Cloud Services Policy

Last updated: November 2023

1. Overview

Cloud computing offers a number of advantages including low costs, high performance, and quick delivery of services. However, without adequate controls, it also exposes individuals and organisations to online threats such as data loss or theft, unauthorized access to corporate networks, and so on.

Cloudoko remains committed to enabling employees to do their jobs as efficiently as possible through the use of technology. The following guidelines are intended to establish a process whereby Cloudoko employees can use cloud services as required without jeopardising Cloudoko's data and computing resources.

2. Purpose

The objective of this policy is to ensure that cloud services are used without exposing Cloudoko to the risks associated with this type of operation. It is imperative that employees neither open cloud services accounts nor enter into cloud service contracts for the storage, manipulation or exchange of company-related communications or company-owned data without the Data Protection Officer's input. This is necessary to protect the integrity and confidentiality of Cloudoko data and the security of the corporate network.

3. Scope

This policy applies to all employees of Cloudoko, with no exceptions.

This policy relates to all external cloud services, e.g. cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. Personal accounts are excluded. If you are not sure whether a service is cloud-based or not, please contact the Data Protection Officer.

4. Policy

- Use of cloud computing services and applications will be authorised by the Data Protection Officer.
- The use of such services must comply with Cloudoko's Acceptable Use Policy.
- Employees must not share log-in credentials with co-workers. All sign-ins should be converted to single sign on.
- All employees must comply with the existing password Policies, and password management systems as mandated by Data Protection Officer.
- The Data Protection Officer decides what data may or may not be stored in the Cloud.
- Personal cloud services accounts may not be used for the storage, manipulation or exchange of company-related communications or company-owned data.

5. Policy Compliance

Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

- Acceptable Use Policy
- Password Protection Policy
- Password Construction Guidelines

7. Definitions and Terms

The following definition and terms can be found in the Cloudoko Glossary.

- Software-as-a-Service (SaaS)
- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)

8. Revision History

Date of Change	Responsible	Summary of Change
March 2024	Kevin Boldy	Initial Version

www.cloudoko.com