CLOUD COMPUTING POLICY

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

AzteQ Group Ltd and the Head of Operations (ISMS Manager) remain 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 Organisation employees can use cloud services as required without jeopardising company data and computing resources.

Responsibilities

This policy applies to all employees in all office locations of the Organisation, 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 Internal IT Manager.

Objectives

The objective of this policy is to ensure that cloud services are used without exposing the Organisation 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 (nominated ISMS representative)'s input. This is necessary to protect the integrity and confidentiality of Organisation data and the security of the corporate network.

Policy and Procedures

1. Use of cloud computing services for work purposes must be formally authorised by the Internal IT Manager. The Internal IT Manager will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing vendor.

2. For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the Head of Operations (ISMS Manager).

3. The use of such services must comply with the Organisation's existing E-mail & Internet Acceptable Usage Policy.

4. Employees must not share log-in credentials with co-workers. The Head of Operations (ISMS Manager) will keep a confidential document containing account information for business continuity purposes.

5. 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 the Organisation.

6. The Internal IT Manager decides what data may or may not be stored in the Cloud.

7. Personal cloud services accounts may not be used for the storage, manipulation or exchange of company-related communications or company-owned data.

General

This Policy applies to all employees with access rights to the Organisation’s network systems and will be reviewed at not greater than annual intervals.

Policy Sign-off

Date of Issue:	27/10/2020
Date of Next Review:	15/09/2021
Name:	Tim Barber
Signed:	

Amendment History

Version	Modified On	Modified By	Comments
1.0	15/09/2020	Jo Holloway	
2.0	27/10/2020	Jo Holloway	Update of responsibilities