Owner :	Jed Hewson
Reference Number :	1SMTS-ALL-POL027
Approved Date :	2024-02-22
Next Review Date :	2024-11-01
Version :	4

INTRODUCTION

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 organizations to online threats such as data loss or theft, unauthorized access to corporate networks, and so on.

This cloud computing policy is meant to ensure that cloud services are NOT used without the Chief Technology Officer's knowledge. It is imperative that employees DO NOT open cloud services accounts or enter into cloud service contracts for the storage, manipulation or exchange of company-related communications or company-owned data without the Chief Technology Officer's input. This is necessary to protect the integrity and confidentiality of 1Stream data and the security of the corporate network

1Stream IT Support 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 1Stream employees can use cloud services without jeopardizing company data and computing resources.

SCOPE

This policy applies to all employees in all departments of 1Stream, no exceptions.

This policy pertains 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 Chief Technology Officer.

OBJECTIVES

The objectives of the Cloud Computing Policy is to ensure that 1Stream Employees only use approved Cloud Computing Services and Systems which have been set up by the business in such a way as not to increase the risk of data and information breaches and loss that could compromise the company and or its clients in any way. The key objective is to ensure that at all times 100% approved Cloud Systems and Services are used.

POLICY

The following Policy requirements are to be adhered to at all times:

- Use of cloud computing services for work purposes must be formally authorized by the Chief Technology

Officer. The Chief Technology Officer will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing vendor.
- For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the CEO.
- The use of such services must comply with 1Stream existing Acceptable Use Policy.
- Employees must not share log-in credentials with co-workers. IT Support will keep a confidential document containing account information for business continuity purposes.
- The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by 1Stream Insurance.
- The CIO or any person nominated by the CIO, 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.
- All documentation may only be shared through approved MS OneDrive or Microsoft Teams or Email or Dropbox or Mega or WhatsApp channels.

PRE-APPROVED CLOUD COMPUTING SERVICES

1Stream has pre-approved the following Cloud Computing Services or Systems:

- Office 365 and associated tools (SharePoint, One Drive, Microsoft Teams etc)
- Azure Development Environment
- Amazon Web Services (AWS)
- GitHub
- Sentry IO
- WhatsApp (Clickatell, Infobip, Collab – Message Bird)
- 1Stream CRM
- Freshdesk
- Tableau
- Google Dialogflow
- Grapevine
- Saicom
- Dimension Data
- Twillio
- Avoxi

POLICY COMPLIANCE

COMPLIANCE MEASURMENT

The IT 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 exceptions to this policy must be approved by the 1Stream Team or the CEO in advance of engaging with additional cloud service solutions or suppliers.

NON-CONPLANCE

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

CORRECTIVE ACTION

The company's Corrective Action Procedure will be activated if this policy fails to meet the objectives.

UPDATING, DISTRIBUTION AND COMMUNICATION OF THIS DOCUMENT

This policy can be updated by the Process Owner following the procedure defined in the Document and Control of Records Process (ISP-04-Control of Documentation Process).

The distribution of this process document is circulated to the following persons:

- Chief Operations Officer
- Other Company Directors
- Information Security Management Officer
- HR Manager
- Chief Financial Officer

MANAGEMENT REVIEW

Management should review this document on a continual improvement basis for suitability, adequacy and effectiveness, at least no less than every twelve months.

Reports required for the reviewing of input and output of this process are:

- Follow-up actions from previous management reviews
- Risk Registers
- Information Security Incident Management Reports

The output from the Management Review will include:

- Improvements of the effectiveness of the Information Security Management System and its processes
- Resources needed
- Improvements of the process related to provision of service to the business
- Updates to Information Security Plans
- Updates to the Information Security Risk Register