**Glasswall Solutions Ltd.**

**Wireless Network 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 Physical Location Guidelines 5

4.2 Configuration and Installation 5

4.2.1 Wireless Access Security Configuration 5

4.2.2 Wireless Access Encryption Configuration 5

4.2.3 Installation and ongoing maintenance 5

4.3 Inactivity 6

4.4 Audits 6

4.6 Applicability of Other Policies 6

5.0 Enforcement 6

6.0 Definitions 6

### 

Glasswall is hereinafter referred to as "the company."

# 1.0 Overview

Wireless communications are essential to a productive workplace, as devices continue to evolve and reduce their reliance on physical media to connect to the company network. Wireless networks can provide convenient network access for third parties such as visitors or contractors. However, wireless networks can introduce security risks to the network that can be mitigated with an appropriate Wireless Network Policy.

# 2.0 Purpose

This policy outlines the steps to secure company owned wireless networks and infrastructure.

# 3.0 Scope

This policy further covers all company owned wireless infrastructure, including but not limited to, access points, routers, wireless network interface cards, and anything else capable of transmitting or receiving a wireless network signal.

# 4.0 Policy

## 4.1 Physical Location Guidelines

For any wireless access point (WAP), the following applies;

* Physical placement;
  + Where possible, access points must be located central to their environment.
  + Access points must not be placed in public or easily accessed locations.
  + Access points must be placed in non-obvious locations.
* Physical requirements;
  + Any physical labels with default administrator credentials and passwords must be recorded in the asset register and then removed or etched to become illegible.

## 4.2 Configuration and Installation

The following guidelines must apply to the configuration and installation of company owned WAPs;

### 4.2.1 Wireless Access Security Configuration

* Signal broadcast strength must be reduced to only what is necessary to cover the physical environment.
* The Service Set Identifier (SSID) of the access point must be changed from the factory default.
* The SSID must not allow a third party to associate the access point's signal to the company or provide any physical location information.
* Administrative access must not use default user names or passwords.
* Administrative access must use strong passwords only that comply to the Password Policy.
* All logging features must be enabled.
* Wireless networking must not be deployed in a manner that will circumvent the company's security controls.

### 4.2.2 Wireless Access Encryption Configuration

* Encryption must be used at all times.
* Only WPA2 using AES, or stronger, encryption types must be used.
* WAP passwords must be changed quarterly.

### 4.2.3 Installation and ongoing maintenance

* Software and/or firmware on the wireless access points must be updated prior to deployment.
* Software and/or firmware on the wireless access points must be updated when available
* Wireless devices must only be installed only by the company's IT department or approved third parties.
* Channels used by wireless devices should be evaluated to ensure that they do not interfere with company equipment.

## 4.3 Inactivity

Inactive wireless access points should be disabled.

## 4.4 Audits

The wireless network audit must;

* Be undertaken at least twice each year to ensure that this policy is being followed.
* Cover location of access points, signal strength, SSID, and use of strong encryption.
* Use only company approved audit software.

## 4.5 Guest Wireless Internet Access Point

Guest Wireless Internet access points must be configured as follows;

* Route directly to the Internet with no access to Glasswall company networks.
* Must display a disclaimer with terms and conditions before Internet access is allowed.

## 4.6 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.