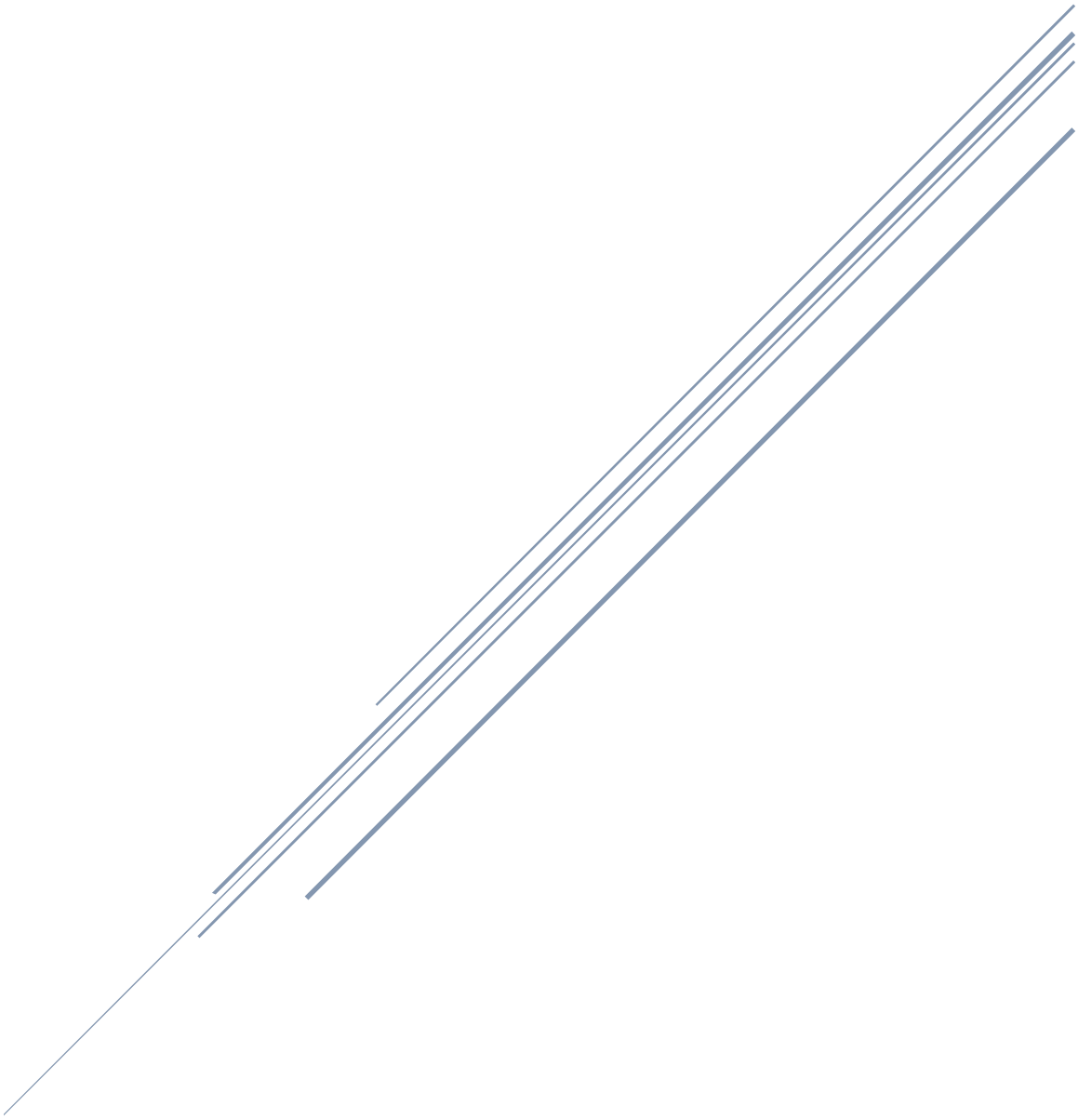
SECUREKLOUD

Data sec Policy



Revision Chart				
Version	**Author(s)**	**Reviewer(s)**	**Description**	**Date**
1.0	Natarajan P	Sasi / Senthil	Original Version	11/Oct/2017
2.0	Sriram	Ravi	Name Conversion	05/Jan/2021
3.0	Silambarasan	Sriram	Version Update	06/Jan/2022
4.0	Silambarasan	Sriram	Version Update	11/Oct/2023
5.0	Balaji S	Sriram	Version Update	24/Apr/2024

Table of Contents

1. Purpose

The purpose of this policy is to define standards for systems that ensures the Information security is implemented and monitored within SecureKloud or external network. These standards are designed to ensure employees understand and adhere to the security principles laid by SecureKloud.

2. Scope

This policy applies to all SecureKloud Technologies Ltd employees, contractors, vendors and agents with an SecureKloud Software Services-owned or personally owned computer or workstation connected to the SecureKloud Technologies Ltd network.

3. Policy Definition:

1. All the Asset (Hardware and Software) assigned issued by SecureKloud should be used for official purpose only.
2. Software: only Company issued licensed software should use, pirated version are strictly restricted and for usage of evaluation version employee should seek approval from BU head, COO and ISMS team
3. Browsing: website for business would be browsed, for any new or additional site requests team member should raise request through the manager / BU approval
4. Premises Entry: User should use his Bio-metric when entering to the premises. No tail gating is encouraged.
5. Hardware: Any Laptop / Desktop / Mobiles provided to employees should be used for official purpose only
6. Software Downloads: SecureKloud restricts all the software downloads directly from website.
7. Data: User / Employees should save data to the centralized repository / share-point portal
8. Emails: SecureKloud emails should only use for official purpose should not use for personal purpose
9. NOC Entry: Only Authorized employees should entry the NoC services of SecureKloud, no tailgating or sharing the Access information were encouraged.
10. Logins: User should use the asset only assets assigned to the resource, if they needed to access the other resources, they should seek approval from BU / Managers / ISMS

4. Policy Compliance

4.1. Compliance Measurement

The ISMS-Team will verify compliance to this policy through various methods like including but not limited to, periodic walk-through, video monitoring, business tools like Firewall logs, AD Logs, Biometric Logs, reports, internal and external audits etc. and feedback to the policy owner.

4.2. Reference

Below Policies and Procedures can be referred:

1. ISMS Policy
2. Internet Policy
3. Email Policy
4. Asset Usage Policy
5. User Access Control and Management Policy
6. Business Continuity policy
7. Communication policy
8. Laptop Usage Policy
9. Firewall Policy
10. Vlan Policy
11. Disciplinary Action Policy

4.3. Exceptions

Any exception to the policy must be approved by the IT-Team team in advance.

4.4. Non-Compliance

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