Securafy™

ARE YOU REALLY SECURE IN THE CLOUD?

BEST PRACTICES TO PROTECT YOUR BUSINESS

For growing businesses like yours, the cloud offers flexibility, cost-effectiveness and efficiency. However, you can't make the most of these benefits without ***cloud security best practices***. Let's explore how you can build strong security in the cloud.

Best Practices to Protect Your Business

1

Data encryption:

Protects your valuable business assets and ensures they remain confidential while shielding your business from costly breaches and reputational damage.

2

Identity and access management (IAM):

Limits access and ensures only those with proper clearance can access business-critical data. By implementing multi-factor authentication (MFA), you further increase your business security.

3

Regular security audits:

Identifies vulnerabilities in your IT infrastructure before they're exploited by malicious users. Think of them as preventative maintenance for your business's IT.

4

Compliance checks:

Allow you to maintain compliance with industry rules and data privacy laws. This helps you enhance customer trust and avoid costly fines.

5

Incident response planning (IRP):

Outlines the steps you should take in the event of a security incident. The main goal of an IRP is to minimize damage and maintain business continuity.

6

Disaster recovery (DR):

Helps your business quickly recover from an IT failure, cyberattack or natural disaster. A robust DR plan reduces costly downtime and data loss, ensuring business continuity.

Adopting the right best practices is the first step to securing your business, but the real advantage comes from ***partnering*** with an expert IT provider who knows how to strengthen your cloud security posture.

Contact us today to get started.