GREENJAY

PROTECTIVE GROUP

Advance Protection

A Private Standard for Controlled Environments

Advance Protection is the controlled creation of arrival conditions.

A principal does not arrive into a neutral environment. The environment has already made decisions that affect privacy, safety, and continuity. Advance Protection is not simply ‘getting there first.’ It is the pre-arrival engineering of certainty so the principal can move through the agenda without disruption, without unnecessary visibility, and without living inside an operation.

Governance Before Tactics

The single most important factor in UHNW protection is decision clarity. Most failures occur when multiple teams act without unified authority or when escalation happens through noise and emotion rather than verification.

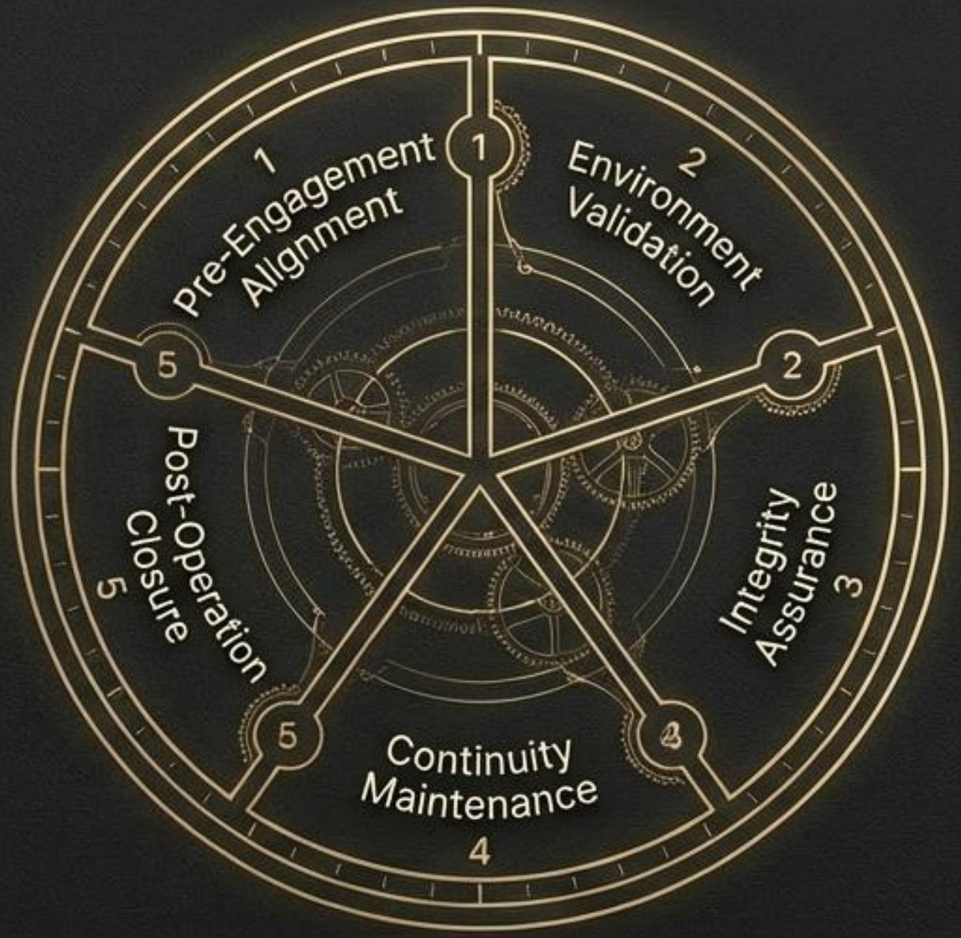
We begin by establishing governance, because without it, the best technical work becomes compromised by uncontrolled human dynamics.

When intent is not defined, even competent teams drift into improvisation, and improvisation creates exposure.

One Governed Condition: The Three Unified Domains

In our standard, these domains are never separated, because the seam between them is where exposure emerges. Physical measures that ignore electronic realities create blind confidence. Electronic measures that ignore human routines create friction and failure. Our program unifies the domains into a **single, governed state.**

A Managed Lifecycle, Not a Singular Event



The principal experiences continuity. The family office experiences accountability.
The program experiences repeatable improvement.

