UpFlux

Smart Process S.A.

# INFORMATION SECURITY POLICY

Version 15 | February 24, 2026

| | |
|---|---|
| **Document Code** | PSI-UPFLUX-v15 |
| **Version** | 15 |
| **Approval Date** | February 24, 2026 |
| **Next Review** | August 24, 2026 (semi-annual cycle) |
| **Classification** | Confidential – Restricted Distribution |
| **Owner** | Cleiton Garcia – DPO / LGPD Data Protection Officer |
| **DPO E-mail** | dpo@upflux.net |
| **Approvers** | ISC (Information Security Committee) + Executive Board |

**Notice on this translation.** This is an English courtesy translation of the document originally issued in Brazilian Portuguese ("Política de Segurança da Informação – PSI-UPFLUX-v15"). The Brazilian Portuguese version is the official document, bears the electronic signatures of the Information Security Committee and the Executive Board, and shall prevail in the event of any discrepancy, divergence of interpretation or omission. Terminology note: **ISC** renders the original *CSI (Comitê de Segurança da Informação)*; **ISP** renders *PSI (Política de Segurança da Informação)*. **ANPD** is the Brazilian National Data Protection Authority and **ANS** is the Brazilian National Supplementary Health Agency. Section and item numbering has been preserved exactly as in the original.

# Table of Contents

# 1 Introduction

## 1.1 Overview

UpFlux Process Intelligence Ltda. (hereinafter “UpFlux”) is a Brazilian company specializing in Process Mining and Process Intelligence, recognized in the Gartner Magic Quadrant 2024. Operating in the B2B SaaS segment, the company provides analytical solutions for hospitals, healthcare cooperatives, industrial companies and large organizations with Procure-to-Pay (P2P) and Order-to-Cash (O2C) operations, with native integrations to TOTVS, SAP and Sankhya.

This Information Security Policy (ISP) establishes the principles, guidelines and responsibilities for the protection of the information managed by UpFlux, ensuring the confidentiality, integrity and availability of client, employee and partner data, in compliance with the LGPD (Law No. 13,709/2018), ISO/IEC 27001:2022 and other applicable regulations.

## 1.2 Objectives

- Protect UpFlux information assets against internal and external threats;
- Ensure compliance with the Brazilian General Data Protection Law (LGPD – Law No. 13,709/2018) and with ANS regulations applicable to the healthcare sector;
- Ensure business continuity and operational resilience;
- Establish standards of conduct for employees, third parties and service providers;
- Adopt ABNT NBR ISO/IEC 27001:2022 and the NIST Cybersecurity Framework as reference models for controls and risk management.

## 1.3 Management Statement

The Executive Board of UpFlux declares its unrestricted commitment to information security, allocating human, financial and technological resources to the implementation and maintenance of the controls described in this policy. Compliance with the guidelines established herein is mandatory for all employees, service providers and partners who access UpFlux systems or data.

The Senior Management Commitment Letter, electronically signed by the legal representative, forms an integral part of this document (LGPD-CARTA-v2).

## 1.4 Scope

This policy applies to:

- All UpFlux personnel (employees under Brazilian labour law, independent contractors and interns);
- Service providers and suppliers with access to the company's systems or data;
- Information assets: systems, equipment, data, documents and technological infrastructure;
- Production, staging and development environments hosted on AWS (us-east-2 region – Ohio);
- The on-premises environment of the administrative headquarters, protected by the Fortinet FortiGate 60F firewall.

