**Glasswall Solutions Ltd.**

**Acceptable Use Policy**

### Information contained herein is the property of Glasswall Limited and is company confidential.

# Revision 2.1

# Document History

### Table 1: Document Change History

|  |  |  |  |
| --- | --- | --- | --- |
| *Issue Date* | *Issue Number* | *Document Owner* | *Description* |
| 2nd January 2018 | 2.0 |  | Final Draft |
| 14 Nov 2019 | 2.1 |  | Review and edits |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Document Reviewers

### Table 2: Document Distribution

|  |  |  |  |
| --- | --- | --- | --- |
| *Name* | *Position* | *Date* | *Signature* |
| Mark Wheelhouse | CFO |  |  |
| Paul Burke | VP, Product Development |  |  |
| Abbas Haidar | IT Manager |  |  |
| Dinis Cruz | CISO |  |  |

## 

# Contents

1.0 Overview 4

2.0 Purpose 4

3.0 Scope 4

4.0 Policy 5

4.1 E-mail and Messaging Use 5

4.2 Confidentiality 5

4.3 Network Access 5

4.4 Unacceptable Use [requires HR input] 6

4.5 Blogging and Social Networking 6

4.6 Instant Messaging 7

4.7 Overuse 7

4.8 Internet Usage 7

4.9 Copyright Infringement 8

4.10 Peer-to-Peer File Sharing 8

4.11 Streaming Media 8

4.12 Monitoring and Privacy 8

4.13 Bandwidth Usage 8

4.14 Personal Usage 8

4.15 Remote Desktop Access 8

4.16 Circumvention of Security 8

4.17 Use for Illegal Activities 9

4.18 Non-Company-Owned Equipment 9

4.19 Personal Storage Media 9

4.20 Software Installation 9

4.21 Reporting of Security Incident 9

4.22 Applicability of Other Policies 10

5.0 Enforcement 10

6.0 Definitions 10

### 

Glasswall is hereinafter referred to as "the company."

# 1.0 Overview

Since inappropriate use of company IT resources exposes the company to risk, it is important to outline what is permitted and what is prohibited.

# 2.0 Purpose

This Acceptable Use Policy is intended to provide a framework for use of the company’s IT resources. It should be interpreted such that is has the widest application, and thus includes new technologies and services that may not be explicitly referred to.

# 3.0 Scope

The scope of this policy includes any and all use of company IT resources, including but not limited to, computer systems, email, the network, and Internet connections.

# 4.0 Policy

## 4.1 E-mail and Messaging Use

For use of Company email and messaging systems, the following applies;

* Company accounts should only be used for Company business related purposes. Personal communication of a non-business nature is permitted on a limited basis.
* The company accounts shall not to be used for;
  + Spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.
  + Creation or distribution of any disruptive or offensive messages, including but not limited to offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
* Employees who receive any emails or messages with this content from company employees should report the matter to their supervisor immediately.
* Information that is considered confidential or proprietary to the company may not be sent via email or messaging systems, regardless of the recipient, without being encrypted.
* It is company policy not to open files from unknown senders, or when such files are unexpected.
* Where systems are not designed to transfer large files, such as such email, should not contain file attachments totalling in excess of 25MB.
* The user is prohibited from attempting to impersonate another person or use another person’s account.
* Please note that detailed information about the use of email is covered in the company Email Policy.

## 4.2 Confidentiality

Confidential data must not;

* Be shared or disclosed in any manner to unauthorised non-employees of the company.
* Be posted on the Internet or any publicly accessible systems.
* Should not be transferred in any insecure manner.

Please note that detailed information about the use of confidential data is covered in the company Confidential Data Policy.

## 4.3 Network Access

Existence of access capabilities does not imply permission to use this access, therefore users must;

* Take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function.
* Report any suspicion or evidence of inappropriate access, accidental or not as per incident response policy.

## 4.4 Unacceptable Use

The following actions shall constitute unacceptable use of the corporate network, these are not exhaustive but act as a frame of reference for activities that are deemed unacceptable by the company. These actions should be considered by HR for inclusion in the company employee manual.

The user may not use the corporate network and/or systems to:

* Engage in activity that is illegal under all applicable laws.
* Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the company.
* Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, insulting, threatening, obscene or otherwise inappropriate messages or media.
* Engage in activities that cause an invasion of privacy.
* Engage in activities that cause disruption to the workplace environment or create a hostile workplace.
* Make fraudulent offers for products or services.
* Perform any of the following unauthorised activities: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques not part of user’s job function.
* Install or distribute unlicensed or "pirated" software.
* Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

## 4.5 Blogging and Social Networking

Users are required to have read all applicable company policies before they begin blogging on behalf of the company. Only authorised users are allowed to blog on behalf of the company on public platforms or using company social media accounts.

