SAZEB TECH
CONSULTING

Best Practices for Securing Data in the Cloud

Protecting Sensitive Information in the Digital Age

www.sazebtech.com

Encrypt Data in Transit and At Rest

Encryption is Key

- **In Transit:** Use SSL/TLS encryption to protect data while it's being transmitted across networks.

- **At Rest:** Encrypt stored data in the cloud to safeguard it from unauthorized access, even if there's a breach.

Tip: Always use strong encryption standards like AES-256 to secure sensitive data.

Implement Access Controls and Authentication

Control Who Accesses Your Data

- Use Role-Based Access Control (RBAC) to assign access rights based on the principle of least privilege.
- Implement Multi-Factor Authentication (MFA) to ensure that only authorized users can access sensitive information.

Tip: Regularly review access logs and permissions to avoid excessive access.

Regularly Back Up Data and Test Recovery Plans

Ensure Business Continuity

- Schedule regular backups of critical data to avoid data loss.
- Test disaster recovery plans periodically to ensure data can be restored efficiently in case of an emergency.
- **Tip:** Store backups in geographically dispersed locations to prevent single-point failures.

Stay Updated with Compliance and Security Standards

Follow Regulations & Standards

- Ensure your cloud environment complies with relevant regulations such as **GDPR, HIPAA,** or **CCPA.**
- Adhere to industry security standards like **ISO 27001** and **NIST** to ensure data security.

Tip: Work with your cloud provider to ensure they also meet these compliance requirements.

SAZEB TECH
CONSULTING

Want to know more about securing your cloud data? Let's talk about how we can help your organization implement these best practices!

#CloudSecurity #DataProtection #Encryption #Cybersecurity #CloudComputing #TechBestPractices