Security and Compliance at CiraApps

CIRAAPPS

How Cira Apps Keeps Customers' Data Secure

As cyber threats continue to evolve, Cira Apps remains committed to upholding the highest standards of data protection and investing in ongoing security improvements to stay at the forefront of cloud security best practices.

By implementing these robust security measures and maintaining compliance with stringent regulations and standards like GDPR, SOC 2, and ISO27001, Cira Apps provides customers with the assurance that their data will remain private and secure within the CiraSync platform. Enterprises can confidently use CiraSync across their organizations, knowing that Cira Apps takes extensive precautions to safeguard their sensitive information.

Great Software! Great Customer Support!

The software works amazingly! It allows us to easily edit user information company-wide! It's easy to use and navigate. Not to mention, the customer support is great!

Jessica R.,
IT Specialist

GDPR Compliance

CiraSync is compliant with General Data Protection Regulation (GDPR), a comprehensive Personal Data Protection law that became enforceable in May 2018, and it is still year to date in the European Economic Area (EEA) and the UK. The GDPR sets a new standard in terms of the safe keeping and confidentiality assurance of Personal Data under Processing that companies must assure. To ensure a compliant mode of operation, Cira Apps has undergone a Corporate Data Protection Impact Assessment, to assert what in both its operation and IT Landscape was compliant with the legal requirements as what was not; having them defined and implemented adequate mitigation actions which led to a compliant mode of operation. These include, yet are not limited to, having implemented Data Processing Agreements with all customers (the Controllers) and vendors (the Processors), having established processes to honor the exercise of Rights by the Data Subjects; maintaining detailed Records of Processing Activities. The company has also appointed a Data Protection Officer to oversee compliance towards applicable Personal Data Protection legislation.

SOC 2 Type 2 and ISO 27001 Compliance

In addition to the GDPR, CiraSync has achieved a SOC 2 Type II report after undergoing rigorous third-party audits. SOC 2 is a widely recognized auditing standard developed by the American Institute of CPAs (AICPA), which evaluates a service provider's controls related to security, availability, processing integrity, confidentiality, and privacy. The Type II designation indicates that these controls have been validated over an extended period. Cira Apps' completion of SOC 2 Type II audit demonstrates its strong commitment to data security.

Additionally, the Corporate Data Protection Impact Assessment which led to a compliant mode of operation with the GDPR, had its IT Security Assessment performed in view of ISO27001 controls and adequate technological mitigation actions were implemented in line with these requirements.

For customers based in the EEA and the UK, CiraSync uses Microsoft Azure data centers located in the European Union (EU) to store and process all customer data (including Personal Data pertaining to resident natural Persons in the EEA). This ensures that Personal Data pertaining to residents in the EEA and the UK is not transferred outside of the EEA and the UK. Microsoft Azure complies with a broad portfolio of international and industry-specific standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2.

As a Software-as-a-Service platform built on Microsoft Azure, CiraSync integrates tightly with Azure's security features and utilizes the Azure Consent Framework for authentication and authorization. The Azure Consent Framework ensures that users have full control over which applications can access their Microsoft 365 data and requires explicit consent before granting access. CiraSync does not store any Microsoft 365 login credentials. All subscriber data is encrypted and stored securely in the Microsoft Cloud, taking advantage of Microsoft's robust physical and logical security measures.

Key Security Features

Some key security features and practices Cira Apps has implemented for CiraSync include:

Single Sign-On (SSO) Support: CiraSync supports single sign-on through Azure Active Directory, Active Directory Federation Services (ADFS), Okta, OneLogin, and other identity providers. SSO allows users to access CiraSync with their existing corporate credentials and enables IT administrators to centrally control authentication policies.

Data Encryption: All customer data is encrypted at rest using AES-256 bit encryption and is encrypted in transit using Transport Layer Security (TLS). Encryption keys are stored in the Azure Key Vault, a secure key management service that leverages FIPS 140-2 validated hardware security modules to protect cryptographic keys.

Multi-Factor Authentication (MFA): CiraSync requires multi-factor authentication (MFA) for all administrator access to the system. MFA provides an extra layer of security beyond usernames and passwords by requiring administrators to provide a second authentication method, such as a code from an authenticator app or a hardware security key. Detailed Audit.

Logging & Monitoring: CiraSync logs all system activities and configuration changes for auditing purposes. All logs are always centrally collected, monitored, and analyzed to detect suspicious activities or potential security breaches. Cira Apps' security team investigates and responds to any security alerts on a continuous basis.

Granular Administrator Permissions & User Provisioning: CiraSync provides a granular permissions model that allows companies to designate multiple administrators and grant them specific privileges. Administrators can be limited to managing only certain features or a subset of users. User provisioning can be automated through integration with Azure AD or other identity management systems.

Automatic Offboarding of User Access: When an employee leaves the company or no longer requires access to CiraSync, their access is automatically revoked through integration with the company's identity management system. This ensures that former employees cannot continue to access sensitive data.

Geographically Distributed Data Centers with Failover and Backup: CiraSync is hosted in geographically distributed Azure data centers to ensure high availability and disaster recovery. Customer data is replicated across multiple data centers within a region. In the event of a data center outage, CiraSync automatically fails over to a secondary data center to minimize downtime. Regular data backups are performed and stored in geographically separate locations.
Penetration Testing by Independent Security Firms: Cira Apps engages independent third-party security firms to conduct regular penetration testing of the CiraSync application and infrastructure. Penetration testing simulates real-world attacks to identify any potential vulnerabilities in the system. Any identified security issues are promptly remediated based on severity.

About Cira Apps Ltd.

Cira Apps Ltd. is a SaaS company with solutions that enhance Microsoft 365 productivity for iPhone and Android business users. CiraSync, the flagship product, is used by more than 300,000+ users at 12,500+ companies around the globe to automate the syncing of contacts and shared calendars to business smartphones.

The company is headquartered in Austin, Texas.

Learn more at www.cirasync.com.

CIRAAPPS