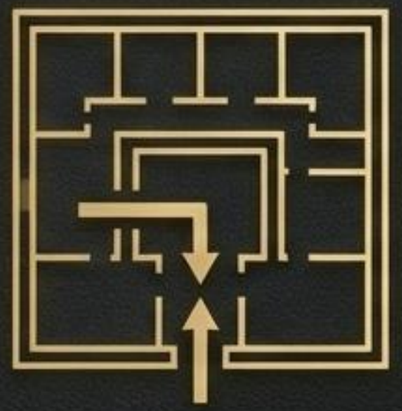
Phase 1: Pre-Engagement Alignment

 Defining Protective Intent	A plain-language definition of success, covering discretion, privacy, and continuity requirements. This is not a questionnaire; it is a controlled alignment.
 Mapping the Operational Perimeter	The explicit boundary of what we are responsible for controlling, eliminating ambiguity between teams.
 Governing the Human Perimeter	Identifying the people whose access and behavior can influence exposure—from staff and vendors to drivers and planners.
 Setting the Communications Posture	Establishing secure, authenticated channels to ensure coordination does not create patterns or exposure.

Phases 2 & 3: Environment Validation & Integrity Assurance

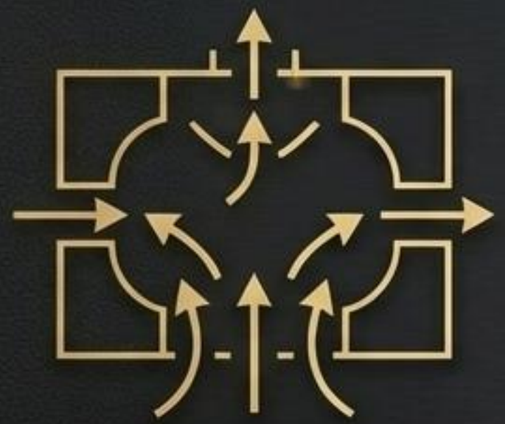
We confirm that locations can sustain privacy, safety, and continuity based on the protective intent. A location can be ‘luxury’ and still be porous. Our validation determines if it can support the standard.

Lodging Environments



Focus on privacy and access integrity, understanding service pathways and staff governance.

Venue Environments



Focus on exposure pathways, ensuring controlled entry, operation, and exit.