## 1.5 Concepts and Definitions

**Information Asset:** any data, system, equipment or document of value to the organization.

**Data Subject:** the natural person to whom the personal data being processed refers (art. 5, LGPD).

**DPO / Data Protection Officer:** the officer in charge of personal data processing, pursuant to art. 41 of the LGPD.

**ISC:** UpFlux Information Security Committee.

**Security Incident:** an adverse event that compromises the confidentiality, integrity or availability of information.

**PAM (Privileged Access Management):** the set of controls for the management and auditing of privileged access.

## 1.6 Related Documents

- Privacy and Data Protection Policy (ADOC-LGPD-v02)
- Data Minimization and Informed Consent Policy
- Information Classification and Handling Policy (PCI v1.1)
- Password and Authentication Policy
- Secure Development Policy – DevSecOps (PS-SEC-DEVSECOPS v1.1 – February 6, 2026)
- Information Security Incident Management Policy
- Log Retention, Immutability and Availability Policy (POL-SI-LOG-001 v1.1 – February 6, 2026)
- Data Anonymization and Pseudonymization Policy
- Privacy Policy – Privacy by Design / Privacy by Default
- Data Protection Impact Assessment Policy (RIPD/DPIA)
- Server Security Policy
- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- General Privacy and Data Protection Agreements (contractual templates)
- Senior Management Commitment Letter – LGPD (LGPD-CARTA-v2)

## 1.7 Authors

This policy was prepared by the UpFlux Information Security Committee (ISC), with the participation of the DPO, the DevSecOps area and the Executive Board.

## 1.8 Disclosure and Distribution

This policy is mandatory reading for all employees and is available on the corporate intranet. A summary version may be made available to clients and partners upon formal request. Distribution of the complete document to third parties is subject to ISC authorization.

## 1.9 Version and Review

This policy is reviewed every 6 (six) months or immediately following: a relevant security incident; a significant change in infrastructure or business model; a regulatory change (LGPD, ANS, ANPD). The next scheduled review is set for August 24, 2026.

## 1.10 Information Security Maintenance

### 1.10.1 Information Security Committee (ISC)

The ISC is the collegiate body responsible for information security governance. Its duties include: approving policies, assessing risks, monitoring indicators and coordinating incident response. Composition and meetings are detailed in Annex I. Ordinary meetings are held quarterly and extraordinary meetings are convened as required.

### 1.10.2 Asset Inventory

UpFlux maintains a formal and up-to-date inventory of all information assets by means of the GLPI tool. The inventory covers hardware (workstations, physical servers, network equipment), licensed software, cloud assets (AWS resources) and critical documents. Each asset has a formally designated Asset Owner, responsible for its appropriate classification and protection, in accordance with PCI v1.1. The inventory is updated quarterly and whenever there is relevant movement of assets.

### 1.10.3 Risk Management

Security risks are assessed periodically by the ISC based on the NIST CSF framework, covering: threat identification, vulnerability assessment, impact analysis and definition of controls. The results feed the Risk Treatment Plan (RTP), which is reviewed semi-annually.

### 1.10.4 Regulatory Compliance

UpFlux operates in compliance with: the LGPD – Law No. 13,709/2018 (DPO: Cleiton Garcia | dpo@upflux.net); ANS regulations applicable in healthcare contexts; ABNT NBR ISO/IEC 27001:2022 and the NIST Cybersecurity Framework as reference frameworks for controls and management.

### 1.10.5 Training and Awareness

All employees undergo information security training upon onboarding and annually thereafter. Additional campaigns are carried out following relevant incidents or updates to this policy.

# 2 Cybersecurity

## 2.1 Authentication and Access Control

### 2.1.1 General Access Policy

a) Access to UpFlux systems and data is granted based on the least privilege principle;

b) Access accounts are individual and non-transferable;

c) Access provisioning is formalized by the responsible manager and approved by the IT department;

d) Access reviews are carried out quarterly;

e) Upon employee termination, all access is revoked within 24 hours of formal notice from HR.

### 2.1.2 Multi-Factor Authentication (MFA)

The use of MFA is mandatory on all systems that support this functionality, including: corporate e-mail (Microsoft 365), VPN, AWS console, DevOps tools and administrative panels. Activation is automatically enforced upon the employee's first access.

