**Glasswall Solutions Ltd.**

**Mobile Device 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 Security 5

4.2 Mobile Device Security 5

4.2.1 Laptops 5

4.2.2 Smartphones/Tablets 5

4.2.3 Mobile Storage Media 6

4.2.4 Personal electronic devices (PEDs) 6

4.2.5 Other Mobile Devices 6

4.3. Connecting to Networks 6

4.3.1 Company Networks 6

4.3.2 Third Party Networks 6

4.4 General Guidelines 6

4.5 Audits 6

4.6 Applicability of Other Policies 7

5.0 Enforcement 7

6.0 Definitions 7

### 

Glasswall is hereinafter referred to as "the company."

# 1.0 Overview

Use of mobile devices is an integral part of standard business operations. Since sensitive data is stored on these devices, risk is associated with their use and requires specific security controls.

# 2.0 Purpose

The purpose of this policy is to define the use and security of mobile devices and associated applications to protect the confidentiality and integrity of sensitive data.

# 3.0 Scope

This policy applies to all mobile devices used to store company data, including, but not limited to, laptops, notebooks, smart phones, tablets and USB drives, regardless of ownership.

# 4.0 Policy

## 4.1 Physical Security

Protective measures include, but are not limited to, the following:

* Laptop locks and cables should be used to secure laptops where practical.
* Mobile devices should be kept out of sight when not in use.
* Due diligence should apply when transporting mobile devices in busy areas.
* Mobile devices should not be stored in any vehicle unattended.
* Using remote wipe/remote delete technology for company owned devices in the event of or evidence of the device being compromised.
* The company should continue to monitor the market for physical security products for mobile devices, as it is constantly evolving.
* As a minimum, access to all mobile devices must be PIN, biometrically or password protected.

## 4.2 Mobile Device Security

The following applies to all mobile devices that contain or access company data;

* Devices must use the most up to date Operating Systems and apply all the latest available software and firmware patches.
* Devices must store all user-saved passwords in an encrypted password store.
* Devices must be configured with a secure password that complies with the Password Policy. This password must not be the same as any other credentials used within the organisation.
* Devices not issued by the company or managed by IT require approval to be connected directly to the company network, and must comply with the Network Access Policy.
* Screen lock must be enabled with a minimum timeout of 5 minutes.
* Devices with a hibernate or sleep mode should require re-authentication before access is permitted.

The following sections define the company's requirements for data security as it relates to specific types of mobile devices;

### 4.2.1 Laptops

Laptops that contain or access company data must comply with the appropriate company policies.

All removable media such as CD-ROMs, DVDs, memory cards and mobile media storage should be removed when not in use.

Laptops must have a firewall and anti-virus software enabled at all times.

### 4.2.2 Smartphones/Tablets

Smartphones/Tablets that contain or access company data must comply with the appropriate company policies.

The devices encryption features must be enabled.

### 4.2.3 Mobile Storage Media

Mobile Storage Media that contain or access company data must comply with the appropriate company policies.

Any USB drive, flash drive, memory stick or other personal data storage media must be encrypted if they contain company confidential data.

### 4.2.4 Personal electronic devices (PEDs)

No company data can be stored on any PED without prior approval.

### 4.2.5 Other Mobile Devices

Unless specifically addressed by this policy, storing company data on other mobile devices, or connecting such devices to company networks is expressly prohibited without prior approval of the IT Manager.

## 4.3. Connecting to Networks

### 4.3.1 Company Networks

Only authorised mobile device are allowed to connect to the company network and must comply with the Network Access & Authentication Policy.

### 4.3.2 Third Party Networks

Users must not connect to any outside network without a secure, up-to-date software firewall configured on the mobile device.

## 4.4 General Guidelines

The following guidelines apply to the use of all mobile devices:

* Loss, Theft, or any other security incident related to all mobile device containing company data must be reported to the IT Manager at the earliest possible opportunity through any communication means available.
* Company data must not be stored on a mobile device for any longer than needed.
* Company data must not be stored on a mobile device that has unlicensed or pirated software installed.
* Confidential data should not be stored on mobile devices unless it is absolutely necessary.
* If confidential data is stored on a mobile device it must be appropriately secured and comply with the Confidential Data policy.
* Data stored on mobile devices must be securely disposed of in accordance with the Data Classification Policy.
* Use of jail broken, cracked OS or mobile devices using unapproved applications that access or process company data is prohibited.

## 4.5 Audits

The company must conduct periodic reviews to ensure policy compliance. A sampling of mobile devices should be taken and audited against this policy on a periodic basis.

## 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.