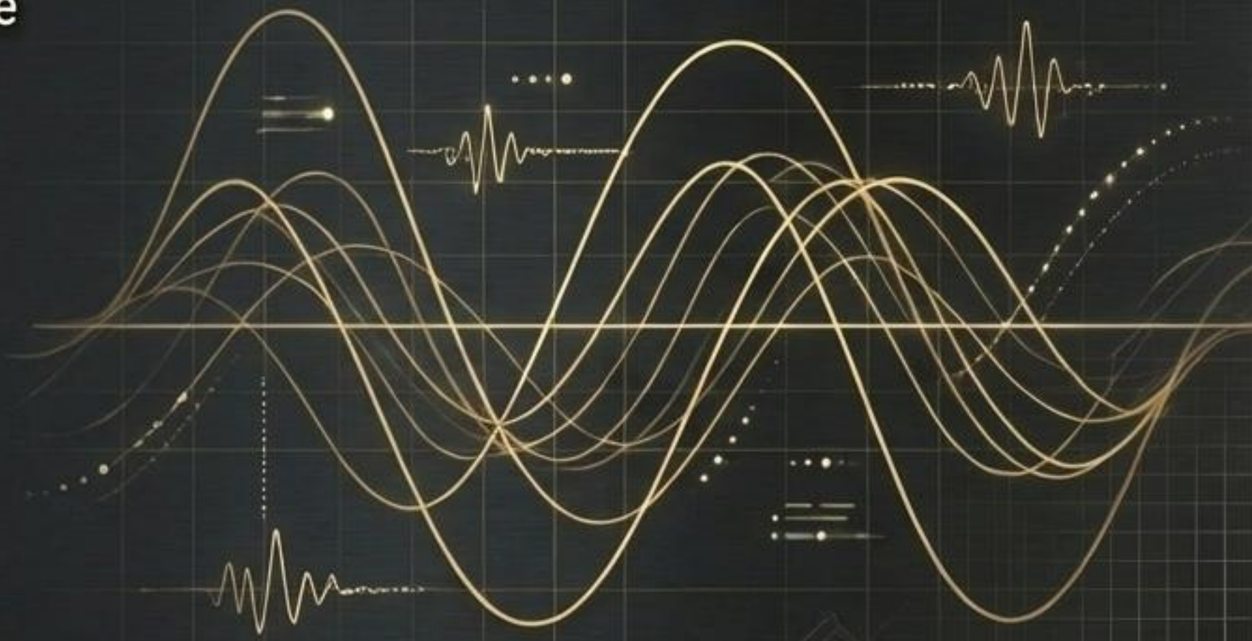
Routes & Transitions

Focus on preserving optionality and reducing predictable exposure windows.

Technical Assurance: Privacy Validation as a Professional Standard

We treat technical assurance as a documented service to reduce uncertainty, not as theatrics. Our posture is quiet, professional, and minimally disruptive.

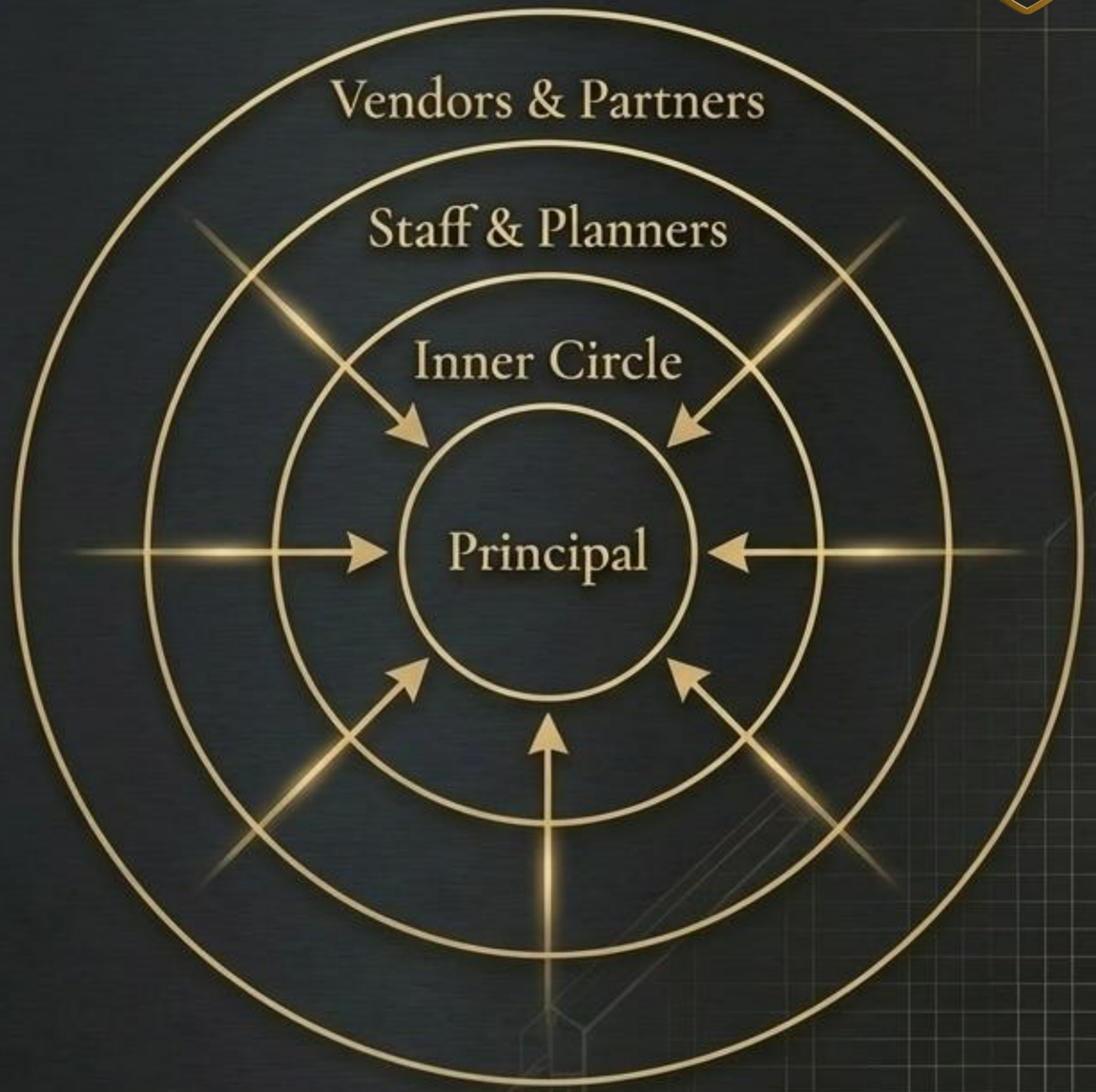
- **Privacy Validation:**
  Inspection for unauthorized observation, audio, or video devices and pathways of data leakage.
- **Spectrum Analysis:**
  A method for identifying and managing unusual emissions and wireless anomalies, providing clarity, not paranoia.
- **TSCM Services:**
  Delivered as documented findings and mitigation guidance, performed by qualified personnel using controlled methods.



