NCAG
Network Claim Assessors Group

Backup and Restore Policy

1. Overview

1.1. Network Claim Assessors Group has a duty to ensure that all information and data which it is responsible for is securely and routinely backed up. The company has a responsibility to ensure that the information and data which has been backed up can be restored in the event of deletion, loss, corruption, and damage or made unavailable due to unforeseen circumstances. The purpose of this policy is to identify and establish processes, procedures, and good working practices for the backup and timely recovery of the company's information and data, existing in both electronic and physical form.

2. Scope

2.1. All employees, contractors, consultants, temporary and other workers at **Error! Reference source not found.** including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by Network Claim Assessors Group, or to devices that connect to the Network Claim Assessors Group network or reside at a Network Claim Assessors Group site.

2.2. The scope of this policy extends to the back-up of important information and data, regardless of the form it takes including the recovery of IT systems and supporting infrastructure.

3. Policy Statement

3.1. General Requirements

There is always a risk that systems and/or procedures will fail resulting in loss of access to information, data and systems, despite the implementation of best practice.

The following steps will help ensure that Network Claim Assessors Group information and data is backed up and restored securely in the most efficient manner possible.

NCAG
Network Claim Assessors Group

4. Data Backups

4.1. Network Claim Assessors Group IT team are responsible for providing system support and data backup tasks and must ensure that adequate backup and system recovery practices, processes and procedures are followed.

4.2. All IT backup and recovery procedures must be documented, regularly reviewed and made available to trained personnel who are responsible for performing data and IT system backup and recovery.

4.3. All infrastructure data on One drive, networking and supporting system configuration files must be systematically backed up in the event of system re-installation and/or configuration.

4.4. All backup media must be encrypted and appropriately labelled with date/s and codes/markings which enables easy identification of the original source of the data and type of backup used on the media. All encryption keys should always be kept securely.

4.5. Backup media which is retained on-site prior to being sent for storage at a remote location must be stored securely.

4.6. Access to the on-site original and backup location must be restricted to authorised personnel only.

4.7. All backups identified for long term storage must be stored at a remote secure location with appropriate environmental control and protection to ensure the integrity of all backup media.

4.8. Regular tests must be carried out to establish the effectiveness of the company's backup and restore procedures by restoring data/software from backup copies and analysing the results. **Error! Reference source not found.** IT Team should be provided with the information relating to any issues that may arise while testing the restored data.

Thys Botes
MD (Network Claims Assessors)

4.9. The IT Team should be notified when backups fail – providing information such as the backup job detail and reasons (if applicable) for the failure. A record must be maintained, detailing the backup job failure including any action taken.

5. User responsibilities

Users also have a responsibility to ensure Network Claim Assessors Group data is securely maintained and is available for backup.

5.1. Users must not store any data/files on the local drive of a computer (this excludes the normal functioning of the Windows operating system and other authorised software which requires the 'caching' of files locally in order to function). Instead, Users must save data (files) on their allocated areas. Data (files) which are stored "locally" will NOT be backed up and will therefore be at risk of exposure, damage, corruption or loss.

5.2. If the company network becomes unavailable for whatever reason and data or work is at risk of being lost, users may have no option but to save the data (files) locally (i.e. on the computer being used) or on approved media storage such as a company owned encrypted Data stick (USB storage). Once the Network Claim Assessors Group network becomes available again, data (files) should be immediately transferred to the company network for it to be backed up safely and local copies of data on the computer or portable storage media must be deleted. This will help to ensure the availability and integrity of data and to avoid duplicate copies of data being stored.

5.3. Mobile phones can be used to store sensitive, business, or personal identifiable information, but must comply with the applicable processing of personal information laws.

6. Data Restores

Data (file) restores are carried out by Network Claim Assessors Group IT Team who will endeavour to restore files from a date specified by the user or from the nearest backed up date.

Thys Botes

MD (Network Claims Assessors)

6.1. Users must request data (files) to be restored by contacting the IT Team. Only files which the user is authorised to access will be provided from the restore.

6.2. The IT Team will need to verify that the User has permission and/or authorisation to view or obtain restored copies of file/s and/or folder/s.

6.3. Users requesting a restore/s are required to provide as much information about the data (file/s) as necessary – this will include:

6.3.1. The reason for the restore.

6.3.2. The name of file/s and/or folder/s and/or system/s to be restored.

6.3.3. Date, day or time of deletion/corruption or nearest approximation.

6.3.4. The last date, day or time which the User recalls the data (files) being intact and accessed/used successfully.

6.4. All backup and recovery (restore) procedures must be documented and made available to Network Claim Assessors Group IT Team for carrying out data (file) restores.

6.5. Requests from third party software/hardware vendors for file or system restores for the purpose of system support, maintenance, testing, or other unforeseen circumstance should be made under the supervision of the IT Manager, CEO or Network Claim Assessors Group representative appointed by the IT Manager or CEO.

6.6. Personnel accessing backup media for the purpose of a restore must ensure that any media used is returned to a secure location when no longer required.

7. Enforcement

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,

Thys Botes
MD (Network Claims Assessors)

contractor or vendor may result in the termination of their contract or assignment with (Network Claim Assessors Group).

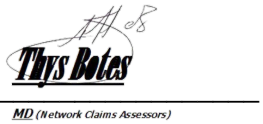
Any exception to the policy must comply with the **Exceptions Policy**.

8. Definitions

Terms	Description
Infrastructure data	This generally refers to data in a database or file that functions as system, application, user or backup data. Such data is physically stored on a data storage device such as a hard drive that may be located locally or on remote infrastructure such as a cloud service.
Backup media	Storage media, these are devices that store application and user information. The primary storage media for a computer is usually the internal hard drive. The secondary storage media is usually referred to as the backup media, a removable hard drive, USB flash Drive, Tape Drive, Cloud Drive. The secondary storage media usually contains copies of the information stored on the primary storage media.
Encryption	The process of converting information or data into a code, especially to prevent unauthorized access.

Thys Botes
MD (Network Claims Assessors)

NCAG
Network Claim Assessors Group

CEO name THYS BOTES CEO signature 

Signed at PAROW on this 12 day of APRIL 2022