4. **Classification Data Subjects consent to retain, hold and collect information**

4.1. The primary consideration before accepting data from any source is to assess whether the data obtained is of a personal, confidential, and or private nature. This will enable you to assess whether the necessary steps following must be adhered to, as the POPI and Privacy Policy only apply to such information. Please see Information Classification Policy and Procedure for classification requirements.

5. **Consent / Permission from the data subject**

5.1. Before accepting any confidential, personal, and/or private information, it is of utmost importance to ensure that you have the written consent and permission of the data subject to keep, transfer, pass on, distribute, use or store such information.

5.2. If no such consent or permission can be obtained or reasonably ascertained, then the data must be returned with immediate effect as per the POPI and Privacy Policy.

5.3. Methods to obtain such permission or consent include but are not limited to the following means:

5.3.1. Letter of consent

5.3.2. Data collection forms

5.3.3. Email consent

5.3.4. Public website downloads (publishing)

5.3.5. Contractual Agreements and Non-Disclosure Agreements

5.3.6. Recorded verbal consent

5.3.7. SMS consent from a verifiable contact source

5.3.8. Other legal permission of written consent

5.4. What will not be deemed as valid consent:

5.4.1. Any form of consent whereby the data subject cannot be identified in the consent

5.4.2. Any form of verbal / written consent on behalf of a data subject, without evidence of the data subject's consent or proxy

5.4.3. Any form of verbal/visual consent whereby it is not recorded and whereby the data subject cannot be identified on any such recording

6. **Data acceptance registration**

6.1. Upon receiving confidential, personal, or private data from such subjects, it is mandatory to record the receipt of such data on a register in the following instances:

6.1.1. When collecting the data in person

6.1.2. When collecting the data using a courier

6.1.3. When collecting the data in a physical format such as:

6.1.3.1. Physical paper documents

6.1.3.2. Physical hard drives/storage devices

7. Data Accuracy and Completeness

7.1. All data collected must serve a purpose and must be of future or current use (Relevance). All data that are to be used therefore must be accurate, complete, and up to date. It is extremely important to verify the source, accuracy, and completeness of data directly with the subject matter and when permitted by data subject to do so.

7.2. It is further recommended that all data be verified and reviewed within the intervals specified in the Legislation Compliance Register for changes, revisions, and or outdated compliance certificates where applicable.

8. Data Storage, Transfer or Discarding Assessment

8.1. When considering taking ownership of data, it is very important to plan the data flow and movement from yourself as the data custodian till ultimate data safeguarding in a “secure safe zone” environment.

8.2. This process involves:

8.2.1. taking ownership of the data and becoming the initial data custodian

8.2.2. transferring or immediately storing the data to a “safe secure zone”

8.2.3. distributing or passing off the data between data end-users

8.2.4. eventual discarding of the data / archiving data

8.3. Upon taking receipt and ownership of data (data custodian owns the risk), it is of utmost importance to ensure that the necessary storage facilities/platform and/or requirements are identified and in place to safeguard and secure all confidential, personal, or private information from receiving through till ultimate destruction or data discarding and after.

Thys Botes

MD (Network Claims Assessors)

8.4. Such storage should ensure proper access controls, proper data registration of movements or transfers as well as enable easy data retrieval and destruction/discarding.

8.5. As to assist in such assessments, Network Claim Assessors Group has established a “Secure Safe Zone” storage facility in that we have:

8.5.1. Access controlled servers’ storage (Electronic files)

8.5.2. Access controlled Server Rooms (Hardware)

8.5.3. Access controlled Storage Rooms (Physical Document room)

8.5.4. Access controlled Offices (Meetings, Documents & IT equipment)

8.5.5. Access controlled finance offices/upper-level access

8.5.6. Data retrieval and storage policies

8.5.7. Access controlled mail servers

8.6. Due to the above, it is essential to assess and identify the storage method and needs upfront, as to enable the best practices and fastest secure route to storage and safeguarding of confidential, personal, and private information.

8.7. For this reason, it is strongly advised that all client and supplier data be sent to or collected from a central contact point and central data collection email, that can be encrypted, securely manned, and monitored. To further control or mitigate this risk area, the next sections deal with the storage formats and data movement between or to a “safe secure zone”.

