**Glasswall Solutions Ltd.**

**IT Outsourcing 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 Deciding to Outsource 5

4.2 Outsourcing Core Functions 5

4.3 Evaluating a Provider 5

4.4 Security Controls 5

4.5 Outsourcing Contracts 6

4.6 Access to Information 6

4.7 Applicability of Other Policies 6

5.0 Enforcement 6

6.0 Definitions 7

7.0 Attributions 7

### 

Glasswall is hereinafter referred to as "the company."

# 1.0 Overview

Outsourcing of IT involves the company transferring responsibility for carrying out specific functions to an outsourcer. The outsourcer provides services based on a set of agreed deliverables, a mutually agreed service level and terms that are normally defined in a formal contract.

Reasons for outsourcing can include, but are not limited to, the following:

* Reducing the organisation’s costs.
* Greater focus on core business by outsourcing non-core functions.
* Access to world-class skills and resources.

The commercial benefits of outsourcing must be balanced against the commercial and information security risks. These risks must be managed through a combination of legal, physical, logical, procedural and managerial controls to mitigate against inappropriate access to, or disclosure of, sensitive information, loss of intellectual property, protection or the inability of the outsourcer to live up to agreed service levels.

# 2.0 Purpose

The purpose of this policy is to reduce the information security risks associated by specifying the actions to take when outsourcing.

# 3.0 Scope

This policy covers any company IT functions being considered for outsourcing.

# 4.0 Policy

## 4.1 Deciding to Outsource

The following must be considered before the company justifies outsourcing:

* Does the outsource service help achieve the company objectives?
* Does the outsourced service perform better or less expensively than insourcing?
* Does the cost of this service provide commercial benefit?
* Are the information security risks balanced against the commercial benefits?

## 4.2 Outsourcing Core Functions

When outsourcing any core function of the company this policy applies.

## 4.3 Evaluating a Provider

Once the decision to outsource has been made, selecting the appropriate provider is critical to the success of the endeavour.

Due diligence must be performed to ensure an appropriate and proportionate short list to contrast each outsourcers security posture.

This should include a review of the providers;

* Quality assurance and security management standards and accreditations.
* Security policies, processes and procedures.
* Financial stability and commercial track record.
* Ability to perform the requested services.
* Reputation through referrals or case studies.
* Technical ability.

## 4.4 Security Controls

The outsourcing contract must provide a mechanism for secure information exchange with the service provider which must comply with any applicable company policy.

The company and outsource provider must maintain a mechanism for confirming any changes that may impact compliance with Company policy.

Outsourcing contracts must have security controls embedded or referenced within the contract. These controls include, but are not limited to;

* Applicable data protection/privacy laws, money laundering etc.
* Information security policies, procedures, standards and guidelines, such as ISO/IEC 27001;
* Background checks on employees or third parties working on the contract.
* Access controls to restrict unauthorised disclosure, modification or destruction of information, including physical and logical access controls, procedures for granting, reviewing, updating and revoking access to systems, data and facilities etc.
* Information security incident management procedures including mandatory incident reporting.
* Return or destruction of all information assets by the outsourcer after the completion of the outsourced activity, or, whenever the asset is no longer required to support the outsourced activity.
* Copyright, patents and similar protection for any intellectual property shared with the outsourcer or developed during the contract.
* Specification, design, development, testing, implementation, configuration, management, maintenance, support and use of security controls within or associated with IT systems, plus source code escrow.
* Anti-malware, anti-spam and similar controls.
* IT change and configuration management, including vulnerability management, patching and verification of system security controls prior to their connection to production networks.

## 4.5 Outsourcing Contracts

All IT outsourcing must be governed by a legal contract that must:

* Specify exact pricing for the services.
* Cover a specified time period.
* Specify how the provider will treat confidential information.
* Include a non-disclosure agreement.
* Specify services to be provided, including Service Level Agreements and penalties for missing the levels.
* Allow for cancellation if contractual terms are not met.
* Specify standards for subcontracting of the services and reassignment of contract.
* Cover liability and insurance.
* Describe how and where to handle contractual disputes.

## 4.6 Access to Information

The provider must be given the least amount of access required to perform the IT outsourced function. This access must be audited on a regular basis, and must comply with applicable policies.

## 4.7 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 Glasswall Information Security Policy Guide.

# 7.0 Attributions

Elements of this policy are attributed to the ISO27k Implementers’ Forum

(www[dot] ISO27001security[dot]com)