pivotree
cyber security

Pivotree Security White Paper

Pivotree is committed to maintaining the highest standards of security, ensuring compliance with industry-leading frameworks such as PCI DSS, SOC 2, and ISO 27001. Our comprehensive security posture is designed to protect our customers' data, mitigate risks, and uphold trust across all aspects of our business. This white paper details our security approach, covering organizational, physical, infrastructure, data, and operational security, among other key areas.

Organizational Security

Pivotree fosters a security-first culture by implementing strong governance, risk, and compliance (GRC) programs. Our security policies align with global standards, and we regularly train employees on security best practices. The leadership team ensures that security objectives are integrated into business strategies, promoting a proactive approach to cybersecurity.

Security Risk Assessment Framework

Pivotree has embedded a robust Security Risk Assessment Framework across all departments and scopes of work. This framework ensures that risk identification, evaluation, and mitigation strategies are integrated into every operational function. Through periodic risk assessments, threat modeling, and compliance reviews, we proactively address security vulnerabilities and enhance resilience. Our approach is data-driven and aligns with industry best practices to safeguard assets and maintain regulatory compliance.

Physical Security

To safeguard physical assets, Pivotree enforces strict access controls, surveillance, and security monitoring across all office and data center locations. Data centers housing critical infrastructure comply with Tier III+ standards, ensuring resilience against unauthorized access and environmental threats.

Infrastructure Security

Pivotree employs a multi-layered security model to protect our IT infrastructure, including network segmentation, firewalls, intrusion detection/prevention systems (IDS/IPS), and regular vulnerability assessments. Our cloud-based environments are secured through best-in-class configurations and automated security monitoring.

Data Security

Protecting customer data is a top priority. We use encryption in transit and at rest, robust data loss prevention (DLP) mechanisms, and stringent access controls to ensure the confidentiality, integrity, and availability of sensitive information. Pivotree also enforces data classification policies to prevent unauthorized exposure.

Identity and Access Control

We implement a zero-trust framework, enforcing least-privilege access across all systems. Multi-factor authentication (MFA), single sign-on (SSO), and role-based access control (RBAC) are mandatory measures to prevent unauthorized access. Regular access reviews ensure compliance with security policies.

Operational Security

Our operational security framework includes continuous monitoring, endpoint protection, and regular security assessments. We leverage Security Information and Event Management (SIEM) systems to detect and respond to threats in real time. Secure software development lifecycle (SDLC) practices ensure applications remain resilient to cyber threats.

Incident Management

Pivotree maintains a well-defined Incident Response Plan (IRP) to handle security incidents effectively. Our Security Operations Center (SOC) operates 24/7, using automated alerts and forensic analysis tools to quickly identify and mitigate threats. Regular tabletop exercises ensure our teams are prepared for any security event.

Vendor Management

Pivotree maintains a rigorous vendor risk management program, ensuring third-party partners meet our stringent security requirements. We conduct thorough due diligence, enforce contractual security obligations, and perform periodic audits to assess vendor security controls.

Customer Controls for Security

We empower customers with security controls to manage their own environments. Pivotree provides security configuration options, logging and monitoring tools, and guidance on implementing security best practices to enhance protection and compliance in customer-managed systems.

Security is at the core of Pivotree’s operations, ensuring compliance, resilience, and trust. By adhering to the highest standards in cybersecurity and continuously improving our security posture, we enable businesses to operate securely and efficiently in an increasingly digital world.

For further details on Pivotree’s security practices or to inquire about our compliance certifications, please contact our security team at [security@pivotree.com].