The following applies to users when writing content on any public platform or any social media account;

* Written content should not disclose any information that is confidential or proprietary to the company or to any third party that has disclosed information to the company.
* Written content must respect copyright, privacy, fair use, financial disclosure, and other applicable laws.
* The company reserves the right to request the certain subjects are avoided, to request withdrawal of certain posts, and request removal of inappropriate comments.

The following applies to users when writing content on behalf of the company on any public platforms or any social media accounts;

* Content must be written in a professional and responsible manner.
* Ensure no information detrimental to the company is published.
* Obtain approval when writing about the company and the industry.

The following applies to users when writing content on behalf of the themselves on any public platforms or any personal social media accounts;

* Users must not comment on any aspect of the company's business.
* Where personally written content draws an association with the company, a disclaimer must be used.
* Disclaimers must contain the following "the views and opinions expressed are mine and do not necessarily reflect the views of my employer”
* Personally written content should not include company logos or trademarks.

## 4.6 Instant Messaging

Only approved Instant Messaging applications are allowed and should only be used for corporate communications. For a list of approved instant messaging apps, please contact the IT team. The user should recognise that Instant Messaging may be an insecure medium and should take any necessary steps to follow guidelines on disclosure of confidential data. Where possible all Instant Messaging communications should be logged.

## 4.7 Overuse

Actions detrimental to the computer network or other corporate resources, or that negatively affect job performance are not permitted.

## 4.8 Internet Usage

For internet usage from any company owned device, the following applies;

* Company employees are expected to use the Internet responsibly and productively. Internet access should be limited to job-related activities, although limited personal use is permitted.
* All Internet data that is composed, transmitted and/or received by company computer systems belongs to the company. It is therefore subject to disclosure for legal reasons or to other authorised third parties.
* Internet must not be used for any;
  + Spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.
  + Creation or distribution of any disruptive or offensive messages, including but not limited to offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
* Obtaining, distributing and installing of unapproved software is strictly prohibited.
* Downloading, copying or pirating software is strictly prohibited.
* Sharing confidential material, trade secrets, or proprietary information outside of the organisation is strictly prohibited.
* Hacking or malicious activities against third parties is strictly prohibited.
* Knowingly introducing malicious software onto the company network and/or jeopardising the security of the company systems is a disciplinary offence.
* The company reserves the right to monitor Internet traffic.
* Sites and downloads may be blocked by company if they are deemed to be harmful and/or not productive to business.

## 4.9 Copyright Infringement

The company's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or Unauthorised copyrighted content.

The following activities constitute violations of acceptable use policy and will result in disciplinary procedures;

* Copying and sharing images, music, movies, or other copyrighted material.
* Posting or plagiarising copyrighted material.
* Downloading copyrighted files which the employee has not already legally procured.

This list is not exhaustive but is included to provide a frame of reference for types of activities that are prohibited. Applicable copyright law applies.

## 4.10 Peer-to-Peer File Sharing

Peer-to-Peer (P2P) networking is strictly prohibited.

## 4.11 Streaming Media

Streaming media is permitted for job-related functions using only approved applications.

## 4.12 Monitoring and Privacy

The company reserves the right to;

* monitor all Internet and network traffic.
* Block websites, services, applications and downloads if they are deemed to be harmful and/or not productive to business.

## 4.13 Bandwidth Usage

Excessive use of company bandwidth or other computer resources that cause detrimental impact on the company is not permitted.

## 4.14 Personal Usage

Limited personal usage of company computer systems is permitted, providing it does not have a detrimental effect on the company or on the user's job performance.

## 4.15 Remote Desktop Access

Remote access to the network must conform to the company's Remote Access Policy.

## 4.16 Circumvention of Security

Using company-owned or company-provided computer systems to knowingly circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited.

## 4.17 Legal Restrictions

No company-owned or company-provided computer systems may be knowingly used for activities that are considered illegal under applicable laws. Such actions may include, but are not limited to, the following:

* Unauthorised Port Scanning.
* Unauthorised Network Hacking.
* Unauthorised Packet Sniffing.
* Unauthorised Packet Spoofing.
* Unauthorised Denial of Service.
* Unauthorised Wireless Hacking.
* Any act that may be considered an attempt to gain Unauthorised access to or escalate privileges on a computer or other electronic system.
* Acts of Terrorism.
* Identity Theft.
* Spying.
* Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statutes.
* Downloading, storing, or distributing copyrighted material.

The company will take all necessary steps to report and prosecute any violations of this policy.

## 4.18 Non-Company-Owned Equipment

The user must obtain express written permission from the IT Manager before installing non-company-provided computer systems on the company network. Once this permission is obtained, all company policies apply.

## 4.19 Personal Storage Media

Connecting personal storage devices to any company owned device or equipment is strictly prohibited.

## 4.20 Software Installation

The user must obtain express written permission from the IT Manager and the employees line manager before installing non-company-provided software. Once this permission is obtained, all company policies apply.

## 4.21 Reporting of Security Incidents

If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify their supervisor and comply with the company Incident Response Policy.

## 4.22 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.