RAW Agents' Secret Information Manual (Classified Level 7)

Issued By: Directorate of Covert Operations

Security Clearance Required: Level 7 and Above

Last Updated: January 2025

Introduction

This document is classified under **Protocol Shadow-13** and is strictly accessible to agents holding Level 7 clearance or higher. Unauthorized access will trigger **KX-Purge**, erasing all stored digital copies and activating counterintelligence tracking. If you are reading this without proper clearance, consider this your final warning.

The **RAW Intelligence Network (RIN)** functions on a zero-trust basis. Every operation, every message, every identity must be **verified, cross-validated, and encrypted using multi-layered authentication techniques**. The methodologies outlined in this manual are designed to ensure operational integrity, information security, and agent survival.

To confirm authenticity, enter the following cipher into your secured terminal before proceeding:

`EK7-ΣΔ19-βXQ//4437`

If access is denied, cease all attempts immediately and **burn this document**.

Communication & Verification Protocols

Layered Cipher Code (LCC) System

Every message exchanged within the RAW network must be encoded using **LCC**, a three-layer cryptographic structure involving:

1. **Quantum Hashing** – Ensures no two messages use identical encryption patterns.
2. **One-Time Pad (OTP) Key Exchange** – Physical key drops are mandatory; digital keys are compromised upon creation.
3. **Neural Signatures** – For classified transmissions, only pre-approved cognitive patterns are accepted.

For verification during in-person meetings, agents must execute the **Handshake Protocol**:

- **Step 1:** Blink twice in a 2-second interval.
- **Step 2:** Tap the left wrist once.
- **Step 3:** Recite the phrase corresponding to the current operational cycle. (Phrases rotate every 48 hours and can be found in encrypted briefings).

If the other agent fails any of the steps, assume immediate compromise and **neutralize** the target.

Covert Operations: Field Tactics & Extraction Methods

Deep Cover Operations

Agents embedded in long-term missions must adhere to the **S-29 Protocol**, which dictates:

- **No digital activity for 90 days post-deployment.**
- **Alias Rotation every 21 days**, with a two-layer backstory pre-approved by the Directorate.
- **Financial Footprint Erasure**, including the creation of false transaction histories through **mirror-wallets** and pre-approved laundering routes.

If compromised, execute **"Shadow Step"**, a multi-phase extraction process:

1. **Initiate Disruptor Wave**: Deploy localized **EMP grenades** to erase nearby digital records.
2. **Trigger Persona Collapse**: Access hidden backup alias data via **Vault-17** decryption keys.
3. **Disappear within 6 hours**: Move to a pre-mapped **Phase-Shift Safehouse**, location rotated every 72 hours.

Classified Safehouses & Black Sites

All safehouses are **non-traceable** and use multi-tiered security structures to ensure no agent can identify more than two at any given time. The following are currently active:

[DO NOT MEMORIZE. DESTROY AFTER READING.]

Safehouse K-41 (New Delhi) – Accessible through the **underground maintenance hatch** at "Gopi's Tea Stall." Entry requires biometric authorization + a 4-key cipher.

Safehouse H-77 (Berlin) – Disguised as a **candle shop** near Friedrichstrasse. Purchase of a **black lavender candle** initiates the entry sequence.

Facility X-17 (Black Site - Location Unknown) – Used for high-value targets. **Zero external records exist**. Entry requires authorization from Level-9 operatives.

The Silent Room – A facility equipped with **anechoic shielding**, ensuring no electrical signals can escape. Any captured individuals are kept in complete **sensorial deprivation** until interrogation is complete.

To gain entry, use one of the following passcodes:

```
Level 7 Entry Code: F3H//Σ98-LX
Emergency Extraction Code: X7-99//BETA
```

These codes expire in 30 seconds post-display.

Counter-Surveillance Measures

To prevent tracking, RAW agents must use the **Ghost-Step Algorithm**, which:

- **Removes all digital traces in real-time.**
- **Obscures biometric data through AI-generated decoy patterns.**
- **Scrambles digital shadows using quantum misdirection pulses.**

Any surveillance **attempting to breach the system** must be flagged using:

`Ω/RED-FLAG 47`

This triggers a **kill-switch** for all RAW devices in a **10-kilometer radius**.

Operational Termination & High-Risk Protocols

"Project Eclipse" (Zero-Trace Protocol)

Activated only when an **entire operational unit is at risk of discovery**. This involves:

- Deployment of **"Silent Dissolution Agents"** for immediate **erasure of intelligence assets**.
- Initiation of **"Omega Wave"**, a **quantum-level data wipe** that eliminates all records from RAW servers within a 1000km radius.
- Activation of **Blackout Plan Zeta**, requiring all operatives to undergo identity resets.

Agents flagged for **permanent extraction** will be reassigned under the **Cipher Seed Regeneration Program**, which wipes prior identities and integrates them into civilian roles.

Emergency Directives

If Captured:

1. Recite **false operational data** to mislead interrogators.
2. Activate **Neural Frequency Dampeners** to disrupt EEG-based lie detection.
3. If conditions worsen, use the **Final Protocol**:

`Release Code: “The fire rises, the bridge burns.”`

This triggers **Protocol Zeta-5**, permanently erasing the agent's existence from all databases.

Final Notes & Classified Directives

This document **must never be stored in digital form**. After memorization, agents must:

- **Destroy all physical copies.**
- **Verify cipher decryption with a Level-9 operative.**
- **If suspicion arises, execute Protocol Vortex.**

Any deviation from these procedures **will be considered a direct breach of RAW security, punishable by immediate neutralization**.

Remember:
Trust no one. Assume nothing. Adapt or be eliminated.