**Glasswall Solutions Ltd.**

**Cloud Computing Policy**

### Information contained herein is the property of Glasswall Limited and is company confidential.

# Revision 2.0

# Document History

### Table 1: Document Change History

|  |  |  |  |
| --- | --- | --- | --- |
| *Issue Date* | *Issue Number* | *Document Owner* | *Description* |
| 2nd January 2018 | 2.0 |  | Final Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Document Distribution

### Table 2: Document Distribution

|  |  |  |  |
| --- | --- | --- | --- |
| *Name* | *Position* | *Date* | *Signature* |
| Mark Wheelhouse | CFO | 2nd January 2018 |  |
| Paul Kennedy | VP, Product Development | 2nd January 2018 |  |
|  |  |  |  |
|  |  |  |  |

# Contents

1.0 Overview 4

2.0 Purpose 4

3.0 Scope 4

4.0 Policy 5

4.1 Cloud Computing Services Provider Policy 5

4.1.1 For IT Manager and Management, the following applies; 5

4.1.2 For Information Owners, the following applies; 5

4.1.3 For Users, the following applies; 5

4.2 Handling of Company Data When Using Cloud Computing Services 6

4.2.1 Personal 6

4.2.2 Public 6

4.2.3 Operational 6

4.2.4 Critical 6

4.2.5 Confidential 6

4.3 Applicability of Other Policies 6

5.0 Enforcement 6

6.0 Definitions 6

### 

Glasswall is hereinafter referred to as "the company."

# 1.0 Overview

Cloud Services provide a cost effective and efficient method of scaling the resources required to support customers and the Company, for example using Microsoft Azure to achieve at scale computing power, without the requirement to purchase and operate expensive computer equipment.

However, without robust controls and processes to protect Company data, there is risk of exposure to online threats such as data loss, or theft and unauthorised access to Company networks.

Cloud Services provided by a third party are typically have the following delivery models;

* Infrastructure as a Service (IaaS)
* Software as a Service (SaaS)
* Platform as a Service (PaaS)
* Network as a Service (NaaS)

Cloud Services are typically provided via the following deployment models:

* Private cloud; where services are managed by the Company on a third-party platform.
* Public cloud; where services are provided and managed entirely by a third party.
* Hybrid cloud; where services are provided partly by the Company in a private cloud and partly provided by a third party in the public or private cloud.

# 2.0 Purpose

The purpose of this policy is to manage the information security risks associated by using Cloud Computing Services.

# 3.0 Scope

This policy applies to any cloud computing resources that provide services, platforms, and infrastructure that provide support for activities involving the processing, exchange, storage, or management of Company data.

# 4.0 Policy

## 4.1 Cloud Computing Services Provider Policy

Only Company approved Cloud Computing Services may be used to store, manage or process Company Data.

The Outsourcing Policy must be followed when selecting any Cloud Computing Services.

### 4.1.1 For IT Manager and Management, the following applies;

* Use of cloud computing services to store, manage or process Company Data must be approved by the IT Manager or Management.
* The IT Manager or Management must ensure that security, privacy and all other IT management requirements are addressed by the cloud computing provider and the Outsourcing Policy must be followed.
* The information risks and security controls associated with any cloud computing service used by the Company must be reviewed at least once per year. Where possible, this review should be performed in collaboration with the provider
* Security incidents that involve Company Data stored, managed or processed by Cloud Computing Services must be dealt with promptly, the Service Level and Support Agreements must detail how these scenarios are handled by the relevant parties.
* Accounts must only be de-provisioned by the IT Manager or Authorised Users. A documented written process must be maintained that defines a communication workflow for content attached to a user’s account.

### 4.1.2 For Information Owners, the following applies;

* Information Owners must ensure any Cloud Computing Services used to store, transfer, manage or process Company and Personal Data comply with all applicable Company Policies, in addition to local, state, federal, or international laws and regulatory requirements.

### 4.1.3 For Users, the following applies;

* Users are not permitted to accept or agree to terms of service on behalf of the Company, such agreements must be reviewed and approved by the IT Manager or Management.
* Users must not share log-in credentials and must not use shared accounts.

## 4.2 Handling of Company Data When Using Cloud Computing Services

All Company Data must be classified as per the Data Classification Policy.

When using Cloud Computing Services, the following applies;

### 4.2.1 Personal

* Employee’s must not store, manage or process their Personal Data on Company Cloud Computing Services.

### 4.2.2 Public

* Public Data is permitted to be stored, managed or processed on any Cloud deployment method.

### 4.2.3 Operational

* Operational Data can be stored, managed or processed on any approved Cloud deployment method, providing the applicable Company Polices are adhered to.

### 4.2.4 Critical

* Critical data must only be stored on approved Private Cloud Computing Services, providing the applicable Company Polices are adhered to.

### 4.2.5 Confidential

* Confidential data can be stored or managed on approved Private or Public Cloud Computing Services, providing the applicable Company Polices are adhered to.

## 4.3 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

# 5.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

# 6.0 Definitions

Refer to Information Security Policy Guide.