Introduction

Lawful processing of Personal Information Personal information may be processed if it is done in accordance with the Act and the responsible party adheres to the conditions for the lawful processing of personal information:

a) Accountability

b) Processing limitation

c) Purpose specification

d) Further processing limitation

e) Information quality

f) Openness

g) Security safeguards

h) Data subject participation

Part 1: The Information Officer Condition 1 - Accountability

Information officer

As a responsible party, NEBEAU ensures that the conditions for the lawful processing of personal information is complied with and has appointed an information officer who will take responsibility and accountability for the provisions of the Act. As NEBEAU is a Private body, the information officer is the Head of the entity. Do to the size of the company, NEBEAU has elected not to appoint any deputy information officers at this time.

We have identified NOLENE OWEN to be our Information Officer in her capacity as Director.

The Information Officer has accepted and acknowledged her role in this capacity and is aware of the accountability that comes with it.

- She will be responsible for implementing the POPI policies and procedures within the entity
- She will be afforded sufficient time, adequate resources and the financial means to devote to matters concerning POPIA and PAIA.

- She will be accessible to all relevant parties within the entity as well as outside to be able to fulfill the duties.

The Information Officer was registered with the Regulator. Should there be a change in Information officer, the particulars will be updated accordingly.

Deputy Information Officer

Section 17 of PAIA provides for the designation of a Deputy Information Officer of a public body, and section 56 of POPIA extends the designation of a Deputy Information Officer for a private body. In order to render a body as accessible as reasonably possible the Information Officers of public and private bodies must designate one or more Deputy Information Officers as are necessary, depending on the structure and size of such bodies.

A Deputy Information Officer should have a reasonable understanding of POPIA and PAIA in order to execute his or her duties. A Deputy Information Officer should have a reasonable understanding of the business operations and processes of a body. An employee(s) with institutional knowledge, at a level of management or above, is preferred for designation as a Deputy Information Officer(s). It is recommended that a Deputy Information Officer should report to the highest management office within a Body.

A person designated as a Deputy Information Officer should be afforded sufficient time, adequate resources and the financial means to devote to matters concerning POPIA and PAIA.

A Deputy Information Officer should be accessible to everyone, particularly to a data subject in respect of POPIA or a requester, in terms of PAIA.

Due to the size and operation requirement of the Company, we have opted not to appoint a Deputy Information Officer at this time.

Part 2: Personal Information Impact Assessment

A personal information impact assessment was performed to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.

Data Subjects

The following data subjects have been identified during the impact assessment for whom the processes will be implemented as per Part 3: Processing Personal Information:

a) Employees and prospective employees
b) Customers
c) Suppliers
d) COVID tracing

Processing of special personal information

We process special personal information for the following data subjects:

Data subject	Reason for processing
Prospective employees	For possible employment purposes
Employees	For employment purposes
Customers	For credit sales and invoicing
Suppliers	For procurement purposes
COVID	For contact tracing

We only process this information if one of the following is applicable:

a) Consent is obtained from the Data subject;
b) Processing is necessary for the establishment, exercise or defense of a right or obligation in law;
c) Processing is necessary to comply with an obligation of international public law;
d) Information has deliberately been made public by the data subject;
e) Processing is authorised by Regulator.

We do not gather or process the following information:

a) Information for historical, statistical or research purposes;
b) Religious or philosophical beliefs;
c) Race or ethnic origin;
d) Trade union membership;
e) Political persuasion;
f) Health or sex life;
g) Criminal behaviour or
h) Biometric information
i) Personal information of children

NEBEAU has not applied for prior authorisation from the Regulator for any exceptions to the processing as above.

Part 3: Processing Personal Information

NEBEAU implements the following policies and procedures on the personal information of all data subjects identified during the Personal Information Impact Assessment as per Part 2 above.

Condition 2 – Processing Limitation

Minimality

NEBEAU will ensure that it only process data that it actually needs for the purposes of running the business, executing its contracts and protecting its legitimate interests. All personal information obtained per data subject will be evaluated against the purpose for processing to identify if it is adequate, relevant and not excessive. If it does not comply, it will not be processed.

