtained through covert techniques.

We engage daily with all levels of law enforcement and intelligence professionals. This helps us ensure that Pegasus remains at the forefront of intelligence technology.

Why choose Pegasus?
Pegasus lets you manage every aspect of covert operational activity in one place. It's modular, so you can tailor it to match the operational needs of your agency, or any collaborative requirements. It's designed for organisations that demand the highest level of data accuracy, security and accountability.

- Improve management control, mitigate risk and maintain a comprehensive record of all actions and decisions
- Comply with all legislative requirements and support law enforcement processes and associated policy compliance
- Demonstrate duty of care to the public, and increase confidence in data management and security
- Optimise management oversight of covert operations to reduce the potential for corruption and deliver financial accountability
- Automatically produce documents and reports to support any internal or external inspections
- Reduce costs and improve efficiency: monitor organisational performance, operational deployment and associated expenses
- Automate real-time, secure sharing of intelligence and reduce double keying
- Search across all covert and intelligence-related functions, subject to appropriate access rights

Pegasus modules allows you to design the system you need

Informant Management
Lets you manage all activities associated with Covert Human Intelligence Sources (CHIS) and helps you manage the many inherent risks. Its tools give you control over all aspects of informant management, and creates a full audit history to reduce the potential for corruption.

Surveillance
Manages various aspects around applications for surveillance operations, including authorisation, risk management and surveillance logs. It also handles the data, images and recordings captured, and the resulting intelligence reports.

Undercover / Discreet Operations
This module manages all requirements for undercover operations. This includes the automated workflow for authorities as well as any required tests or training, management of assets, associated capabilities, and legend building. It lets you demonstrate compliant and effectively managed undercover activity.

Debrief
Manages the debrief of witnesses and others who have provided evidence or intelligence. It lets you record all relevant data and provides an auditable record of exchanges with potential or actual witnesses.

Protected Persons
Manages the entire process of witness protection and other at-risk people. It also simplifies contact report production, tracks financial expenditure and associated risk assessments, and delivers comprehensive records relating to admission and removal from protection schemes.

Communications Data Management
This module manages authorisations and data obtained from telecoms companies, including subscriber information, digital data and call records.

Community Intelligence
Manages intelligence obtained in confidence from the public and other non-registered 'sources'. This lets you establish a 'trigger-point' to commence registration, which helps demonstrate the appropriate duty of care. It also lets you record the origin of intelligence and produce intelligence reports.

Intelligence
You can use this module on its own to manage the beginning-to-end process of intelligence management. You can use it alongside other modules to achieve a more proactive and effective use of covert intelligence.

Case Management
Pegasus supports case management to its conclusion, and produces agency specific or legislatively required prosecution papers. It provides management and case oversight at required points in the process, automated workflow and reminders and warnings based on time settings.

Assumed Identities
The Assumed Identity module provides auditable tracking of applications for and authorisation of such identities, including their creation, on-going management and provision of appropriate certificates and notifications for internal and external use.

The process is supported by an automated workflow that can be configured to the organisational requirements.