The Human Layer: Integrity, Access, and Discretion

In UHNW environments, people create both security and exposure. The risk is not ‘staff.’ The risk is unmanaged access and unmanaged knowledge. We manage these risks through disciplined process.

- Verification of roles and appropriate access levels.
- Restricting sensitive information to those who must know.
- Partner alignment to the GreenJay standard.
- Treating vehicles and drivers as controlled operational environments.



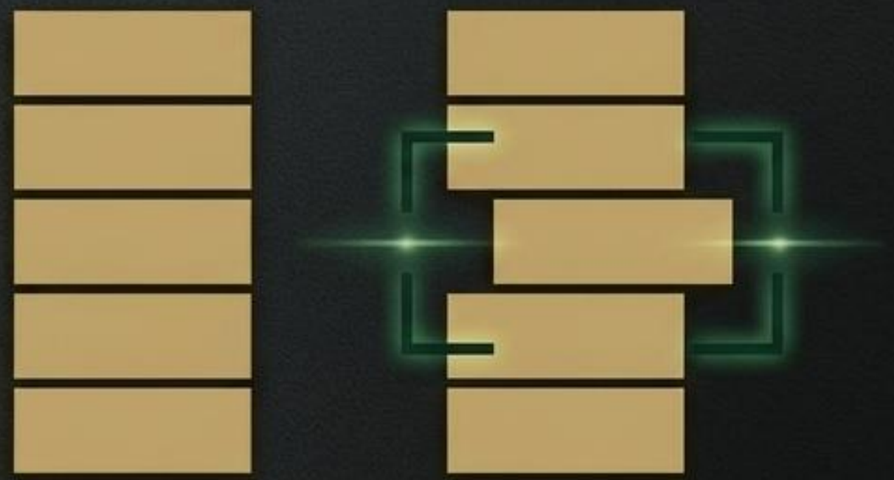
The Objective: A State of Controlled Arrival

We shape the environment to support the principal's life, rather than forcing the principal's life to be shaped by the environment. The principal arrives into a state where privacy is realistic, access is governed, and communications are stable.

A secure operation should not announce itself. The best protection is calm and invisible.