Collection of data

NEBEAU will always aim to collect data directly from a data subject. In the following instances it is not required by the Act to receive it directly from the data subject and as such will not be a contravention:

a) The information is contained in or derived from a public record or has deliberately been made public by the data subject;
b) The data subject or a competent person where the data subject is a child has consented to the collection of the information from another source;
c) Collection of the information from another source would not prejudice a legitimate interest of the data subject;
d) Collection of the information from another source is "necessary":
    a. To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
    b. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act 34 of 1997);
    c. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
    d. In the interests of national security; or
    e. To maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied.
e) Compliance would prejudice a lawful purpose of the collection; or
f) Compliance is not reasonably practicable in the circumstances of the particular case.

Consent, justification and objection

NEBEAU will only process personal information in terms of our personal information impact assessment, if any of the following applies:

a) Consent is obtained from the Data subject;
b) Processing is necessary for the establishment, exercise or defense of a right or obligation in law;
c) Processing is necessary to comply with an obligation of international public law;
d) Information has deliberately been made public by the data subject;
e) Processing is authorised by Regulator.

We do not gather or process the following information:

a) Information for historical, statistical or research purposes;
b) Religious or philosophical beliefs;
c) Race or ethnic origin;
d) Trade union membership;
e) Political persuasion;
f) Health or sex life;
g) Criminal behaviour or
h) Biometric information
i) Personal information of children

NEBEAU bears the burden of proof for the data subject's or competent person's consent as referred to above. The way in which consent was received, if relevant, or the reason why consent is not necessary, is documented per data subject.

The data subject or competent person may withdraw his, her or its consent, or object to the processing of personal information, at any time. The data subjects are also informed of the consequences should they withdraw consent, and where consent cannot be withdrawn as the personal information is required by law or for the proper execution of the contract or agreement.

Withdrawal of consent or objection to processing personal information, if not done at the inception stage of agreements or when the information is obtained, may be done on Form 1 as per the regulations.

Where data subjects object to the processing of personal information, and the processing is not necessary for the proper execution of a contract or not required by law, we will stop processing the data immediately.

Condition 3: Purpose specification

Personal information will only be collected for a specific, explicitly defined and lawful purpose related to a function or activity:

Data subject	**Reason for processing**
Prospective employees	For possible employment purposes
Employees	For employment purposes
Customers	For credit sales and invoicing
Suppliers	For procurement purposes
COVID	For contact tracing

The data subjects are informed of:

a) The nature or category of the information being collected;
b) The purpose for processing thereof;
c) When such information is not received directly from them, the source thereof;
d) The name and address of the responsible party;
e) The retention period of the information;
f) Whether or not the supply of the information by that data subject is voluntary or mandatory;
g) The consequences of failure to provide the information;
h) Any particular law authorising or requiring the collection of the information;
i) If the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organization;
j) Recipient or category of recipients of the information;
k) Existence of the right of access to and the right to rectify the information collected;
l) Existence of the right to object to the processing of personal information;
m) Right to lodge a complaint to the Information Regulator.

It will not be necessary to provide the information as above if:

a) The data subject or a competent person where the data subject is a child has provided consent for the non-compliance;
b) Non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of this Act;
c) Non-compliance is "necessary" (as previous described):
d) Compliance would prejudice a lawful purpose of the collection;
e) Compliance is not reasonably practicable in the circumstances of the particular case; or
f) The information will:
    a. Not be used in a form in which the data subject may be identified; or
    b. Be used for historical, statistical or research purposes.

Data Retention

Personal information will not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless:

a) Retention of the record is required or authorised by law;
b) The responsible party reasonably requires the record for lawful purposes related to its functions or activities;
c) Retention of the record is required by a contract between the parties thereto; or
d) The data subject or a competent person where the data subject is a child has consented to the retention of the record.

NEBEAU's policy is to retain all information for a maximum of 10 years after the conclusion of the transaction, contract or service for which it was obtained. This will allow NEBEAU to comply with all legislative requirements of retention. This will be communicated to data subjects as provided.

Should a Data subject object to this, the retention period will default back to the prescribed period as per legislation. These Data subjects will be flagged to ensure that their records are destroyed after the retention period.

Condition 4: Further processing limitation

Further processing refers to any processing of personal information for reasons other than those for which it was obtained and that have already been communicated to the data subject. To assess whether further processing is compatible with the purpose of collection we will take the following into account:

a) The relationship between the purpose of the intended further processing and the purpose for which the information has been collected;
b) The nature of the information concerned;
c) The consequences of the intended further processing for the data subject;
d) The manner in which the information has been collected; and
e) Any contractual rights and obligations between the parties.