### 2.1.3 Privileged Access Management (PAM)

UpFlux adopts the following controls for the management of privileged access:

- Corporate password vault (Bitwarden): all institutional passwords and service secrets are managed in Bitwarden, a tool approved by the ISC. Access to the vault is controlled by MFA and audited;
- Managed identities in AWS: production workloads use IAM Roles with least-privilege permissions. Static credentials (access keys) are not used in production;
- Restricted interactive access: production servers and containers have no local users or SSH access enabled. All interactions occur through controlled CI/CD pipelines;
- Pipeline secrets: sensitive credentials are injected temporarily into the build process and are not stored in the final image;
- Emergency access (break-glass): formal procedure with automatic notification to the ISC and audit logging.

## 2.2 Endpoint Protection

f) All corporate endpoints have an EDR solution deployed: Bitdefender GravityZone Enterprise, covering 100% of managed devices;

g) Signature updates: automatic, with a maximum window of 24 hours;

h) Scheduled scans: every 5 days on all endpoints;

i) Threat Intelligence feeds: integrated with GravityZone and with the Elastic SIEM for detection based on up-to-date IOCs;

j) Detection alerts are automatically forwarded to the security team through the Elastic integration;

k) Unmanaged devices (BYOD) are not authorized to access corporate systems without formal ISC approval.

## 2.3 Firewall and Perimeter Protection

l) On-premises environment: Fortinet FortiGate 60F with rules based on network least privilege, content inspection and active IDS/IPS;

m) Cloud environment (AWS Ohio – us-east-2): protection via Security Groups, Network ACLs and WAF (Web Application Firewall). Inbound rules restricted to the minimum necessary;

n) All network configuration is managed as Infrastructure as Code (IaC) and audited by the CI/CD pipeline.

## 2.4 Penetration Testing (Pentest)

o) External and internal pentest: semi-annual (March and September), performed by an independent specialized firm;

p) After each pentest, an Action Plan with deadlines and owners is formalized by the ISC;

q) Critical vulnerabilities: remediated within 2 business days;

r) Reports classified as Restricted; available to clients under NDA.

## 2.5 Vulnerability and Patch Management

s) Automatic vulnerability scanning: every 5 days across the entire infrastructure (endpoints, servers, containers, AWS);

t) Patch management by criticality: CVSS ≥ 9.0 within 2 days; CVSS 7.0–8.9 within 14 days; CVSS 4.0–6.9 within 30 days; CVSS < 4.0 as scheduled;

u) Software Composition Analysis (SCA): integrated into the CI/CD pipeline to detect dependencies with known CVEs;

v) Container images are periodically rebuilt to incorporate security fixes.

## 2.6 Cryptography and Key Management

w) Data at rest: AES-256 in all environments (RDS, S3, EBS);

x) Data in transit: TLS 1.2 or higher in all communications;

y) Key management: AWS KMS with automatic rotation and IAM-based control;

z) Secrets and credentials: managed in Bitwarden (corporate vault) and/or AWS Secrets Manager. Storage in source code or in configuration files in clear text is prohibited;

aa) Obsolete algorithms (MD5, SHA-1, DES, SSL 3.0, TLS 1.0) are expressly prohibited.

## 2.7 Data Loss Prevention (DLP)

bb) DLP controls are applied to prevent the unauthorized transfer of Confidential and Restricted information (in accordance with PCI v1.1);

cc) The storage of confidential data on personal devices or on non-approved cloud services is prohibited;

dd) Sending client data through non-encrypted or non-corporate channels is expressly prohibited.

## 2.8 Traceability and Monitoring

### 2.8.1 SIEM and Cloud Monitoring (AWS)

UpFlux maintains full traceability by means of:

- Elastic Security (SIEM): centralization, correlation and analysis of application and infrastructure logs. Integrated with AWS CloudTrail, GuardDuty and CloudWatch;
- AWS CloudTrail: auditing of all actions in the AWS account (API calls, console access, configuration changes);
- AWS GuardDuty: detection of threats and anomalous behaviour in the AWS infrastructure;
- Amazon CloudWatch: monitoring of operational metrics and performance alerts;
- Fortinet FortiGate 60F: firewall, IDS/IPS and network traffic logs for the on-premises environment.

