Hackers4Justice – Legal and Ethical Charter

1. Mission Statement
Hackers4Justice is an international collective of volunteer OSINT analysts, software developers, and ethical hackers dedicated to supporting law enforcement and public interest investigations. Our mission is to harness technical expertise to promote justice, prevent cybercrime, and protect communities—while strictly operating within the bounds of applicable law.

2. Core Principles
Legality First: All activities must comply with local, national, and international laws, including but not limited to the U.S. Computer Fraud and Abuse Act (CFAA), General Data Protection Regulation (GDPR), and Digital Millennium Copyright Act (DMCA).

Ethics Over Exploitation: We do not engage in unauthorized access, data breaches, or surveillance outside lawful parameters.

Transparency & Accountability: All members will log research sources, act transparently with leadership, and maintain secure, auditable records.

Consent & Authorization: No penetration testing, social engineering, or deep scans may occur without explicit written permission from the system owner or authorized entity.

Privacy Protection: We do not collect or retain personally identifiable information (PII) without legal justification, and we anonymize reports to protect innocent parties.

3. Scope of Activities
Hackers4Justice members may participate in:

Collecting and analyzing open-source intelligence (OSINT) from public sources.

Reporting suspected criminal activity or cyber threats to law enforcement.

Supporting law enforcement investigations upon request or invitation.

Developing tools or frameworks that assist in crime prevention or threat analysis.

Running honeypots or research systems on their own infrastructure to monitor malicious behavior legally.

4. Prohibited Conduct
Members are strictly forbidden from:

Gaining unauthorized access to any system, device, or network.

Downloading, storing, or distributing leaked/stolen data.

Impersonating law enforcement, government officials, or private entities.

Conducting social engineering attacks without pre-authorized, scoped testing.

Engaging in vigilante activity or public exposure of suspects without due process.

5. Relationship with Law Enforcement
Hackers4Justice does not act as an agent of any law enforcement body. All assistance is offered voluntarily and in a support capacity. Any formal collaboration will be based on mutual agreements (e.g., MOUs) and may require member background checks or vetting.

6. Membership Code of Conduct
All members must:

Pass a basic vetting process.

Sign a confidentiality and ethics agreement.

Undergo regular training on legal compliance and best practices.

Report any breaches of this charter to leadership immediately.

7. Liability and Disclaimers
Hackers4Justice is not liable for unauthorized actions performed by individual members outside the organization's policies. Participation in Hackers4Justice does not confer immunity from law enforcement scrutiny if legal boundaries are violated.

8. Amendments
This charter may be revised by majority vote of the core leadership team and legal advisors, in consultation with law enforcement liaisons as needed.