Information may be processed further without performing the above considerations if:

a) The data subject or a competent person where the data subject is a child has consented to the further processing of the information;
b) The information is available in or derived from a public record or has deliberately been made public by the data subject;
c) Further processing is “necessary” (as previous described);
d) The further processing of the information is necessary to prevent or mitigate a serious and imminent threat to public health or public safety; or the life or health of the data subject or another individual;
e) The information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form; or
f) The further processing of the information is in accordance with an exemption granted.

The above considerations will be made every time information is subjected to further processing and documented per class of data subject for which further processing may be necessary.

Condition 5: Information quality

A responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

To ensure quality of personal information, data subjects are provided with the opportunity to contest the accuracy of the information. On receipt of a request for correction we will, as soon as reasonably possible:

a) Correct the information or destroy or delete the information, depending on the relevant request;
b) Provide the data subject, to his or her satisfaction, with credible evidence in support of the information, or where agreement cannot be reached between us and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made;
c) Inform each person or body or responsible party to whom the personal information has been disclosed of these steps;
d) Inform the data subject of the result of the request.

The process for ensuring information quality per data subject is as follows:

Data Subject	**Process**
Employees	Employees to submit information to the person responsible for HR and Payroll, to ensure that all information is amended when changes occur.
Customers	Customer liaison officers or reps to provide information to Warehouse / Logistics for update of the system.
Suppliers	Accountant to update and ensure accuracy of supplier information.
Shareholders	Company secretary compiles and safeguards the information.
Directors	Company secretary compiles and safeguards the information.

Part 4: Data Subject Participation

The data subject has the right to be aware of their personal information being processed and to take part in this process by either objecting to such processing or ensuring that the information is correct by requesting the responsible party to remove or correct incorrect information.

Condition 6: Openness

NEBEAU will take all reasonably practicable measures to inform data subjects about the personal information being processed and other information as documented under Condition 3: Purpose specification.

Any data subject may, having provided adequate proof of identity, request us to confirm whether or not we hold personal information about them and the identity of third parties who have, or have had access to the information. This is done in terms of the Promotion of Access to Information Act. If, in response to a request as above, personal information is communicated to a data subject, the data subject will be advised of their right to request the correction of information. A data subject may need to pay a fee for these services provided to the data subject to enable us to respond to a request. These fees will always be charged in terms of the Promotion of Access to information Act. Where these fees are applicable, we will give the applicant a written estimate of the fee before providing the services.

Part 5: Safeguarding of Information

Condition 7: Security safeguards

NEBEAU will secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent:

a) Loss of, damage to or unauthorised destruction of personal information; and
b) Unlawful access to or processing of personal information.

NEBEAU performed a risk assessment to identify internal and external risks to personal information in our possession or under our control, based on where information is stored and who has access to it.

The risks identified are as follows:

Risk identified	**Mitigating safeguards implemented**
Loss of Data	Hosted cloud-based system includes daily backup of data Weekly and monthly hard drive backups of local information Shared information on One drive includes daily backup of data
Unauthorised access or theft of data	Passwords, encryption, antivirus software and firewalls
Unauthorised sharing of data	Access control & encryption
Inaccurate and outdated data	Client liaison officers or reps to confirm basic information (such as contact number and delivery address) with customers with each transaction. Supplier information to be confirmed before every payment Employee details to be amended as advised by the employee

These safeguards are monitored on a regular basis and updated as necessary where deficiencies are identified.

Operator services

NEBEAU does not make use of any operators to process personal information.

NEBEAU does not perform services as an operator.

Part 6: Breaches

Notification of security compromises

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, NEBEAU shall notify:

a) The Regulator; and
b) The data subject, unless the identity of such data subject cannot be established.

The notification will be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

The notification to a data subject shall be in writing and communicated to the data subject in at least one of the following ways:

a) Mailed to the data subject's last known physical or postal address;
b) Sent by e-mail to the data subject's last known e-mail address;
c) Placed in a prominent position on the website of the responsible party;
d) Published in the news media; or
e) As may be directed by the Regulator.