### 2.8.2 Log Retention

Logs are retained in accordance with the Log Retention, Immutability and Availability Policy (POL-SI-LOG-001 v1.1), with WORM protection against improper alteration and availability for audits and investigations.

### 2.8.3 Threat Intelligence

Threat Intelligence feeds are integrated with Elastic Security and Bitdefender GravityZone, enabling detection based on continuously updated IOCs (Indicators of Compromise).

# 3 Logical Security

## 3.1 Internet Access

ee) Internet access must be carried out through the corporate connection, with monitoring and content filtering;

ff) Downloading or running software not approved by IT is expressly prohibited.

## 3.2 Corporate Network Access

gg) Remote access exclusively via corporate VPN with mandatory MFA;

hh) Devices without the EDR agent installed and up to date will not be authorized on the corporate network;

ii) Authentication via Microsoft Entra ID (Azure AD), OpenID Connect and approved secure protocols.

## 3.3 Information Storage and Handling

### 3.3.1 Information Classification

All information must be classified in accordance with PCI v1.1 into the following levels: Public, Internal, Confidential and Restricted.

### 3.3.2 Authorized Storage

Confidential and Restricted information must be stored exclusively in approved systems. The use of personal devices, non-corporate clouds or unmanaged removable media is prohibited.

### 3.3.3 Transmission

All transmission of Confidential/Restricted information must use encrypted channels (TLS 1.2+). Transmission via personal e-mail or non-corporate channels is prohibited.

### 3.3.4 Production Infrastructure

The production infrastructure is hosted entirely on Amazon Web Services (AWS), us-east-2 region (Ohio, USA). Main components:

- Database: Amazon RDS (us-east-2), AES-256 at rest and TLS in transit;
- Storage: Amazon S3 with SSE-S3/SSE-KMS encryption;
- Processing: containers orchestrated via CI/CD pipeline;
- Key management: AWS KMS with automatic rotation;
- Monitoring: AWS CloudTrail, GuardDuty, CloudWatch and Elastic (SIEM).

### 3.3.5 Backup and Recovery

Backup policy with three retention tiers:

- Incremental: every 6 hours;
- Weekly: retained for 30 days;
- Monthly: retained for 6 months.

All backups are encrypted on AWS. Restoration tests are performed periodically. Recovery objectives (in accordance with the DRP): RPO of up to 4 hours; RTO of up to 8 hours.

### 3.3.6 Retention and Disposal of Client Data

Following contract termination, client data is retained for up to 90 (ninety) days, in accordance with Clause 3.2 of the General Privacy and Data Protection Agreements, after which it is definitively deleted from all environments. The client may request the export of its data prior to disposal. Disposal prevents any recovery of the information.

## 3.4 Intellectual Property

jj) Source code, documentation and developments produced at UpFlux are the exclusive property of the company;

kk) The reproduction of software without a valid licence is prohibited;

ll) The use of open source libraries must be assessed for licence compatibility and vulnerabilities, through the SCA process (DevSecOps).

## 3.5 Use of Corporate Systems

mm) Corporate systems are to be used exclusively for professional purposes;

nn) Any software installation on corporate devices requires IT approval;

oo) Access to client systems is limited to the minimum necessary, logged and justified.

## 3.6 Use of E-mail

pp) Corporate e-mail is to be used exclusively for professional communications;

qq) Confidential/Restricted information must be sent via encrypted channels or authorized platforms;

rr) Forwarding corporate e-mails to personal accounts is prohibited;

ss) Accessing personal e-mail on corporate devices during working hours is not permitted.

