Sovereign Starter Kit v1.0

Project Sovereignty Public Module — CC-BY 4.0

Module 1: ProtonMail + Alias Strategy

TL;DR

Establish a compartmentalized, encrypted email setup that protects your identity, limits metadata leakage, and enables flexible identity routing.

Why This Matters

Your email address is often the root identifier across surveillance and marketing ecosystems. Splitting identity surfaces—while using a hardened, encrypted provider—significantly reduces your digital footprint.

Step-by-Step Setup

1. Create Core ProtonMail Account

- Go to proton.me and register a new account using a clean network (VPN recommended).
- Avoid real name or personal data.
- Choose a handle that is context-neutral and non-identifiable (e.g., “anchorframe@proton.me”).

2. Enable Key Protections

- **Two-factor auth**: use Proton’s built-in TOTP or an offline authenticator app (e.g., Aegis, Raivo).
- **Recovery code**: store your Proton recovery phrase in an encrypted vault (e.g., Bitwarden with 2FA).
- **Display name**: remove or pseudonymize in settings.

3. Set Up Aliases via ProtonMail or SimpleLogin

- **Option A (ProtonMail aliases)**:
    - Use + aliases for contextual routing (e.g., anchorframe+gov@proton.me or anchorframe+burner@proton.me).
    - Route aliases into folders with filters.
- **Option B (SimpleLogin)**:
    - Link your Proton account to simplelogin.io.
    - Create forward-only aliases by use-case (e.g., newsletter@yourdomain.com → anchorframe@proton.me).
    - Turn off reply-to where anonymity is critical.

4. Folder + Tagging Scheme

- /GovID
- /Banking
- /Accounts
- /Burner
- /Newsletters

Assign filters for auto-routing by alias.

Operational Notes

- Use **ProtonBridge** only on fully encrypted local devices.
- Don’t autofill emails into browsers or forms—keep aliases deliberate.
- Maintain an offline list of alias mappings (air-gapped or written, not stored online).

Outcome

You now control multiple digital identities, route communications based on exposure risk, and operate from an encrypted Swiss-hosted backend that resists dragnet surveillance.

Author: Sovereign Systems (Project Sovereignty)

Version: v1.0 — 2025-06-01

License: CC-BY 4.0

Metadata: AI assisted (GPT-4), ProtonMail verified, Markdown compiled

---

Module 2: Secure Messaging & MySudo Layer

TL;DR

Set up encrypted, pseudonymous communication channels for daily use, contact compartmentalization, and short-life outreach.

Why This Matters

Messaging apps are a top vector for metadata profiling, behavioral tracking, and social graph extraction. Encrypted apps with deliberate contact protocols block mass-correlation.

Step-by-Step Setup

1. Secure Signal Install

- Use a separate burner phone or install Signal on GrapheneOS/iOS device.
- Register with a clean SIM or use a number via MySudo.
- Set to auto-delete messages after 1–7 days depending on context.

2. Setup MySudo Profiles

- Download MySudo and configure multiple Sudo profiles.
- Use each for specific roles: e.g., BizOps, Burner, Media.
- Link email, phone, and browser identities within each silo.

3. Contact Onboarding Protocol

- Verify fingerprint in Signal settings for trusted contacts.
- Use custom emoji tags or internal notes to track exposure risk.
- Avoid syncing contacts to phone—add manually.

4. Anti-Correlation Hygiene

- Never reuse Signal QR codes between contexts.
- Avoid answering unknown cold outreach unless routed via known intro alias.
- Rotate Sudos quarterly or after travel.

Operational Notes

- MySudo is U.S.-jurisdiction—use for mid-trust operations, not high-risk ops.
- Signal stores zero message content but does expose registration date and contact hash (minimized with contact discipline).
- Periodically export and wipe logs.

Outcome

You've established a durable, encrypted, and identity-compartmentalized messaging layer that cannot be easily correlated to your legal identity.

Author: Sovereign Systems (Project Sovereignty)

Version: v1.0 — 2025-06-01

Metadata: AI assisted (GPT-4), MySudo + Signal validated, Markdown compiled

---

Module 3: Mobile Device Lockdown

TL;DR

Transform a mobile phone into a hardened personal node—free from telemetry, ad identifiers, and silent compromise vectors.

Why This Matters

Your phone is the most intimate tracking device. Without hardening, it continuously leaks your location, behavior, biometrics, and network graph.

Step-by-Step Setup

1. Choose Your Base OS
    - Option A: GrapheneOS (recommended for advanced users)
        - Buy a Pixel 6a/7/7a direct from Google or secondary seller (avoid logged-in resale platforms).
        - Flash GrapheneOS using the web installer.
        - Remove OEM accounts and install only essential apps from F-Droid or Aurora Store.
    - Option B: iPhone (simplified hardening)
        - Disable location services for all but maps.
        - Turn off ad ID tracking, Siri, analytics sharing.
        - Set content restrictions and lock down iCloud sync to minimum viable exposure.
2. Network Privacy
    - Install Mullvad VPN or ProtonVPN and enable at boot.
    - Use a privacy-respecting DNS (e.g., NextDNS, ControlD) with blocking lists for tracking domains.
3. App & Sensor Control

- Limit apps to messaging, authentication, maps, and encrypted files only.
- Revoke all unnecessary permissions—especially camera, mic, location, Bluetooth.
- Disable background refresh for all apps.

