Policy on Ethical Use of Threat Intelligence

Latest Update: 7/28/2025

Flare collects and structures data that may be exposed online, leaked by cybercriminal groups, or otherwise obtained through lawful means to generate threat intelligence. While some of this data may be technically accessible elsewhere, it is often fragmented, sensitive in nature, and subject to misuse if not handled responsibly.

This policy applies to how we collect, process, and structure threat intelligence across all of our operations, including during research and development. It outlines the safeguards we implement to control access, prevent misuse, and protect any personal data that may be included.

We believe responsible threat intelligence work requires balancing two priorities: enabling organizations to defend themselves against cyber threats, and ensuring that the intelligence we provide is not used in ways that violate rights, privacy, or trust. This policy reflects the measures we take to maintain that balance.

You can reach out to us at any time. We are located in Canada, and our ownership structure is simple, and transparent.
Flare Systems, Inc.
Address
legal@flare.io

1. Principles

To prevent misuse and enable responsible use of the threat intelligence data we collect, Flare follows clear principles that apply across our platform and services:

- **Purpose-Driven**: Threat intelligence shared through Flare must be used to prevent cybercrime, protect organizations, or support investigations. Use for unrelated commercial purposes, and re-distribution, are strictly prohibited by contract. We enforce our contracts with anyone who breaches our acceptable use requirements.

- **Human Rights**: When deciding if we should work with a third-party, a client, or a partner, we assess any potential impacts on human rights.

- **Confidentiality First:** Even when data is exposed online, we treat it with care. Threat intelligence may include leaked credentials, internal documents, or sensitive patterns – whether or not it qualifies as personal or client data. We secure it accordingly.

- **No Re-Identification**: If personal data is de-identified, re-identification is strictly prohibited. Safeguards are built-in to prevent this, aligned with laws like the California Consumer Privacy Act.

- **Controlled Distribution**: Data shared through our services cannot be redistributed to third parties, for commercial gains. Clients and partners are under strict contractual obligations. Redistribution or resale is not permitted outside defined cybersecurity use cases. We screen all data recipients, including against export control restrictions.

- **Transparency**: We clearly explain what data we collect, how we use it, and who can access it. This applies to clients, users, and individuals whose data may be implicated.

- **Accountability**: We log data access and monitor how our platform is used. Our infrastructure and processes are covered by SOC 2 Type II audits, which we renew annually.

- **Compliance & Ethics:** We follow regulatory requirements, but we also aim for the ethical decision when the law lacks clear boundaries for our case study. When gray situations emerge, we seek legal counsel, industry feedback, and ensure measures are in place to mitigate risks.

2. Access Controls and Safeguards

Access to threat intelligence – especially when it involves leaked or sensitive material – must be controlled. We apply strict safeguards to determine who can use or access our services, under what conditions, and for what purposes. Our platform is not publicly searchable or broadly available, and access is gated by design. This is non-negotiable for us.

Eligibility and Access

We only work with organizations that meet our policy requirements. If they don't, access to our threat intelligence is denied—plain and simple. Before granting access to our platform, we apply a structured know-your-customer (KYC) process to ensure all organizations and individuals are clearly identified, vetted, and approved. No access is anonymous, and our services are not available through self-serve sign-up. Threat intelligence is only made available through an annual subscription, including any API integrations.

- All clients are screened through a due diligence process to ensure that they are duly registered, located in a country that allows for sufficient protection of the information, including personal data, shared with the recipients. We also validate clients against sanctions and restrictions list, and maintain our own additional "do not sell list".

- Human rights are a fundamental part of our assessment. We don't limit ourselves to export control and sanctions, we go further. We've built a custom risk scoring system that incorporates human rights data from Freedom House, rule of law data from the World Justice Project that we use in decisions for which organizations we do business with.

- Our solution engineering team validates customers' use cases to ensure the platform's projected use aligns with our contractually permitted use and is for cybersecurity purposes, and with external laws and limitations on use in certain industries. Our Customer Success Manager continues to follow the client through the relationship after.

