Title: AcmeCloud Internal Policies
Last Updated: March 2025

Data Privacy Policy

AcmeCloud is committed to protecting customer and employee data. All personal data is processed in accordance with applicable data protection laws, including GDPR and CCPA. Customer data is encrypted at rest and in transit using industry-standard encryption protocols. Access to sensitive data is restricted to authorized personnel only and reviewed on a quarterly basis.

Information Security Policy

All employees must use company-approved devices when accessing internal systems. Multi-factor authentication is required for all production systems. Passwords must be changed every 90 days and may not be reused. Any suspected security incident must be reported to the Security Operations team within 24 hours.

Remote Work Policy

Employees may work remotely up to three days per week with manager approval. Remote workers must ensure a secure internet connection and may not use public Wi-Fi without a VPN. Company-issued laptops must be locked when unattended.

Data Retention Policy

Customer data is retained for a maximum of five years unless otherwise required by law. Backup data is stored for 30 days. Upon termination of service, customer data is deleted within 60 days.