**Glasswall Solutions Ltd.**

**Physical Security 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 Choosing a Site 5

4.2 Security Zones 5

4.2.1 At a minimum, the company must; 5

4.2.2 Security zones should include: 5

4.3 Access Controls 5

4.3.1 Keys & Keypads 6

4.3.2 Keycards & Biometrics 6

4.3.3 Alarm System 6

4.4 Physical Data Security 6

4.5 Physical System Security 6

4.5.1 Minimising Risk of Loss and Theft 6

4.5.2 Minimising Risk of Damage 6

4.6 Fire Prevention 7

4.7 Entry Security 7

4.7.1 Use of Identification Badges 7

4.7.2 Sign-in Requirements 7

4.7.3 Visitor Access 7

4.8 Applicability of Other Policies 7

5.0 Enforcement 7

6.0 Definitions 8

### 

Glasswall is hereinafter referred to as "the company."

# 1.0 Overview

Securing company digital assets requires appropriate measures to address standard and non-cyber related risks that may affect physical assets and company premises.

# 2.0 Purpose

The purpose of this policy is to govern the company's physical information systems.

# 3.0 Scope

This policy covers the security of the company's physical assets and company premises, and excludes non-IT assets.

# 4.0 Policy

## 4.1 Choosing a Site

At a minimum, the company's site should:

* Not be particularly susceptible to fire, flood, earthquake, or other natural disasters.
* Not be located in an area where the crime rate and/or risk of theft is higher than average.
* Not have an excessive number of entry points.
* Have proportionate physical security such as CCTV, Fire and Burglar alarms.

## 4.2 Security Zones

### 4.2.1 At a minimum, the company must;

* Maintain industry standard security controls such as locks on exterior doors and a fire and burglar alarm system.
* Provide security in layers by designating different security zones within the building.

### 4.2.2 Security zones should include:

* Public
  + This includes areas of the building or office that are intended for public access such as lobby, common areas of the building.
    - Access Restrictions: None.
    - Additional Security Controls: None.
* Company
  + This includes areas of the building or office that are used only by employees and other persons for official company business such as hallways, private offices, work areas, conference rooms.
    - Access Restrictions: Only company personnel and approved/escorted individuals.
    - Additional Security Controls: Additional access controls should be used, such as keys, keypads, keycards, or similar devices, with access to these areas logged if possible.
* Restricted
  + This includes areas that are restricted to use by certain persons within the company, such as executive offices, network or server room(s), and storage areas that contain sensitive information.
    - Access Restrictions: Only company personnel and approved/escorted individuals.
    - The following must be used as a minimum:
      * keys, keypads, keycards, or similar devices, with access logged and reviewed.
      * CCTV and intruder alarm system(s) that will alert to unauthorised access.

## 4.3 Physical Access Controls

Where physical access controls are implemented, the following applies;

### 4.3.1 Keys & Keypads

* The use of keys and keypads is acceptable, as long as keys are marked "do not duplicate" and their distribution is limited.

### 4.3.2 Keycards & Biometrics

* The company requires that keycards or biometrics be used for all user access controls and provide the least amount of access required to do their job.
* If a keycard is suspected or confirmed as lost or stolen it must be immediately disabled.
* If an employee is terminated or resigns, that user's access must be immediately disabled.

### 4.3.3 Alarm System

* The company mandates the use of professionally monitored 24/7 alarm system.
* Company personnel must be assigned and notified if an alarm is tripped at any time.
* A weekly test must be conducted to verify normal operation.

## 4.4 Physical Data Security

Certain physical precautions must be taken to ensure the integrity of the company's data. At a minimum, the following applies:

* Computer displays and monitors should be positioned where information displayed cannot be seen by outsiders.
* Privacy filters must be used where computer displays or monitors may be seen by outsiders.
* Confidential and sensitive information should not appear on a computer display or monitor where it can be viewed by those not authorised to view the information.
* Physical network cabling should not intrude or be clearly visible in commonly used public zones.
* Physical network ports that are not in use should be disabled or disconnected.

## 4.5 Physical System Security

For physical company assets, the following applies;

### 4.5.1 Minimising Risk of Loss and Theft

* To reduce loss or theft of company property, the following applies:
  + If a system is not in use for an extended period of time it should be moved to a secure area with restricted access.
  + Mobile devices: refer to the company's Mobile Device Policy for guidance.
  + Systems that store confidential data: Refer to the company's Confidential Data Policy for guidance.

### 4.5.2 Minimising Risk of Damage

* For systems that store company data, the following applies;
  + Environmental controls should keep the operating environment of company systems within manufacturer specified standards
  + Where applicable, measures should be taken to eliminate any effect or impact of static electricity.
  + Strong magnets must not be used in proximity to company systems or media.
  + Beverages must never be placed where they can be spilled onto company systems.
  + Uninterruptible Power Supplies are required for all systems that store or process Critical data.

## 4.6 Fire Prevention

To reduce risk of fire for systems that store company data, the following applies;

* Fire, smoke alarms, and/or suppression systems must be used, and must conform to industry standards.
* Electrical outlets must only be used within the manufactures guidelines.
* Electrical equipment must conform to the local industry standards.
* Unused electrical equipment should be turned off when not in use for extended periods of time.
* Regular inspection of electrical equipment must be performed.
* A smoke alarm monitoring service must be used that will alert a designated company employee if an alarm is tripped during non-business hours.

## 4.7 Entry Security

Where entry is required to Company and Private zones, the following applies;

### 4.7.1 Use of Identification Badges

Visitor badges are required to identify third party persons on company premises.

### 4.7.2 Sign-in Requirements

Third parties must sign-in a log facility in the lobby or entry area upon arrival. At a minimum, the sign-in register must include the visitor's name, company name, reason for visit, name of person visiting, sign-in time, and sign-out time.

### 4.7.3 Visitor Access

Visitors must only be given the level of access to the company premises that is appropriate to the reason for their visit.

## 4.8 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.