Cloud Usage Policy

1. Purpose

This Cloud Usage Policy defines the principles and rules for the appropriate use of cloud services within the organization. Its aim is to enable productivity, collaboration, and innovation while safeguarding organizational data, meeting regulatory obligations, and protecting against misuse or security risks.

---

2. Scope

The policy applies to all employees, contractors, consultants, and third parties who use cloud resources for business purposes. This includes cloud platforms such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), and any cloud-hosted storage or collaboration tools provided by the company.

---

3. Acceptable Use

Employees may use cloud services for legitimate business purposes only. Proper usage includes storing work-related files in the approved cloud storage platform, collaborating with colleagues through authorized cloud applications, and deploying cloud resources in accordance with approved projects and budget.

For example, a marketing manager uploading campaign materials to the corporate-approved cloud drive and sharing them securely with an external design vendor is considered a good practice. This ensures that the files are both accessible and backed up while staying within the company’s approved ecosystem.

In contrast, uploading the same materials to a personal Dropbox account, outside of organizational control, is a violation of this policy. Doing so creates unnecessary risk, as the organization cannot guarantee security, auditability, or retrieval of the files if needed.

---

4. Data Classification and Protection

All data placed in cloud systems must be handled according to its classification level. Confidential and sensitive data, such as customer records, employee information, or intellectual

property, must only be stored in cloud services that meet organizational security and compliance requirements.

Consider an HR specialist who needs to store salary review documents. Placing these documents in the organization's secure HR cloud system, protected with encryption and multi-factor authentication, represents proper use. On the other hand, emailing those documents to a personal Gmail account for "easy access at home" is unacceptable, as it bypasses security measures and could result in a data breach.

---

5. Security and Access

Access to cloud resources will be controlled using the principle of least privilege. Users should only be given the access they require to perform their duties. Multi-factor authentication is mandatory for all logins, and users must safeguard their credentials.

A positive example would be a developer using the corporate single sign-on and MFA to log in to the cloud development environment. This ensures that both the user and the company are protected against unauthorized access. A negative scenario would be the same developer sharing their login credentials with a teammate "for convenience." Not only does this violate security policy, but it also makes accountability and auditing impossible.

---

6. Prohibited Activities

Cloud resources must never be used for personal storage of non-business data, distribution of offensive or inappropriate materials, or hosting of unapproved applications. Activities such as cryptocurrency mining, unauthorized software testing, or circumvention of security controls are strictly forbidden.

A good example is a data scientist spinning up a temporary compute instance in the cloud to run machine learning experiments that align with an approved project. This is legitimate business use. A poor example would be that same scientist using cloud credits to run a personal cryptocurrency mining operation. This not only wastes company resources but also exposes the organization to reputational and regulatory risk.

---

7. Data Retention and Disposal

Employees must follow organizational data retention schedules when storing or deleting cloud-based data. Business-critical documents should never be deleted outside of approved processes.

For instance, a project lead archiving completed project files in the designated retention folder of the cloud drive, ensuring they are preserved for seven years, is following good practice. In contrast, deleting the same files to free up space without considering retention obligations is a policy breach that could compromise compliance.

---

8. Monitoring and Compliance

The organization reserves the right to monitor all cloud usage for compliance, security, and operational needs. Any inappropriate, suspicious, or non-compliant use will be investigated.

An example of compliant behavior would be a finance analyst responding to a compliance check by providing a log of files uploaded and shared in the accounting cloud platform. A non-compliant scenario would be the same analyst refusing to cooperate with a compliance inquiry or attempting to conceal unauthorized storage of financial data.

---

9. Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment, revocation of system access, and legal proceedings where applicable. The organization takes misuse of cloud services seriously, as it directly affects security, compliance, and business continuity.