OTASA POPIA DATA RETENTION POLICY

1. Purpose

1.1. The purpose of this Policy is to set out the required retention periods for specified categories of information, including personal information, and to establish minimum standards to be applied when destroying certain personal information within OTASA.

1.2. The Policy applies to all officers, directors, employees, agents, affiliates, contractors, consultants, advisors or service providers of the organisation that may collect, process, or have access to information (including personal information). It is the responsibility of each and every party to whom the Policy applies to ensure that he/she/it understand and complies with this Policy.

1.3. The Policy will apply to all data/information held by the organisation, including personal information as defined in the Protection of Personal Information Act ("POPIA"), irrespective of the format it is held in, including but not limited to, electronic information, electronic mail, hard copy documents, digitally recorded information such as voice recordings, photographs and video footage, CCTV footage, information generated by access control systems, COVID screening, etc.

2. Definitions

The terms listed hereafter shall bear the following meanings:

2.1. **"Data"** means all information in possession or under the control of the organisation, irrespective of the nature thereof;

2.2. **"De-identify"** means in relation to personal information of a data subject, means to delete any information that—

(a) identifies the data subject;

(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.

2.3. **"PAIA"** means the Promotion of Access to Information Act 2 of 2000;

2.5 **"Personal information"** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to —

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
(d) the biometric information of the person;
(e) the personal opinions, views or preferences of the person;
(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
(g) the views or opinions of another individual about the person; and
(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

2.4. **"Personal information of children"** means personal information about a natural person under the age of 18 years as referred to in section 34 of POPIA

2.5. **"POPIA"** means the Protection of Personal Information Act, 4 of 2013;

2.6. **"Special Personal Information"** means personal information as referred to in section 26 of POPIA; and

2.7. **"Record"** means any recorded information—
(a) regardless of form or medium, including any of the following:
(i) Writing on any material;
(ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
(iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
(iv) book, map, plan, graph or drawing;
(v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
(b) in the possession or under the control of a responsible party;
(c) whether or not it was created by a responsible party; and
(d) regardless of when it came into existence

3. Retention Rules

3.1. <u>General Principles</u>

3.1.1. Information must be held in terms of statutory retention periods and maybe held in the legitimate interest of the organisation.

3.1.2. It is the responsibility of the Information Officer to determine retention periods, in respect of information that is held otherwise than in terms of statutory retention periods.

3.1.3. In the event any category of records is not specified in this Policy (and in particular within the Data Retention Schedule) and unless otherwise mandated by applicable law, the required retention period for such record will be determined by the Information Officer on request, taking into consideration the principles set out in POPIA.

3.2. Retention Periods

3.2.1. The Information Officer defines the time period for which records should to be retained as set out in the Data Retention Schedule.

3.2.2. As an exemption, retention periods within the Data Retention Schedule can be extended within the discretion of the Information Officer, within the requirements of POPIA, where special circumstances justifiable in terms of POPIA or PAIA exist, which may include protection against potential litigation, pending litigation, request by or consent of the data subject, etc.

3.3. Destroying and De-identifying Data

3.3.1. The organisation and its employees should, on a regular basis, review all data and parts thereof in terms of this Policy, irrespective of the format thereof and where it is stored, to determine whether the data should be retained, de-identified, destroyed or deleted, either because of the expiry of the retention period or if the reason for which it was collected or retained is no longer relevant.

3.3.2. The ultimate control and responsibility for the destruction of data is the responsibility of the Information Officer.

3.3.3. If a decision is made to retain records for historical, research or statistical purposes, the information should be de-identified.

3.3.4. Once the decision is made to destroy or delete data in accordance with this Policy and the Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality.

3.3.5. In this context, employee delegated for this purpose by the Information Officer shall perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way. The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the Information Officer subcontracts for this purpose. Any applicable general provisions under relevant data protection laws and the organisation's Privacy Policy, shall be complied with.

3.4. Breach, Enforcement and Compliance

3.4.1. It is the responsibility of the Information Officer to ensure that the entire organisation complies with this Policy.

3.4.2. Any suspicion of a breach of this Policy must be reported to the Information Officer immediately. All instances of suspected breaches of the Policy shall be investigated and action taken as appropriate.

3.4.3. Failure to comply with this Policy may result in serious adverse consequences, including, but not limited to, loss of confidence, litigation and loss of competitive advantage, financial loss, administrative fines imposed by the Regulator and damage to the organisation's reputation, personal injury, harm or loss.

4. **Record Disposal**

4.1. Destruction Method

4.1.1. *Level I* records are those that contain information that is at the highest security and confidentiality level and those that include any personal information. These records shall be disposed of in a manner that the data is entirely destroyed and cannot be reconstituted. Disposal of the records must include proof of destruction.

4.1.2. *Level II* records are proprietary records that contain confidential information such as parties' names, signatures and addresses, or which could be used by third parties to commit fraud, but which do not contain any personal information. The records shall be disposed of in a manner that the data is entirely destroyed and cannot be reconstituted. Disposal of the records must include proof of destruction

4.1.3. *Level III* records are those that do not contain any confidential information or personal information such as organisation records in the public domain. These may be shredded and disposed of through recycling. Disposal of the records do not need proof of destruction.

5. Retention Register

5.1. OTASA Retention period is 5 years unless otherwise advised by internal needs.