4. Physical Hygiene

- Use Faraday sleeve in transit or off-grid operations.
- Regularly clean cached data and perform cold reboots weekly.
- For GrapheneOS, use separate user profiles per context (e.g., Travel, Comms, Auth).

Operational Notes

- GrapheneOS gives full control but requires technical patience. It is the closest thing to a sovereign mobile OS.
- iPhone remains partially closed but can be secured for moderate threat levels.
- Always assume cellular networks are hostile: never tie secure devices to your real identity SIM.

Outcome

Your mobile device is no longer a passive surveillance node. Instead, it becomes a compartmentalized tool for private operations with minimal exposure.

Author: Sovereign Systems (Project Sovereignty)
Version: v1.0 — 2025-06-01

Metadata: AI assisted (GPT-4), GrapheneOS + iOS validated, Markdown compiled

Sovereign Starter Kit v1.0

Project Sovereignty Public Module — CC-BY 4.0

Module 4: File + Data Encryption

TL;DR

Encrypt and store sensitive files using open-source tools that allow secure local and cloud storage, while scrubbing embedded metadata and creating verifiable backups.

Why This Matters

Data at rest is a prime surveillance and compromise target. Most cloud and local storage leaks silently via metadata, sync logs, or unencrypted archives. Encryption must be the default, not the exception.

Step-by-Step Setup

1. Create Encrypted Containers

- VeraCrypt (for full-volume or file container encryption):
  - Download from veracrypt.fr.
  - Create a hidden or standard container with AES or Serpent encryption.
  - Store container on external drive, USB, or cold backup disk.
- Cryptomator (for user-friendly cloud sync encryption):
  - Install from cryptomator.org.
  - Create a vault inside Dropbox, ProtonDrive, or local folder.
  - Access via mobile or desktop client with real-time encryption.

2. Metadata Scrubbing

- Install MAT2 (Linux/macOS) or ExifTool (Windows/macOS).
- Run all sensitive docs, PDFs, and images through metadata scrubbing before storage or transmission.
- For PDFs: print to PDF or export via safe processors (e.g., Typst, LibreOffice).

3. Backup + Redundancy

- Export a copy of your encrypted container or vault monthly.

- Store one version in a cold offline drive (AES-256 encrypted, disconnected).
- Mirror one vault to a secure ProtonDrive folder or air-gapped device.

4. File Handling Discipline

- Never leave decrypted versions in cloud sync folders.
- Only mount vaults on trusted, clean OS environments.
- Use SHA256 hashes to verify vaults after sync or transfer.

Operational Notes

- VeraCrypt supports hidden volumes for deniable access.
- Cryptomator is easier for mobile access but assumes cloud sync trust (minimize risk).
- Keep a printed or hardware-backed record of all vault passwords and keys.

Outcome

Your sensitive files are now protected against both network surveillance and physical compromise, with a layered backup system and scrubbed content free of identifying metadata.

Author: Sovereign Systems (Project Sovereignty)
Version: v1.0 — 2025-06-01

Metadata: AI assisted (GPT-4), VeraCrypt + Cryptomator tested, Markdown compiled

---

Module 5: Browser Privacy & Metadata Obfuscation

TL;DR

Use hardened browsers, custom DNS routing, and anti-fingerprinting techniques to prevent tracking, profiling, and passive telemetry while browsing.

Why This Matters

Browsers are surveillance goldmines. They leak fingerprints, behavioral signals, and session identifiers to ad networks and hostile trackers. Obfuscation and discipline are essential.

Step-by-Step Setup

1. Hardened Browser Selection
    - Primary Recommendation: Brave (with Shields set to Aggressive)
    - Secondary Option: Firefox (with Arkenfox user.js or Librewolf variant)
    - Disable WebRTC, set homepage to blank, turn off telemetry.
2. Install Core Extensions
    - uBlock Origin — for tracker and ad blocking
    - NoScript — blocks JS execution by default
    - ClearURLs — strips tracking parameters from links
    - Cookie AutoDelete — erases cookies after tab close
3. DNS + Network Obfuscation
    - Use Mullvad VPN or ProtonVPN with auto-start
    - Route DNS through NextDNS or ControlD with hardened filters
    - Set browser to use DNS-over-HTTPS (DoH) pointing to trusted provider
4. Fingerprint Mitigation
    - Avoid resizing browser windows—keep them full screen
    - Disable canvas, font, and audio fingerprinting (Firefox users: set prefs manually)

- Randomize or rotate user agent with an extension like Chameleon (Firefox only)

5. Operational Discipline

- Never log into personal accounts in privacy browsers
- Use separate browser profiles or containers per context (work, research, burner)
- Clear all sessions after use; avoid bookmarking in privacy mode

---

Operational Notes

- Chrome and Safari are not safe for high-integrity browsing.
- Mobile users should use Brave or Firefox Focus with similar precautions.
- Periodic browser fingerprint tests via amiunique.org or browserleaks.com

---

Outcome

You've significantly reduced your browser fingerprint, blocked surveillance APIs, and compartmentalized browsing sessions to disrupt passive surveillance.

Author: Sovereign Systems (Project Sovereignty)
Version: v1.0 — 2025-06-01

Metadata: AI assisted (GPT-4), Brave + Firefox validated, Markdown compiled