Information Security Policy

Public Version

Company: dex Tecnologia LTDA
CNPJ: 48.412.896/0001-42
Document Version: 3.2 - Public
Last Updated: September 2025
Next Review Date: December 2025
Contact: support@dexlabs.io

---

1. Our Security Commitment

Key Principles: • Comprehensive security framework protecting all customer data and operations • Control/data plane architecture ensuring complete customer data sovereignty • Industry-leading security standards and compliance frameworks • Continuous security monitoring and improvement programs

1.1 Security Mission

dex Tecnologia LTDA is committed to maintaining the highest standards of information security to protect our customers' data, business operations, and privacy. This policy demonstrates our dedication to implementing enterprise-grade security controls while enabling innovative data engineering solutions.

1.2 Customer Data Protection Promise

We understand that your data is your most valuable asset. Our security framework is designed around a fundamental principle: **your data remains exclusively under your control**. Through our innovative control/data plane architecture, customer business data never leaves your own cloud environment, ensuring complete data sovereignty and regulatory compliance.

1.3 Our Unique Architecture

dex operates using a sophisticated control and data plane separation that provides unmatched security and compliance benefits:

Control Plane (dex-managed): Our platform manages orchestration, workflow coordination, user interfaces, and system monitoring without ever accessing your business data.

Data Plane (customer-controlled): All your sensitive business data remains exclusively within your own cloud infrastructure (Amazon S3, Google BigQuery, Google Cloud Storage). We never store, cache, or process your business data on our systems.

This architectural approach ensures that your data enjoys the same security protections as your existing cloud infrastructure while benefiting from our advanced data engineering capabilities.

---

2. Security Standards and Compliance

Our Commitments: • AWS Well-Architected Security Pillar implementation • OWASP security guidelines adherence • Target SOC 2 Type I certification by Q2 2026 • Full GDPR and LGPD compliance for international operations • Regular third-party security assessments

2.1 Industry Standards

We align our security practices with globally recognized frameworks including the AWS Well-Architected Security Pillar, OWASP Security Guidelines, and ISO 27001 principles. Our approach ensures comprehensive security coverage while preparing for formal compliance certifications.

2.2 Regulatory Compliance

dex maintains full compliance with applicable data protection regulations including GDPR for European customers and LGPD for Brazilian operations. Our architectural approach simplifies compliance by ensuring your data processing occurs within your own jurisdiction and security controls.

2.3 Continuous Certification

We are actively pursuing SOC 2 Type I certification to provide third-party validation of our security controls. Through our AWS partnership, we inherit numerous enterprise-grade security certifications and maintain alignment with global security standards.

---

3. Access Control and Authentication

Security Features: • Multi-factor authentication required for all system access • Role-based access control with least privilege principles • Customer-controlled access through dual-layer security model • Regular access reviews and automated provisioning/deprovisioning

3.1 Strong Authentication

Every interaction with dex systems requires multi-factor authentication, ensuring that only authorized individuals can access platform capabilities. We implement zero-trust principles where authentication is required for every system interaction.

3.2 Customer-Controlled Access

Our unique architecture means that even after authenticating with dex, users must also satisfy your organization's own cloud security requirements to access data and execute operations. This dual-layer approach provides enhanced protection through customer-controlled security policies.

3.3 Privileged Access Management

Access to sensitive system functions follows strict approval processes with regular reviews to ensure continued appropriateness. We implement the principle of least privilege throughout our systems, ensuring users receive only the minimum access necessary for their functions.

---

4. Data Protection and Encryption

Encryption Standards: • Industry-standard encryption for all data in transit and at rest • Advanced key management with automated rotation • Customer data sovereignty with zero data persistence on dex systems • Complete audit trails for all data operations

4.1 Comprehensive Encryption

All data communications utilize TLS 1.3 encryption, providing strong protection against interception. Customer credentials and sensitive information receive additional encryption layers using advanced cryptographic techniques.

4.2 Your Data Stays Yours

Our architectural approach ensures that your business data never leaves your cloud environment. Data flows directly from third-party APIs (like TikTok Shop) into your own storage systems, with dex orchestrating the processing without ever storing or caching your information.

4.3 Audit and Transparency

Complete audit trails document all data operations, providing full transparency into how your data is accessed and processed. These logs support compliance requirements and incident investigation capabilities.

---

5. Infrastructure Security

Technical Safeguards: • Enterprise-grade cloud infrastructure with multi-region deployment • Advanced threat detection and monitoring systems • Automated security scanning and vulnerability management • Container security with image scanning and validation

5.1 Cloud-Native Security

Our infrastructure leverages AWS enterprise security controls, including native firewalls, DDoS protection, and comprehensive monitoring systems. Multi-region deployment provides both security and operational resilience.

5.2 Automated Security

Continuous security monitoring provides real-time threat detection and automated response capabilities. Our development pipeline includes automated security scanning to identify and address vulnerabilities before they reach production systems.

5.3 Container and Application Security

All applications run in secure containerized environments with comprehensive image scanning and validation. Our development practices follow secure coding guidelines with regular security assessments.

---

6. Incident Response and Monitoring

Response Capabilities: • 24/7 security monitoring and alerting systems • Rapid incident response with defined escalation procedures • Transparent customer communication during security events • Post-incident analysis and improvement processes

6.1 Continuous Monitoring

Our security operations center provides around-the-clock monitoring of all systems and infrastructure. Real-time alerting ensures rapid response to potential security events or operational issues.