9. Data Storage Format

9.1. The following preferred data storage is permitted by the Network Claim Assessors group:

9.1.1. Electronic data (PDF, Word, Excel, PPT) on official Network Claim Assessors Access controlled servers

9.1.2. Electronic data (PDF, Word, Excel, PPT) on a password protected and encrypted Network Claim Assessors computer devices

9.1.3. Physical Server Rooms for IT hard drives, storage drive, and servers

9.1.4. Physical Financial Statements / Data within the finance secure offices (CFO locked office)

9.1.5. Physical Supplier Statements within finance secure offices

Thys Botes

MD (Network Claims Assessors)

9.1.6. Physical Business Continuity Plan / IT Disaster Recovery Plan (Filed in CEO / COO & CIO Secure office)

9.1.7. Physical files stored in secure product offices and archived.

9.2. It is Network Claim Assessor's best practice to minimize and prevent physical document storage as far as humanly possible. It is recommended that all information be scanned, converted to electronic format as quickly and as soon as possible during the information life cycle. All physical documents must be limited and if legally required, then such must be stored at Network Claim Assessor's "safe secure zone" as soon as possible after initial receipt or generation of such documents/reports.

9.3. Information on removable hard drives, external storage devices must adhere to the information technology security practices as prescribed under the Removable Media Policy.

10. Data Transfer Requirements and Protocol (Data in Transit)

10.1. When data must be transferred between two "safe secure zones", all protocols to limit exposure of a data breach must be followed, during such transfer phase. Which include but are not limited to the following:

10.1.1. Limit trips from collection source (client/supplier) to Safe Secure Zone storage point (No personal or unneeded trips or stops)

10.1.2. Do not store the documents in the plain or open site during transit

10.1.3. Ensure documents are placed in a lockable bag, suitcase, or backpack that has a hidden Zip locks setup

10.1.4. When using private transport, ensure documents are kept in a lockable rear boot of a car, or underneath the seat where not possible as to limit visibility.

10.1.5. When using public transport, ensure that the bag with information is controlled and held at all times and not out of reach or sight.

10.1.6. Ensure that your bag, luggage is in sight at all times and never left unattended.

10.1.7. When reaching the "Safe Secure Zone", prioritize handover of information as follows:

10.1.7.1. Confidential, personal, and or private information, may not be moved, transferred, without a formal movement register.

11. Data Discarding

11.1. When data no longer serves any purpose or no longer has a use, it is mandatory to discard such data or information. This is to limit any potential data breach exposure and losses to our business resulting from such risks.

11.2. During the discarding phase, it is discovered that data still hold potential future benefits use or needs, the best practice is to formally Archive such data files.

11.3. When discarding data, the rules and guidelines set out under the Data Disposal and Destruction Policy must be adhered to.

12. Data Archiving

12.1. It remains the Head of each product department and support service department to annually assess what documents are in the archive and which documents must be purged and discarded under the guideline of the Disposal and Destruction Policy. Please refer to the internal retention policy for guidelines.

13. Data Retrieval

13.1. When data is initially stored, it must be done in such a way, that it can easily be tracked, traced, and retrieved upon request. As to ensure that data retrieval is done by only valid, permitted, and authorized users, data/information must always be stored in line with the Information Classification Policy.

14. Data Revisit and Continuous Update

14.1. When data is collected from an external data subject and frequently used or shared or of a personal/private nature, it is the responsibility of the data custodian to ensure that the data used, held in possession is accurate and up to date and does not cause any disrepute to the data subject.

15. Data Breach

15.1. When a user suspects that there has been a breach in data access, confidentiality, or private information has escaped the secure zone to unauthorized users, such a user should follow the steps defined within the Incidents and Non-Conformance Procedure.

16. The following records need to be kept and stored securely.

16.1. All records must be stored in the pre-allocation location. All physical copies need to be stored in a lockable cabinet or drawer.

Thys Botes
MD (Network Claims Assessors)

17. Enforcement

17.1. 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.

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

CEO name THYS BOTES CEO signature 

Signed at PAROW on this 12 day of APRIL 20 22