**Glasswall Solutions Ltd.**

**Remote Access 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 Prohibited Actions 5

4.2 Use of unapproved secure remote access methods or equipment 5

4.3 Network Access 5

4.4 Idle Connections 5

4.5 Applicability of Other Policies 5

5.0 Enforcement 6

6.0 Definitions 6

### 

Glasswall is hereinafter referred to as "the company."

# 1.0 Overview

To maintain productivity, access is often required to the company network from homes, remote networks, public Wi-Fi hotspots, or whilst while traveling, etc., but this can introduce risks that must be addressed.

# 2.0 Purpose

The purpose of this policy is to define how to protect confidential information when accessed outside the company network.

# 3.0 Scope

The scope of this policy covers all employees, contractors, and external parties that access company resources over a remote third-party network, whether such access is performed with company-provided or non-company-provided equipment.

# 4.0 Policy

## 4.1 Prohibited Actions

Remote access to company systems is only allowed through company approved means.

When remotely accessing the company network, users must;

* Obtain prior approval to remotely connect to the company network.
* Use company approved remote desktop tools.
* Use company approved remote access software.
* Ensure the remote host is not connected to any other network at the same time.
* Use company approved methods to protect their login and password.
* All devices that are connected to company networks remotely must;
  + Have company approved anti-virus software with the latest updates applied.
  + Have the default firewall enabled where applicable.
  + Have the most up to date software updates applied.
  + Use company approved VPN software.
* Ensure third party connections comply with requirements as stated in the Third-Party Connection Policy.
* Ensure Mobile Devices used to connect to the company network comply with the Mobile Device Policy.

## 4.2 Use of unapproved secure remote access methods or equipment

Use of unapproved methods or equipment, such as public terminals, to access the company network is strictly prohibited.

## 4.3 Network Access

Remote users access privileges must be restricted to only those information assets that are reasonable and necessary to perform their job function.

## 4.4 Idle Connections

Remote connections to the company network must be timed out after 30 minutes of inactivity due to the associated security risks.

## 4.5 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.