6.2 Incident Response

We maintain comprehensive incident response procedures with clear escalation paths and communication protocols. Customers are notified promptly of any

incidents that might affect their data or services.

6.3 Transparency and Communication

We believe in transparent communication about security events and regularly share relevant security updates with our customers. Post-incident analysis helps us continuously improve our security posture.

---

7. Employee Security and Training

Human Security: • Comprehensive background verification for all personnel • Regular security training and awareness programs • Strict access controls and monitoring for internal systems • Remote work security best practices implementation

7.1 Personnel Security

All team members undergo background verification and comprehensive security training before accessing any customer-related systems. Ongoing training ensures awareness of current threats and best practices.

7.2 Internal Access Controls

Internal access to systems follows the same strict authentication and authorization requirements as customer access. Regular reviews ensure that access remains appropriate and necessary.

7.3 Security Culture

We foster a security-conscious culture through regular training, open communication about security concerns, and continuous improvement of our security practices based on team feedback and industry developments.

---

8. Vendor and Partnership Security

Third-Party Management: • Rigorous security assessments for all partnerships • Comprehensive API security for third-party integrations • Clear data processing agreements and responsibilities • Regular review and validation of vendor security practices

8.1 Strategic Partnerships

Our partnership with AWS provides access to enterprise-grade security infrastructure and compliance certifications. We carefully evaluate all technology partnerships to ensure they meet our security standards.

8.2 API Integration Security

Third-party API integrations (including e-commerce platforms) implement OAuth 2.0 security with comprehensive logging and monitoring. We access only the minimum data necessary for service delivery.

8.3 Data Processing Agreements

Clear agreements define data processing responsibilities and security requirements for all partnerships, ensuring consistent protection standards across our entire service ecosystem.

---

9. Business Continuity and Availability

Resilience Features: • Automated backup systems with encrypted storage • Multi-region deployment for high availability • Disaster recovery testing and validation procedures • Scalable architecture supporting business growth

9.1 High Availability Design

Our infrastructure is designed for continuous availability with automatic failover capabilities and load distribution across multiple regions. This ensures service availability even during infrastructure maintenance or unexpected events.

9.2 Data Protection and Recovery

Comprehensive backup systems with encryption and cross-region replication provide protection against data loss. Regular testing validates our ability to recover quickly from various failure scenarios.

9.3 Scalability and Performance

Our security controls are designed to scale automatically with business growth, ensuring that security protection remains effective as usage increases and new capabilities are added.

10. Privacy and Data Rights

Privacy Commitments: • Privacy by design implementation across all systems • Comprehensive data subject rights support (access, portability, deletion) • Global privacy regulation compliance (GDPR, LGPD, CCPA) • Transparent data processing practices with customer control

10.1 Privacy by Design

Privacy considerations are integrated into every aspect of our system design and operations. We implement data minimization, purpose limitation, and storage limitation principles to ensure responsible data handling.

10.2 Individual Rights

We provide comprehensive support for individual data rights including access, portability, and deletion requests. Our systems include automated procedures to fulfill these rights efficiently and completely.

10.3 Global Compliance

Our privacy practices comply with major global privacy regulations including GDPR, LGPD, and CCPA. Regular assessments ensure continued alignment with evolving privacy requirements.

11. Security Assessment and Validation

Validation Programs: • Regular third-party security assessments and penetration testing • Continuous vulnerability scanning and management • Compliance audits and certification processes • Customer security reviews and documentation support

11.1 Independent Validation

Annual third-party security assessments provide independent validation of our security controls and identify opportunities for enhancement. We engage qualified security firms to conduct comprehensive penetration testing.

11.2 Continuous Improvement

Regular security reviews and assessments inform continuous improvement of our security posture. We actively monitor threat landscapes and update our controls to address emerging risks.

11.3 Customer Collaboration

We work closely with customers who require security assessments, providing documentation and support for their vendor security review processes. Transparency in our security practices builds trust and enables informed decisions.

12. Contact and Support

12.1 Security Team

For security-related questions, concerns, or incident reporting:

- **Email:** support@dexlabs.io
- **Website:** https://www.dexlabs.io
- **Business Hours:** Standard support during business hours, emergency response available 24/7

12.2 Security Assessments

Organizations requiring security assessments or additional documentation can request information through our standard support channels. We provide comprehensive security documentation to support customer compliance and vendor management requirements.

12.3 Compliance and Privacy

For compliance-related inquiries, data processing questions, or privacy concerns:

- **General Inquiries:** support@dexlabs.io
- **Privacy Requests:** Include "Privacy Request" in subject line
- **Company Information:** dex Tecnologia LTDA, CNPJ: 48.412.896/0001-42

Policy Updates and Transparency

This security policy is reviewed quarterly and updated as needed to reflect changes in our security practices, regulatory requirements, or business operations. We notify customers of material changes to our security practices and maintain transparency about our ongoing security improvements.

For the most current version of this policy and additional security information, visit our website at https://www.dexlabs.io/security.

This policy demonstrates dex's commitment to maintaining the highest standards of information security while enabling innovative data engineering solutions for our customers.

Last Updated: September 2025
Next Review: December 2025
Document Classification: Public
Distribution: Available to all customers, prospects, and the general public