Secure Backup | Smart Recovery

SECURITY OVERVIEW

Trusted by 20,000+ Customers

Never Face Data Loss Again!

CloudAlly provides a secure cloud backup solution with internationally recognized accreditation for information security management.

Audit-ready Backup: ISO 27001 Certified, HIPAA and GDPR Compliant

- CloudAlly is ISO 27001 certified, an internationally recognized accreditation for information security management.
- We are HIPAA and GDPR compliant and can provide a BAA Agreement upon request. Our GDPR compliance includes adherence to its data sovereignty, data security, and data processing requirements, among others. Read more about our GDPR mandate.
- CloudAlly is certified Microsoft Platform Ready and has been tested and verified secure by Amazon Web Services, Salesforce.com, and Google Apps.
- CloudAlly is also part of the Cloud Security Alliance STAR (Security, Trust, and Assurance Registry) program using CSA's Cloud Controls Matrix (CCM). CCM is a framework of cloud-specific security controls that ensures participating organizations adhere to leading industry standards, best practices, and regulations.
- CloudAlly provides detailed Security and System Audit logs with a filterable log of both user activities such as records of sign-ins, settings, and permissions changes, as well as system activities such as completed scheduled backups and user-initiated recovery operations.

HIGHLIGHTS

- ISO 27001 certified, HIPAA and GDPR compliant
- AES-256-bit encryption at-rest and SSL (HTTPS) in-flight
- OAuth access, SAML-Okta and 2FA support, IP restrictions
- PCI compliant payment processor
- Certified by Microsoft, Salesforce.com, Google and AWS
- 9+ global data centers and BYOS support

Secure Backup | Smart Recovery

SECURITY OVERVIEW

Trusted by 20K+ Customers

End-to-end Data Encryption and Sovereignty: AES-256 bit and SSL

- All data is stored in Amazon S3 storage and encrypted using advanced AES-256-bit encryption algorithms.
- Transmitted data is encrypted and secured using SSL (HTTPS) enabled servers.
- Easily comply with data sovereignty regulatory laws and choose your backup data center location from a growing network of multiple AWS data centers in the US, Canada, Europe (France, Germany, and Ireland), the UK, Africa (South Africa) and Asia Pacific (Australia and Japan).
- Adhere to data regulations with support for Salesforce data anonymization for Sandbox Seeding.
- Choose to BYOS (Bring Your Own Storage). Back up to your own AWS S3 storage and/or AWS S3 compatible Google Cloud Platform and Azure Blob storage. This provides flexible storage options to meet all industry, compliance, and legal requirements.

Stringent Application Security and Access: OAuth, 2FA, SAML-Okta

- CloudAlly uses industry-standard OAuth for permission-based access when possible, eliminating the need to enter or store user credentials on the CloudAlly system. The OAuth "token" limits access to exactly what CloudAlly needs to do and doesn't provide general access to your account. You can revoke authorization at any time.
- We also support SAML authentication via the leading industry provider Okta in addition to OAuth for secure authentication.
- Choose to add mandatory or optional Two-Factor Authentication (2FA) to your CloudAlly account using any industry-standard authentication app.
- We support multi-admin access with fine-grained access management per admin.
- Improve security and prevent unauthorized access with IP restrictions using allow and deny IP lists. Restrict backup/restore requests to company-approved IP addresses.
- Payment processing, including credit card information, is hosted by our payment processor, which is fully PCI compliant. No payment information is handled or stored on the CloudAlly system.

Customer-controlled Data: Access, Retention, and Deletion

- Data Access: Customer backup data is not accessible directly; it can only be accessed using the CloudAlly platform. CloudAlly backups can only be activated, deactivated, or restored by the customer's Data Administrator. Internal CloudAlly staff do not have access to customer data, and only a limited number of core team members have access to production keys based on a "need to know" policy for problem resolution.
- Data Retention: All backed up data is retained as long as you maintain your CloudAlly subscription. After deletion by customer, the customer's backup data is marked as deleted and kept for a grace period. Via a Support request, the customer can change their default data retention period. We recommend downloading the data prior to de-activation if you want to retain the backed-up data for local archiving.