## 3.7 Use of Passwords

### 3.7.1 General guidelines

tt) Passwords are personal and non-transferable; the employee is responsible for actions carried out with their credentials;

uu) Passwords must not be shared under any circumstances;

vv) Minimum complexity: 8 characters, including uppercase and lowercase letters, numbers and special characters;

ww) Reuse of the last 3 password versions is prohibited;

xx) Mandatory storage in the corporate Bitwarden vault. Recording in non-encrypted files is prohibited;

yy) Account lockout after 5 consecutive invalid access attempts;

zz) Temporary passwords must be replaced upon first access.

### 3.7.2 Institutional passwords

aaa) All institutional passwords have a formally defined owner and are stored in the corporate Bitwarden vault;

bbb) Passwords are changed whenever an employee holding access is transferred or terminated.

## 3.8 Instant Messaging Software

ccc) Only Microsoft Teams is approved for corporate communications;

ddd) Personal applications (WhatsApp, Telegram) must not be used for communications involving confidential information.

## 3.9 Management of External Parties

eee) Service providers must sign an NDA before receiving any access;

fff) Third-party access is provisioned with least privilege, a defined term and monitoring;

ggg) Contracts must include security and data protection clauses in accordance with the General Privacy Agreements.

## 3.10 Physical Security

hhh) Physical access to the facilities is controlled and monitored;

iii) Corporate equipment must not be left unattended in public places;

jjj) Automatic screen lock is enabled on all devices.

## 3.11 Equipment Control

kkk) All corporate equipment is registered in GLPI before being put into use;

lll) Movement, replacement or disposal must be reported to IT for inventory update and secure disposal.

## 3.12 Control of Physical Documents

mmm) Confidential/Restricted physical documents are stored in a locked location;

nnn) Disposal by paper shredder or by a certified secure disposal service.

# 4 Internal Process Policies

## 4.1 Secure Development (DevSecOps)

UpFlux adopts a DevSecOps approach, integrating security into all phases of the SDLC, in accordance with the Secure Development Policy (PS-SEC-DEVSECOPS v1.1, effective February 6, 2026). Minimum controls per phase:

- Planning: Threat Modeling;
- Development: IDE Security Plugins (real-time insecure code alerts);
- Build/CI: SAST (static analysis) + SCA (third-party dependencies);
- Testing: DAST (dynamic analysis) in the staging environment;
- Deploy/CD: IaC validation with configuration auditing;
- Operation: continuous monitoring via Elastic SIEM and audited logs.

All production changes go through a controlled review and approval flow in the CI/CD pipeline, with full traceability.

## 4.2 Security Incident Management

UpFlux maintains a formal incident management process in accordance with the Information Security Incident Management Policy. Incidents are classified by severity and handled within defined SLAs. Incidents with potential impact on personal data are reported to the DPO, who assesses the need for notification to the ANPD and/or to data subjects, pursuant to art. 48 of the LGPD.

## 4.3 Business Continuity and DRP

UpFlux maintains an active Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP), tested annually. Objectives: RPO up to 4 hours; RTO up to 8 hours.

## 4.4 Supplier and Third-Party Management

The engagement of suppliers that will access data or systems requires: a prior security assessment, execution of an NDA/DPA, security clauses in the contract and monitoring of access. Suppliers acting as personal data processors are subject to the obligations of the LGPD.

## 4.5 Privacy and Data Protection (LGPD)

UpFlux is committed to the principles of the LGPD (Law No. 13,709/2018), adopting Privacy by Design and Privacy by Default across all products and processes. DPO: Cleiton Garcia | dpo@upflux.net. The processing of personal data occurs on a defined legal basis, with a specific purpose and data minimization. The Record of Processing Activities (ROPA) is kept up to date by the DPO.

## 4.6 Audit and Compliance

Internal security audits are performed annually by the ISC. Enterprise clients and regulatory bodies may request an audit under a formal agreement. Compliance evidence is available on demand, subject to the applicable confidentiality classifications.

