

CLOUD SECURITY POLICY

Effective	Date	
Reviewed by	The	
next scheduled review date		
Supersedes		All previous similar policies
Approved by		
Date Approved		

1.1 Purpose

This policy defines the security standards and practices for using cloud computing services within our company to ensure data confidentiality, integrity, and availability.

1.2 Scope

This policy applies to all employees, contractors, and third parties who access or use cloud services on behalf of the company and to all cloud service providers (CSPs) that process or store company data.

2.0 Cloud Security Policy

2.1 Cloud Provider Evaluation

- Only cloud service providers (CSPs) that meet the company's security standards will be approved. Providers must support data encryption, access controls, and logging as company policies require.
- All CSPs must comply with industry standards such as ISO/IEC 27001, SOC 2, and CSA STAR.

2.2 Data Encryption and Access Control

- All sensitive data stored in the cloud must be encrypted using industry-standard encryption protocols in transit and at rest. Multi-factor authentication (MFA) must be enforced to access cloud-based services containing sensitive data.

2.3 Cloud Security Monitoring

- Implement monitoring tools to log and track all cloud activities, including access logs, configuration changes, and security events. The company must retain cloud activity logs for at least one year to support security investigations and audits.

2.4 Backup and Disaster Recovery

- Ensure that data stored in the cloud is backed up regularly and disaster recovery plans are in place to minimise the risk of data loss. Regularly test backup and recovery procedures to ensure data integrity.

3.0 Policy Compliance

3.1 Compliance Measurement

Cloud services will be subject to security audits and monitoring.

3.2 Exceptions

Any exceptions to the policy must be documented and approved by Infosec.

3.3 Non-Compliance

May result in the revocation of cloud access privileges.