Security & Data Protection

We Are Relentless About Protecting Data

At Kiken Technologies, protecting customer information is not simply a requirement—it is a core part of our mission.

As a company focused on cybersecurity, data protection, and information security, we understand that trust is earned through transparency, accountability, and strong security practices. Data protection is integrated into every aspect of our operations, from product design and infrastructure management to employee training and vendor oversight.

Our security-first approach helps ensure that customer information remains protected while supporting the confidentiality, integrity, and availability of the systems and services we provide.

Security by Design

Kiken Technologies designs and operates its systems using secure cloud-based architectures and industry-recognized security principles.

We continuously evaluate our environment, processes, and technologies to identify opportunities for improvement and to reduce security risks. Our security program incorporates recognized cybersecurity frameworks, industry best practices, and risk-based decision-making processes to support a strong security posture.

Security and privacy considerations are integrated throughout our operational processes, product development lifecycle, and service delivery practices.

How We Protect Your Data

To support our commitment to security, privacy, and operational resilience, Kiken Technologies has implemented a comprehensive Information Security Program that includes:

Continuous Security Monitoring

We continuously review and improve our security controls, policies, and procedures to help ensure that customer information remains protected against evolving threats.

Employee Security Awareness

All employees receive security and privacy training:

- During onboarding
- Throughout their employment
- Through ongoing awareness initiatives
- Through annual security training and policy reviews

Our team is trained to recognize and respond to security risks, phishing attempts, social engineering attacks, and other cyber threats.

Vendor Risk Management

We evaluate third-party vendors and service providers before granting access to systems or data.

Vendor agreements may include security, privacy, confidentiality, and data protection requirements designed to help safeguard customer information.

Operational Security Integration

Security and privacy controls are embedded throughout our standard operating procedures and day-to-day business processes to help ensure consistent protection of information assets.

Threat Detection and Response

Kiken Technologies utilizes advanced monitoring, detection, and response technologies to identify, investigate, and respond to potential security events and suspicious activity within our environment.

Vulnerability and Risk Management

We continuously assess our systems for vulnerabilities and security weaknesses, prioritize remediation efforts, and implement corrective actions designed to reduce overall cyber risk exposure.

Security Controls and Safeguards

Our defense-in-depth security strategy includes administrative, technical, and physical safeguards designed to protect customer data and business systems.

Key security controls include:

Governance & Policy Management

- Information Security Policies
- Acceptable Use Policies
- Data Protection Standards
- Risk Management Processes
- Security Governance Reviews

Workforce Security

- Background screening where permitted by law
- Role-based access controls
- Least-privilege access principles
- Ongoing access reviews
- Security awareness training

Data Protection

- Information classification procedures
- Data handling standards
- Data retention and disposal policies
- Encryption technologies where appropriate
- Secure data storage practices

Infrastructure Security

- Endpoint protection and monitoring
- Network security controls
- Firewall management
- Threat detection and monitoring systems
- Secure cloud infrastructure

Vulnerability Management

- Vulnerability assessments
- Patch management processes
- Security updates and maintenance
- Configuration management

Application Security

- Secure Software Development Lifecycle (SSDLC)
- Security testing and validation
- Change management processes

- Code review procedures
- Development security standards

Incident Response

- Information Security Incident Response Program
- Security event monitoring and escalation procedures
- Investigation and remediation processes
- Communication and reporting procedures

Business Continuity & Resilience

- Business Continuity Planning (BCP)
- Disaster Recovery Planning (DRP)
- Data backup procedures
- Recovery testing and validation

Our Commitment

Cybersecurity is an ongoing process, not a one-time project.

Kiken Technologies continually evaluates emerging threats, evolving technologies, and industry best practices to strengthen our security posture and improve the protection of customer information.

Our goal is simple: provide our customers with confidence that their information is handled responsibly, protected diligently, and secured using modern cybersecurity principles and best practices.

Contact Us

If you have questions regarding our security practices, privacy controls, or information protection measures, please contact:

Kiken Technologies

Email: Sales@KikenTechnologies.com

Website: https://KikenTechnologies.com

For security-related inquiries, please include "Security Inquiry" in the subject line.