## 5 Disciplinary Measures

Non-compliance with the guidelines of this ISP subjects the offender to measures proportionate to the severity of the violation:

- Formal warning;
- Suspension of system access until remediation;
- Administrative disciplinary measures, including dismissal for just cause;
- Immediate contract termination for service providers;
- Civil and/or criminal liability under applicable Brazilian legislation, including the LGPD.

The application of disciplinary measures is the responsibility of the ISC together with the Executive Board and, where applicable, the legal department. UpFlux reserves the right to notify the competent authorities (Federal Police, ANPD, Public Prosecutor's Office) upon evidence of cybercrime or of violations of the LGPD.

## Annex I – Information Security Committee (ISC)

Ordinary meetings: quarterly. Extraordinary meetings: convened in the event of relevant incidents.

| Member | Position / Role | Responsibility in the ISC |
|---|---|---|
| Cleiton Garcia | DPO / LGPD Data Protection Officer | ISC Chair \| LGPD \| dpo@upflux.net |
| Flávio Kannenberg | Director of Engineering and Information Security | Technical coordination of information security controls |
| Djiovani Douglas | IT and Information Security Operations | Risk analysis, compliance and infrastructure |
| Helton Souza | DevSecOps | Security in the SDLC and CI/CD pipeline |

** Composition in force as of February 24, 2026.*

## Annex II – Schedule of Recurring Activities

| Activity | Frequency | Next Date | Owner |
|---|---|---|---|
| ISP review | Semi-annual | August 24, 2026 | ISC / DPO |
| ISC meeting | Quarterly | May 2026 | ISC |
| External pentest | Semi-annual | March 2026 | ISC + Specialized Firm |
| Vulnerability scanning | Every 5 days | Continuous | IT / DevSecOps |
| Access review | Quarterly | May 2026 | IT / ISC |
| Information security training | Annual + on onboarding | December 2026 | ISC |
| DRP/BCP test | Annual | November 2026 | IT / DevSecOps / ISC |
| Backup + restoration test | Semi-annual | August 2026 | IT / DevOps |
| Internal information security audit | Annual | October 2026 | ISC |
| Inventory update (GLPI) | Quarterly | May 2026 | IT |

## Annex III – Revision History

| Version | Date | Type | Owner | Description |
|---|---|---|---|---|
| v1–v13 | 2020–2023 | Various | ISC | Earlier history held in the custody of the ISC |
| v14 | February 19, 2024 | Ordinary review | Cleiton Garcia | Update of technical controls; signature (SHA-256) |
| v15 | February 24, 2026 | Ordinary review | ISC / Cleiton Garcia | AWS Ohio infrastructure; Bitwarden; DevSecOps v1.1; GLPI; POL-SI-LOG-001 logs; 90-day post-contract retention; ISC composition update (Flávio Kannenberg, Djiovani Douglas, Helton Souza); 2026 schedule; LGPD formalized. |

### Electronic Signature

This document is approved by electronic signature with SHA-256 hash generation, pursuant to Provisional Measure No. 2,200-2/2001 and Law No. 14,063/2020. The signed version is the official document and has full legal validity.

Cleiton Garcia – DPO / LGPD Data Protection Officer | dpo@upflux.net
*On behalf of the Information Security Committee (ISC) and the Executive Board*
UpFlux Process Intelligence Ltda. – February 24, 2026

*The original Portuguese version of this policy was electronically signed on February 24, 2026, through Adobe Acrobat Sign, by Cleiton dos Santos Garcia (DPO), Djiovani Douglas (IT and Information Security Operations), Flavio Kannenberg (Director of Engineering and Information Security) and Helton Denis Souza (DevSecOps). The complete audit trail, including the transaction identifier and signature timestamps, remains available in the original signed document and is not reproduced in this translation.*