Phase 4: Continuity Maintenance – Managing Drift

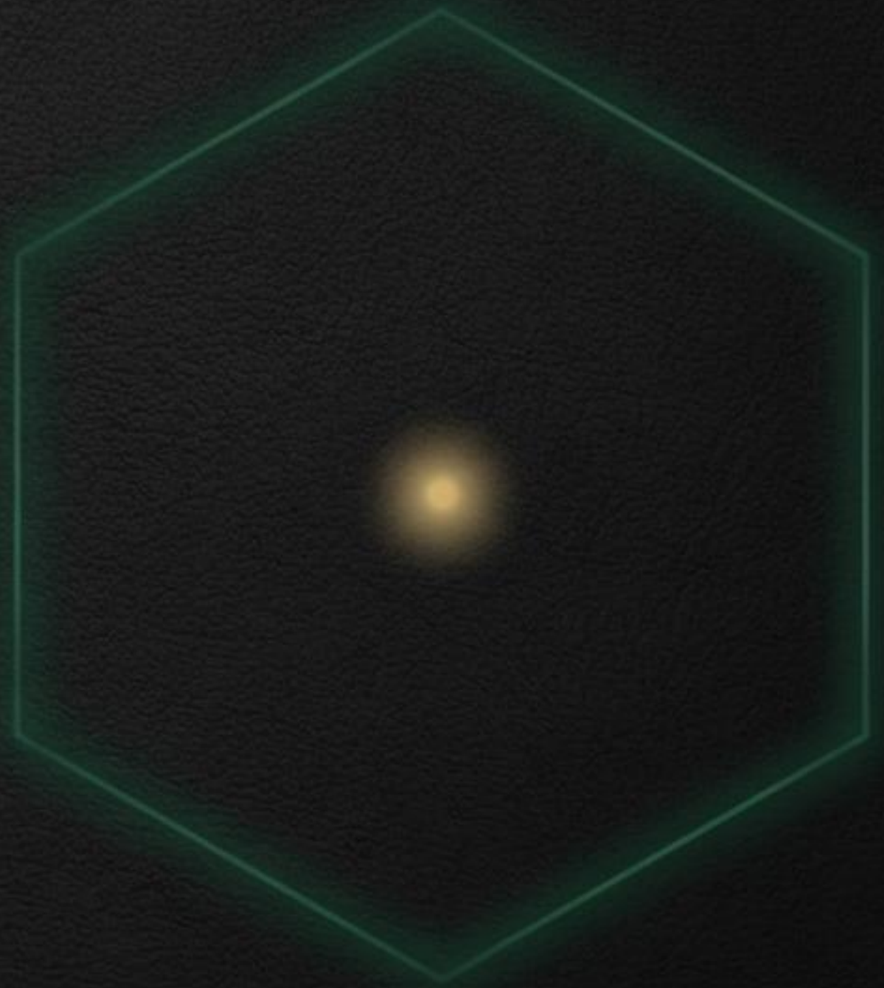
Locations drift. Staff rotate, vendors perform maintenance, schedules shift. We implement a controlled process of monitoring for meaningful change and managing it without disruption. Surprises create exposure.



Verify before escalating. This discipline protects the principal from drama and unnecessary disruption.

Incident Governance: Response Without Spectacle

UHNW protection is not only about preventing harm. It is about preventing public disruption and reputational damage. Our model governs response privately, with decision authority known and actions taken with restraint.



Our Service Commitment

Verification-first.
Calm escalation.
Discretion preserved.
Continuity prioritized.

The Deliverable Set: A Defensible, Retained Standard

The primary weakness in most security engagements is the lack of defensible outputs. Our program delivers a written and governed output set, stored in your private portal for continuity and governance.

- Protective Intent Document
- Environment Conditions Summary
- Access and Personnel Governance Summary
- Communications Posture Summary
- Continuity Oversight Summary
- Post-Operation Closure Report

The GreenJay Standard: An Operating Condition

Advance Protection is successful when the principal experiences **controlled arrival, quiet continuity**, and **minimal disruption**. It is successful when privacy is preserved without lifestyle compromise. It is successful when the family office has **documentation, accountability**, and a **standard that scales**.

It is successful when the principal does not feel the operation,
yet the operation is unquestionably in control.

GREENJAY

PROTECTIVE GROUP

The Architecture of Certainty.