The following information will be included in notifications:

a) Description of the possible consequences of the security compromise;
b) Description of the measures that we intend to take or have taken to address the security compromise;
c) A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
d) If known, the identity of the unauthorised person who may have accessed or acquired the personal information.

Part 7: Direct Marketing

The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail is prohibited unless the data subject:

a) Has given his, her or its consent to the processing; or
b) Is a customer of the responsible party and:

i. The responsible party has obtained the contact details of the data subject in the context of the sale of a product or service;
ii. The processing is for the purpose of direct marketing of the responsible party's own similar products or services; and
iii. The data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its electronic details.

Consent

A responsible party who wishes to process personal information of a data subject for the purpose of direct marketing by electronic communication must submit a request for written consent to that data subject. This consent must be positive and not an absence of objection. Where Direct marketing is sent by electronic means, it must contain details of the identity of the sender or the person on whose behalf the communication has been sent, and an address or other contact details to which the recipient may send a request that such communications cease.

A responsible party may approach a data subject only once, and in the prescribed manner and form, for this consent. If the consent has been withheld previously, the data subject may not be approached again to request consent or to provide such direct marketing. The data subject may opt-in to the direct marketing again should they choose to.

Direct marketing by electronic means to new potential clients

NEBEAU will request consent prior to any direct marketing by electronic means.

Direct marketing by electronic means to existing clients

NEBEAU communicates to customers via electronic means on various issues, but only to clients that have opted-in for these communications.

Directories

A data subject who is a subscriber to a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which his, her or its personal information is included, must be informed, free of charge and before the information is included in the directory:

a) about the purpose of the directory;
b) about any further uses to which the directory may possibly be put, based on search functions embedded in electronic versions of the directory.

A data subject must be given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its personal information or to request verification, confirmation or withdrawal of such information if the data subject has not initially refused such use.

NEBEAU does not make their directories available to the public.

Part 8: Internal training and awareness

Training will be provided at regular intervals to employees as well as to the Information Officer and Deputy Information Officers in order to ensure that everyone is informed and keep abreast of the requirements of POPIA and PAIA, as well as the policies and procedures within the entity to ensure compliance.

Training will be provided as follows:

New employees	Formal training session upon employment as part of the induction process
Existing employees	Internal discussion on the requirements and responsibilities to be held at least once per year
Information officer	None (Compiled this manual)
Deputy Information Officers	When appointed

Part 9: Information Regulator

The Information Regulator has jurisdiction over the Act to educate, guide, monitor and enforce the Act.

Reporting to the Information regulator

The entity is required to report any breach of personal information to the Information Regulator.

Complaints

Any person may submit a complaint to the Regulator in the prescribed manner and form alleging interference with the protection of the personal information of a data subject.

A responsible party or data subject may submit a complaint to the Regulator in the prescribed manner and form if he, she or it is aggrieved by the determination of an adjudicator.

Part 10: Promotion of Access to Information Act

A responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of the Promotion of Access to Information Act.

Section 51: Manual on functions of, and index of records held by, private body

The head of a private body must make a manual available containing:

a) in general:
   a. the postal and street address, phone and fax number and, if available, electronic mail address of the head of the body;
   b. such other information as may be prescribed;
b) insofar as PAIA is concerned:
   a. a description of the guide of how to use the PAIA as referred to in section 10, if available, and how to obtain access to it;
   b. the latest notice, if any, regarding the categories of records of the body which are available without a person having to request access in terms of PAIA;

c. a description of the records of the body which are available in accordance with any other legislation;
d. sufficient detail to facilitate a request for access to a record of the body, a description of the subjects on which the body holds records and the categories of records held on each subject;

c) insofar as the Protection of Personal Information Act, 2013, is concerned:
   a. the purpose of the processing;
   b. a description of the categories of data subjects and of the information or categories of information relating thereto;
   c. the recipients or categories of recipients to whom the personal information may be supplied;
   d. planned transborder flows of personal information; and
   e. a general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information which is to be processed.

The head of a private body must on a regular basis update the manual.

The manual must be made available:

a) on the web site, if any, of the private body;
b) at the principal place of business of the private body for public inspection during normal business hours;
c) to any person upon request and upon the payment of a reasonable amount; and
d) to the Information Regulator upon request.