**Glasswall Solutions Ltd.**

**Third Party Connection 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 Use of Third Party Connections 5

4.2 Restricting Third Party Access 5

4.3 Auditing of Connections 5

4.4 Applicability of Other Policies 5

5.0 Enforcement 5

6.0 Definitions 6

### 

Glasswall is hereinafter referred to as "the company."

# 1.0 Overview

Direct connections to external entities are required for some business operations. These connections typically allow access to vendors or customers for service delivery. Careful management of these connections is required so as to ensure company information and digital assets are protected.

# 2.0 Purpose

The policy is intended to provide guidelines securing direct connections to third parties.

# 3.0 Scope

The scope of this policy covers all direct connections between the company's network and non-company owned networks. This policy excludes Remote Access and Virtual Private Network (VPN) access, which are covered in separate policies.

# 4.0 Policy

## 4.1 Use of Third Party Connections

When considering a third-party connection, the following applies;

* Third party connections must have a compelling business need.
* All other reasonable alternative options must be considered before allowing any third-party connection.
* Requests must be approved and implemented by the IT Manager.
* Third parties must only be provided with the minimum access to perform the task required.
* Access to company information and digital assets must be restricted and carefully controlled and monitored.
* Connections to third parties must use a firewall or Access Control List (ACL) to separate the company's network from the third party's network.

## 4.2 Restricting Third Party Access

The third party must agree to:

* Restrict access to the company's network to only those users that have a legitimate business need for access.
* Supply the company with on-hours and off-hours contact information for users responsible for the connection.
* Supply documented escalation processes and procedures.
* Supply names and information relevant about individuals that will have access to the company's confidential data.
* Provide audit logs and be audited by the company on a regular basis.

## 4.3 Auditing of Connections

In order to ensure that third-party connections are in compliance with this policy, they must be audited at least once per quarter.

## 4.4 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.