IPS Data Taxonomy White Paper – Systems Data

The purpose of this document is to provide customers with a clear understanding of how IPS collects, uses, and protects Systems Data across IPS platforms, IPS OneSecure™, and all related security, cloud, and AI-driven services.

1. What Is Systems Data?

Systems Data refers to information generated or collected when you use IPS products, solutions, platforms, and managed services. This may include security logs, file metadata, telemetry, session activity, usage insights, threat intelligence, NetFlow data, AI assistant interactions, potentially malicious artifacts, and derivatives created through analysis or detection engines.

2. How IPS Uses Systems Data

- To provide IPS products and services (telemetry reporting, troubleshooting, sandboxing, Zero Trust enforcement)
- To improve and develop IPS technologies (optimize detection engines, enhance IPS OneSecure™ AI, improve performance)
- For cyber threat research and intelligence (analyze emerging threats, attacker behaviors, create signatures)
- To support customer success and relationship management (optimize onboarding, strengthen configurations)

3. Core Principles

- IPS processes Systems Data only for the purposes defined.
- Systems Data is protected through IPS Information Security Measures.
- IPS restricts disclosure except to authorized affiliates, partners, subprocessors, or when required by law.
- IPS does not train generative AI on identifiable Systems Data.
- Some on-premise deployments may limit or localize collection.

4. Interaction with Other Data Types

Customer Data is protected under contractual obligations and used only to deliver services. Personal Data collected incidentally is processed according to applicable laws, the IPS Data Processing Addendum, and IPS Global Privacy Policy.

5. How IPS Secures Systems Data

IPS applies encryption, least-privilege access, Zero Trust architecture, auditing, secure SDLC practices, monitoring, and supply-chain controls as defined in the IPS Information Security Measures.

6. Examples of Systems Data

- Logs
- File attributes
- Session data
- Telemetry data
- Support data
- Usage data
- Threat intelligence / threat actor data
- Statistics
- NetFlow data
- IPS OneSecure™ AI assistant inputs/outputs
- Potentially malicious files or policy violations

About This White Paper

The information in this document is for informational purposes only and may be updated periodically as IPS security and service capabilities evolve.