NCAG
Network Claim Assessors Group

Minimum access Policy

1. Introduction

1.1. Overview

The purpose of this policy is to define rules and requirements for connecting to Network Claim Assessors Group network from any host that is not managed or owned by Network Claim Assessors Group. These rules and requirements are designed to minimize the potential exposure to Network Claim Assessors Group from damages which may result from unauthorized use of Network Claim Assessors Group resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Company internal systems, and fines or other financial liabilities incurred as a result of those losses.

1.2. Scope

This policy applies to all parties operating within Network Claim Assessors Group network environment or utilizing Information Resources. It covers personal computers (stand-alone or network-enabled), located at Network Claim Assessors Group offices and Network Claim Assessors Group production related locations, where these systems are under the jurisdiction and/or ownership of Network Claim Assessors Group or subsidiaries, and any personal computers, laptops, mobile devices and or servers authorized to access Network Claim Assessors Group data networks.

2. Policy Statement

2.1. General requirements

It is the responsibility of Network Claim Assessors Group employees, contractors, vendors, and agents with access privileges to Network Claim Assessors Group corporate network to ensure that their personal computer, laptop, mobile device or server conforms with the standards set out in this policy. When accessing Network Claim Assessors Group network from a personal computer, Authorized Users are responsible for preventing access to any company computer resources or data by non-Authorized Users. Performance of illegal activities through Network Claim Assessors Group network by any user (Authorized or otherwise) is prohibited.

Thys Botes
MD (Network Claims Assessors)

The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access.

Authorized Users will not use Network Claim Assessors Group networks to access the Internet for outside business interests.

2.2. **Operational Procedures**

Before any personal computer, laptop, mobile device, or server is connected to any Network Claim Assessors Group resource it is the responsibility of the owner of such equipment to request Internal IT to assess the device before it is connected to any of Network Claim Assessors Group owned corporate network or any network managed by the Internal IT department or subsidiaries.

Internal IT will assess the personal computer, laptop, mobile device, or server prior to connecting the device to the corporate network, the assessment will include all the requirements set out in section 2.3.

3. Minimum Requirements

3.1. All Windows critical and security updated will be installed and up to date, if any pending updates are found on the device, the device will need to be updated prior to connecting to the corporate network.

3.2. Anti-Virus software must be installed and must be up to date. If no Antivirus is present an IT representative will install a free or trial version of Anti-Virus software to ensure the device does not contain any malicious applications or files.

3.3. Require employees to allow the organization to install mobile device management software, if desired by the organization, and prohibit them from taking any actions to circumvent security protections put in place by the organization.

3.4. Prohibit employees from utilizing any of the following applications:

3.4.1. Proxy Applications

3.4.2. Peer to Peer file transfer applications

3.4.3. File Transfer Software other than those identified by the IT department.

3.4.4. Network Monitoring software unless approved IT.

3.5. Require employees to fully segregate personally owned data from company-owned data possible.

3.6. The owner assumes liability for any damages caused by malfunction, viruses, etc.

Thys Botes

MD (Network Claims Assessors)

3.7. Only authorised individuals will be given access to confidential and/or personal information based on whether the individual requires access to the confidential and/or personal information to perform their duties.

4. Enforcement

4.1. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Network Claim Assessors Group.

5. Definitions

TERMS	**DESCRIPTION**
MINS	Manager: Infrastructure, Network and Security

CEO name THYS BOTES CEO signature Thys Botes MD (Network Claims Assessors)

Signed at PAROW on this 12 day of APRIL 20 22