- Users to the platform must be associated with a customer, and must be an employee in a related role, such as cybersecurity.

Even when we provide free trials, a vetting is in place. We also mask sensitive data, and only provide a sanitized version of the platform; no full access is granted until the full vetting is completed. Access to the full version of Flare is not possible without a contract in place.

We do not sell to, or work with organizations that are not engaged in legitimate, cybersecurity defensive use-cases, or law enforcement activities. Our work with law enforcement and the government is subject to the same ethical standards.

Privacy

Threat intelligence often contains fragments of personal data – whether leaked, publicly exposed, or unintentionally included. We treat these signals with care. Our position is clear: if data can identify a person or be linked back to one, we apply safeguards—regardless of how it was obtained or whether local laws would classify it as personal data.

We are not a data broker. We don't traffic data for profit. We provide vetted access to structured intelligence services to organizations based on their needs to protect their own networks. Our privacy posture reflects the sensitivity of that responsibility.

- We conduct privacy assessments (DPIA, PIA) before launching new features or changing how we process personal data. This helps us evaluate what data is necessary, what can be filtered out, what our clients truly need to access, how to make this determination, and how to apply proportional controls.

- When applicable, we honor individual privacy rights based on the context and purpose of collection. Requests are evaluated seriously, and handled with clear procedures. We have named persons responsible for this who are trained with data protection laws, and have experience with these complex requests.

- **Cross-Jurisdiction Safeguards:** We don't downgrade protections based on geography. Whether a data subject is in the European Union, the United States, or Canada, we apply the same baseline security and handling rules.

Privacy isn't just about compliance. It's about making informed decisions during collection, structuring, and distribution, and ensuring those decisions hold up under scrutiny. We also published our Product Privacy Notice for transparency on how our platform handles personal data.

3. Technical Measures

We apply layered technical safeguards to limit access, monitor use, and protect the integrity of the threat intelligence available through our services. These measures apply internally to our staff and externally to clients accessing the platform.

Access Control

Access to our systems and infrastructure is restricted using role-based access controls (RBAC). Internally, only personnel with a defined operational need can access sensitive environments. All permissions are reviewed periodically.
On the client side, platform access is gated by account and role. Each user must be linked to a verified organization and operate within approved scopes.

Logging and Monitoring

We maintain full audit logs of all access to the platform. This includes user queries, accessed records, and any actions taken within the system. We regularly review logs for abnormal activity or out-of-scope usage.

Client interactions with the platform are also monitored to ensure searches align with the approved use case. When activity appears inconsistent with the agreed purpose or contract, it is escalated internally.

Fraud and Abuse Monitoring

We actively monitor for misuse, including automated scraping, token abuse, and credential sharing. While we don't publicly disclose the full scope of these controls, they are embedded across the platform and supported by internal response protocols.

4. Values

We genuinely want to help. The nature of the data we process creates a responsibility to use it constructively—to prevent harm, not cause it. That's why Flare regularly conducts **responsible disclosures** when we identify information that could put individuals, organizations, or communities at risk.

We report relevant findings to law enforcement and coordinate with trusted partners in the cybersecurity community when the situation warrants it. Our actions are guided by impact, not optics.

We also launched **Flare'24**, a program offering free platform access—valued in the millions of dollars—to 24 nonprofit organizations working in critical sectors. These include civil society groups, healthcare institutions, and humanitarian organizations that often lack access to threat intelligence, despite being frequent targets of attacks.

Our commitment to ethical use is not theoretical. It's something we practice in the field, every day, in the choices we make about who we serve, how we act on what we see, and where we invest our time and resources.

---

5. Complaint Mechanism

We recognize that trust is earned not just through policies, but through accountability. If you have a concern about how threat intelligence is handled on our platform—whether it involves privacy, access, or ethical use—we encourage you to raise it.
You may submit concerns or complaints by email to:
📧 **legal@flare.io**
Reports are reviewed by our legal and compliance team, and where needed, escalated internally. We respond as promptly as possible, and we are committed to handling all concerns with transparency and professionalism.