IPS Information Security Measures

1. Scope

Considering the nature, scope, context, and purposes of processing, as well as the state of the art, implementation costs, and risks of varying likelihood and severity to the rights and freedoms of individuals, this document describes the technical and organizational measures that IPS Network Inc. (“IPS”) maintains and implements to secure Personal Data, Customer Data, and Systems Data (collectively, “Data”) processed by any IPS Product or Service (“Measures”).

These Measures apply across all IPS platforms, including IPS OneSecure™, Intelligent GenAI services, security analytics, cloud solutions, SASE/SSE environments, managed infrastructure, and any supporting systems.

---

2. Definitions

“Agreement”
Any underlying IPS agreement governing Products or Services, including but not limited to: Master Services Agreements, Subscription Agreements, Statements of Work, Ordering Documents, Engagement Letters, or any other binding written or electronic agreement entered into by Customer and IPS.

“Customer Data” / “End User Data”
Data provided by or on behalf of Customer to IPS during the delivery of IPS Products or Services. Customer Data does not include Systems Data.

“Personal Data”
Any information processed by IPS on behalf of Customer that (i) identifies or could identify a natural person; or (ii) is classified as “personal data,” “personal information,” or similar terms under applicable data protection laws.

“Product”
Any IPS hardware, software, subscription service, cloud platform, or any combination thereof, including IPS OneSecure™, AI-powered services, and enterprise security solutions.

“Systems Data”
Data generated or collected in connection with Customer’s use of IPS Products, including logs, session metadata, telemetry, usage data, threat actor indicators, statistics, netflow, malware samples, and derivative intelligence.

All capitalized terms not defined herein carry the meaning assigned within the applicable Agreement.

---

3. Security Management

3.1 Information Security Program

IPS maintains a comprehensive, written, risk-based security program that:

3.1.1 is overseen by senior leadership, including the IPS Chief Information Security Officer (CISO) or designated security authority;
3.1.2 incorporates administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of Data; and
3.1.3 is appropriate to the scale, complexity, and operational risk profile of IPS’ global business and security platforms.

3.2 Personnel Security

IPS ensures that employees and contractors handling Data meet stringent security standards.

- IPS uses reputable, internationally recognized background-screening providers.
- All screening is performed in accordance with applicable laws and regional regulations.

For U.S. personnel: Screening may include county and federal criminal checks (7-year history), pending charges, employment verification, education verification, and global sanctions checks.

For non-U.S. personnel: Checks may include global watchlist verification and criminal checks where legally permissible and appropriate based on IPS risk assessment.

IPS ensures that all personnel:

- possess appropriate skills and experience for positions of trust;
- undergo security, privacy, and compliance training; and
- acknowledge and adhere to IPS information security policies.

---

4. Due Diligence on Sub-contractors

IPS may engage trusted sub-processors and service partners, subject to rigorous security oversight. IPS will:

4.1.1 conduct security due diligence prior to onboarding any subcontractor;
4.1.2 periodically assess each subcontractor's security controls to ensure compliance with these Measures;
4.1.3 enforce written contractual security requirements that are consistent with—and no less protective than—IPS' own security standards.

---

5. Physical Security

5.1 General

IPS maintains strict control over all secure physical locations ("Secure Areas") where Data is processed. IPS enforces 24/7 physical security, surveillance, and access restrictions. Physical access is revoked promptly when no longer required.

5.2 Access & Authorization Processes

IPS maintains documented processes for:

5.2.1 generating and retaining access logs for all Secure Areas, including identity, date, and time of entry;
5.2.2 maintaining continuous video surveillance at all entry and exit points, where legally permissible.

5.3 Data Centers

Where IPS operates or leverages data centers, IPS ensures alignment with industry standards such as:

- ISO/IEC 27001
- SOC 2 (SSAE 18 / ISAE 3402)
- Tiered physical access controls
- Independent third-party audits

---

6. Logical Security

6.1 System & Network Access Controls

6.1.1 IPS enforces access controls designed to:

- prevent unauthorized access;
- enforce need-to-know and least-privilege principles;
- detect and log unauthorized access attempts.

6.1.2 Each IPS user is assigned a unique account. Passwords follow industry best practices and may be required to change if risk is detected.

6.1.3 IPS performs annual access control reviews for systems storing or transmitting Data.

6.1.4 Remote access to IPS systems containing Data requires multi-factor authentication.

6.1.5 Access is revoked promptly when no longer required.

6.2 Telecommunications & Network Security

6.2.1 IPS employs enterprise-grade firewalls, segmentation, and encrypted communication channels.
6.2.2 IPS maintains intrusion detection and response capabilities to detect and investigate abnormal activity.
6.2.3 IPS enforces logical separation between corporate, development, staging, and production systems.

6.3 Malicious Code Protection

6.3.1 IPS workstations and servers run industry-standard anti-malware solutions with real-time scanning and frequent signature updates (within 24 hours of release).
6.3.2 IPS scans inbound and outbound content for malicious code at network gateways.

6.4 Data Loss Prevention

IPS deploys Data Loss Prevention (DLP) technologies and policies designed to prevent unauthorized transfer or exposure of Data.

---

7. Software Development & Maintenance

7.1 Security by Design

IPS applies secure development lifecycle (SDLC) practices, incorporating threat modeling (e.g., STRIDE), security architecture review, and code-level safeguards from inception to deployment.

7.2 Open Source & Third-Party Libraries

IPS assesses vulnerabilities associated with OSS and third-party components, integrates automated static and dynamic analysis, and uses third-party penetration testing, red-team operations, and continuous security scanning.

7.3 Change Management

IPS maintains documented change management processes and uses logically or physically isolated development, testing, and staging environments.

7.4 Vulnerability Management & Security Assessments

IPS conducts:

- quarterly internal and external vulnerability scans

- immediate scanning after material network changes
- timely remediation for critical vulnerabilities

Additionally:

7.4.1 IPS performs annual (or major-release) application security assessments aligned to OWASP, CWE/SANS, and current industry threats.
7.4.2 IPS conducts mobile application security reviews for Android, iOS, and other supported platforms.
7.4.3 IPS may use qualified third-party firms or internal experts following industry best practices.

---

8. Storage, Handling & Disposal

8.1 Data Segregation

IPS ensures logical or physical segregation of Customer Data from other customers' data.

8.2 Encryption

IPS uses strong, industry-recognized cryptographic standards:

- **AES-256** for data at rest
- **TLS 1.2+** for data in transit over public and wireless networks

8.3 Secure Disposal

IPS uses industry-recognized data destruction standards (e.g., **NIST SP 800-88**) to securely wipe or destroy media containing Personal or Customer Data.

---

9. Business Continuity & Disaster Recovery

9.1 Resilience Program

IPS maintains an enterprise resilience program that includes:

9.1.1 **Business Impact Analysis (BIA)** – annual assessment of critical systems, dependencies, risks, and recovery objectives;
9.1.2 **Incident & Crisis Management Plan** – covering escalation, communication, and coordinated response;
9.1.3 **Business Continuity Plan (BCP)** – detailing alternate work locations, remote operations, and recovery strategies;
9.1.4 **Disaster Recovery (DR) Plans** – covering system restoration, infrastructure recovery, roles, and annual testing.

9.2 Plan Content

Plans address:

- continuous operations of IPS core services;
- recovery of essential functions required to provide IPS Products;
- restoration of necessary technology, infrastructure, personnel, and Data in the event of disruption.