



The Governed Domain

An Operating Standard for Digital Protection in
the Private Environment.

The Invisible Environment Is the New Front Line



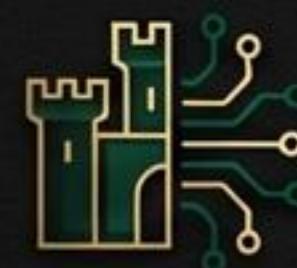
In modern UHNW life, digital exposure does not sit “next to” physical risk. It often precedes it.



It creates the conditions that make physical compromise easier: predictable movement, discoverable identity recognition, exposed communications, and accessible systems.



The mistake many firms make is treating “cyber” as a separate service, handled by a separate vendor, disconnected from protection.



In the GreenJay standard, the digital domain is part of protective operations. It is a governed state, not a set of products.



The Unique Complexity of the Private Estate

UHNW environments are a dense ecosystem of connected systems, each representing a potential access surface if left unmanaged.



Luxury-Compatible Security Engineering

We do not attempt to make the client live like a security professional. We build a secure state around the client's lifestyle.

The goal is quiet confidence. Convenience remains, but it is no longer an ungoverned liability.

The best secure estate is one where the security posture is powerful but visually quiet.

Privacy modes are engineered and controlled, not left to chance.



Our Operating Model: A Foundation of Four Disciplines



Control Identity

Prevent unnecessary visibility and stop exposure from compounding into physical risk.



Govern Access

Treat access surfaces as protective controls, not as “IT details.”



Preserve Integrity

Ensure systems behave predictably and are insulated from vendor convenience risks.



Verify Change

Monitor for meaningful deviations and verify them without creating noise.



Executing the Model Across Eight Governed Domains



Our disciplined model is applied consistently across the entire digital domain, ensuring no single point of failure and creating a holistic state of quiet confidence.



The Foundation: Controlling Discoverability and Access

Domain One: Identity Exposure Control

Governing Principle:

Reducing discoverability without disrupting lifestyle.

Key Disciplines:

- Govern how the principal's identity is used in bookings, deliveries, and service schedules.
- Discipline identity handling across staff, vendors, and travel.
- Reduce routine digital signals that make location and movements inferable.

The Deliverable:

An Identity Exposure Standard.

Domain Two: Access Governance

Governing Principle:

Who can touch what, from anywhere, and why.

Key Disciplines:

- Control broad, persistent, and unmanaged access for staff and vendors.
- Define how access is granted, revoked, and escalated.
- Provide clear visibility into who can access critical estate and family office systems.

The Deliverable:

The Access Governance Charter and Access Ledger.



Securing Communications and the Physical Environment

Domain Three: Communications Integrity

Governing Principle:

Making sure your words remain yours.

Key Disciplines:

- Establish appropriate channels for sensitive communications for both principal and staff.
- Counteract the degradation of security posture during travel.
- Provide an engineered infrastructure that makes secure habits easy to follow.

The Deliverable:

The Communications Integrity Standard.

Domain Four: Estate Systems Hardening

Governing Principle:

Viewing surveillance, AV, IT, and smart home as one domain.

Key Disciplines:

- Ensure the entire ecosystem functions together under one secure state.
- Integrate security discreetly to protect aesthetics and luxury.
- Engineer “privacy modes” to respectfully manage household life.

The Deliverable:

The Secure Estate Architecture Summary.



Managing Third-Party and Travel-Related Risk

Domain Five: Vendor Integrity

Governing Principle:

Governing the quiet risk that most estates underestimate.

Key Disciplines:

- Align vendor convenience with the UHNW protective intent.
- Limit and control remote access, ensuring it is time-bound and accountable.
- Prevent vendor systems from creating a 'shadow network' inside the estate.

The Deliverable:

The Vendor Access Governance Summary.

Domain Six: Travel Network Security

Governing Principle:

Establishing a secure network anywhere we go.

Key Disciplines:

- Provide an operating capability for secure connectivity, not just a gadget.
- Make reliance on untrusted hotel or public Wi-Fi optional.
- Ensure the protective team can coordinate privately and reliably on the move.

The Deliverable:

The Travel Connectivity Standard.



Proactive Awareness and Intelligent Oversight

Domain Seven: Counter-Surveillance Awareness

Governing Principle:

Reducing opportunistic observation through engineered defaults.

Key Disciplines:

- Validate digital conditions and treat untrusted infrastructure as risky by default.
- Maintain disciplined device posture for both principals and staff.
- Reduce the probability of operating inside an environment that is quietly collecting information.

The Deliverable:

The Digital Counter-Surveillance Assurance Statement.

Domain Eight: Monitoring and Verification

Governing Principle:

24/7 oversight without the noise.

Key Disciplines:

- Focus on verification-first oversight for meaningful deviations from baseline.
- Verify access anomalies, system integrity drift, and unusual activity before escalation.
- Ensure the principal is not burdened with noise; response is calm and private.

The Deliverable:

The Digital Continuity Oversight Summary.



The Private Deliverable Set: A Retained Standard for the Estate

Digital Domain Protection produces a consistent set of documents that create a living standard for the family office and estate, ensuring continuity and governance.

- ✓ Digital Protective Intent
- ✓ Identity Exposure Standard
- ✓ Access Governance Charter
- ✓ Communications Integrity Standard
- ✓ Secure Estate Architecture Summary
- ✓ Vendor Governance Summary
- ✓ Travel Connectivity Standard
- ✓ Digital Continuity Oversight Summary

Highly sensitive system architecture diagrams and implementation methods are retained in restricted annexes, available only to authorized stakeholders.



The Operating Promise of a Governed Domain

To preserve privacy without disrupting lifestyle.

To prevent convenience from becoming compromise.

The principal experiences a quiet life.

Devices work. Systems work. Staff operate without improvisation.

Travel remains connected without relying on untrusted infrastructure.

Monitoring exists without noise.

Response is calm and governed privately.

That is the secure state.



