Kiteworks

COMPLIANCE BRIEF

FOR COMPLIANCE AND SECURITY LEADERS

Kiteworks Supports Puerto Rico's Data Privacy and Cybersecurity Acts

One Platform Mapped to Two Puerto Rico Compliance Acts: Breach Reporting and Government Cybersecurity

Puerto Rico | Data Privacy | Cybersecurity

Solution Highlights

- Encryption at Rest and in Transit
- Data Policy Engine (ABAC/RBAC)
- AI-Based Intrusion and Anomaly Detection
- Real-Time SIEM Feed of Audit Log
- Web Email with Tracking and DRM

Puerto Rico enforces two distinct data protection and cybersecurity acts, each with its own enforcement authority. The Citizen Information Security of Information Banks Act (Act No. 111 of 2005, 10 L.P.R.A. § 4051 et seq.) requires any entity that owns or has custody of a database containing personal information of Puerto Rico residents, along with any reseller or access provider that handles that data, to notify affected citizens after a security breach within a strict reporting window, backed by Department of Consumer Affairs (DACO) fines of $500 to $5,000 per violation. The Government Cybersecurity Act (Act No. 40 of 2024, 3 L.P.R.A. §§ 10121 et seq.) requires every Executive Branch agency, along with its contracted service providers, to build a zero trust security program under PRITS, the Puerto Rico Innovation and Technology Service, with daily fines for general non-compliance and steeper per-violation fines for obstruction, negligence, or bad faith. Kiteworks supports organizations working toward compliance with both acts. Here's how:

Two Acts at a Glance

Citizen Information Security of Information Banks Act (Act 111-2005)
10 L.P.R.A. § 4051 et seq. Enforced by DACO. Ten-day breach reporting window; fines of $500 to $5,000 per violation.

Government Cybersecurity Act (Act 40-2024)
3 L.P.R.A. §§ 10121 et seq. Enforced by PRITS. Zero trust security mandate for Executive Branch agencies; fines of $50 to $100 per day per incident, rising to $1,000-$5,000 per violation for willful non-compliance.

Encrypted, Authenticated Notification Within DACO's Ten-Day Window

Encryption in transit applies TLS 1.3/1.2 with AES-256, and encryption at rest double-encrypts stored files, protecting the channels an entity uses to notify Puerto Rico residents after a breach under Article 3. AI-based intrusion and anomaly detection helps an entity identify a breach event as early as possible. Web Email satisfies Article 4's authenticated-electronic-means requirement under the Digital Signatures Act, reinforced by native email-based one-time-password authentication. User authentication and file access logging give resellers and access providers the evidentiary trail Article 3 requires to show they detected and escalated a breach to the database owner, and the real-time SIEM feed of audit log pushes that data to QRadar, LogRhythm, ArcSight, and Splunk in real time. Log timeliness appends entries immediately, and compliance reports from the Data Policy Engine give compliance teams exportable documentation to reconstruct the detection timeline Article 3's non-extendable ten-day reporting deadline demands, while tracking of sent email messages proves each notice reached its recipient.

Zero Trust Architecture and Continuous Monitoring for PRITS-Governed Agencies

Encryption at rest, encryption in transit, and the FIPS 140-3 validated encryption option (NIST certificate #4980) meet the Government Cybersecurity Act's mandate to protect confidential information, including PII, in every state. The Data Policy Engine enforces ABAC and RBAC aligned with the principle of least privilege, while the embedded web application firewall, network firewall, antivirus scanning, and advanced threat prevention block malware and unwanted programs at the perimeter. AI-based intrusion and anomaly detection, paired with embedded managed detection and response connecting to Kiteworks' 24x7 security staff, supports the continuous monitoring PRITS requires of Executive Branch agencies and their contracted service providers. The real-time SIEM feed of audit log and comprehensive audit logs give PRITS the evidence base for quarterly risk assessments and incident reporting, legal hold and eDiscovery access controls preserve records for investigation, and Kiteworks' FedRAMP High (In Process) status, alongside FedRAMP Moderate Authorization since 2017, supports the federal security obligations placed on contracted service providers.

Across both Puerto Rico acts, Kiteworks operates as a single governed platform spanning encryption, access governance, and audit intelligence. Encryption in transit and at rest, authenticated Web Email, and real-time audit logging give entities the protected, evidenced notification chain the Citizen Information Security of Information Banks Act requires within its ten-day window, giving DACO the timestamped record it needs to confirm compliance. The Data Policy Engine, embedded threat defenses, FIPS 140-3 validated encryption, and continuous SIEM-fed monitoring give PRITS-governed agencies and their contracted service providers the zero trust architecture the Government Cybersecurity Act mandates, while legal hold and eDiscovery access controls preserve records for investigation and the real-time SIEM feed of audit log keeps PRITS informed as events happen. Organizations still own the process-level obligations behind each act, including managing contracts, developing formal cybersecurity programs, and filing statutory reports to DACO and PRITS, but Kiteworks gives them a technically grounded foundation for meeting both.

See How Kiteworks Maps to Puerto Rico's Privacy and Cybersecurity Acts

www.kiteworks.com

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.