

# **Cloud Access and Security Standards**

## **Approved Cloud Services**

Use only IT-approved cloud services listed in the IT portal. Approved services have undergone security review and have appropriate data protection agreements.

Request new cloud services through IT portal with business justification. Security review typically takes 5-10 business days.

## **Cloud Authentication**

Use SSO (Single Sign-On) for cloud services when available. This provides centralized access control and MFA enforcement.

For services without SSO, use strong unique passwords stored in password manager. Enable MFA on all cloud accounts.

## **Data Storage in Cloud**

Store company data only in approved cloud storage (Google Drive, SharePoint). Follow data classification guidelines for cloud storage.

Confidential and Restricted data requires encryption and access controls. Don't store sensitive data in personal cloud accounts.

## **Cloud Sharing and Collaboration**

Share files using secure sharing links with expiration dates and access controls. Don't share confidential data with external parties without approval.

Review and revoke unnecessary sharing permissions regularly. Use view-only access when editing isn't required.

## **Cloud Application Security**

Keep cloud applications updated. Review and minimize third-party app integrations. Revoke access for unused integrations.

Review cloud application permissions before granting access. Be cautious of apps requesting excessive permissions.

## **Shadow IT Prevention**

Don't use unapproved cloud services for company work. Shadow IT creates security gaps and compliance risks.

If you need a tool not currently approved, request it through proper channels. IT will evaluate and approve if appropriate.

## **Cloud Access Monitoring**

Cloud access is monitored for security and compliance. Unusual activity may trigger security review.

Access logs are retained per retention policy. Comply with access audits and reviews.

## **Cloud Data Backup**

Company data in approved cloud services is automatically backed up. Don't rely solely on cloud provider's backup - maintain local copies of critical data.

Test data recovery periodically to ensure backups are functional.

## **Cloud Cost Management**

Be mindful of cloud resource usage and costs. Delete unnecessary files and resources. Use cost allocation tags for departmental resources.

Review cloud spending reports. Optimize resource usage to control costs.

## **Offboarding and Access Revocation**

Cloud access is revoked upon termination or role change. Transfer ownership of shared resources before departure.

Document cloud resources and access for knowledge transfer. Don't retain access to company cloud services after leaving.