**Glasswall Solutions Ltd.**

**Virtual Private Network (VPN) 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 Encryption 5

4.2 Authentication 5

4.3 Implementation 5

4.4 Management 5

4.5 Logging and Monitoring 5

4.6 Encryption Keys 5

4.7 Applicability of Other Policies 5

5.0 Enforcement 5

6.0 Definitions 6

### 

Glasswall is hereinafter referred to as "the company."

# 1.0 Overview

A Virtual Private Network, or VPN, provides a method to communicate between networks securely over insecure networks, such as the Internet.

# 2.0 Purpose

The purpose of this policy is to ensure the confidentiality and integrity of data transmitted and received between networks.

# 3.0 Scope

The scope of this policy covers all site-to-site VPNs that connect to company infrastructure, including both sites requiring access to the company's network (inbound) and sites where the company connects to external resources (outbound).

Note that remote access VPNs are covered under a separate Remote Access Policy.

# 4.0 Policy

## 4.1 Encryption

Site-to-site VPNs must utilise strong encryption to protect data during transmission. Encryption algorithms must meet or exceed current minimum industry standards.

## 4.2 Authentication

Site-to-site VPNs must utilise a strong password, pre-shared key, certificate, or other means of authentication to verify the identity the remote entity. The strongest authentication method available must be used, which can vary from product-to-product.

## 4.3 Implementation

When site-to-site VPNs are implemented, they must adhere to the policy of least access, providing access limited to only what is required for business purposes. This must be enforced with a firewall or other access control that has the ability to limit access only to the ports and IP addresses required for business purposes.

Company systems that will be accessed by third parties over the site-to-site VPN should be located in a segmented network, and logically separate from the company's trusted network.

## 4.4 Management

The company should manage its own VPN gateways, meaning that a third party must not provide and manage both sides of the site-to-site VPN, unless this arrangement is covered under an outsourcing agreement.

If an existing VPN is to be changed, the changes must only be performed with the approval of the IT Manager.

## 4.5 Logging and Monitoring

Audit logging must be enabled by default. Monitoring of suspicious activity in audit logs must be completed daily and retained as per the Retention Policy.

## 4.6 Encryption Keys

Encryption keys should be changed in accordance with the Encryption Policy.

## 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 Information Security Policy Guide.