SAICA GROUP
General Personal Data Protection & Retention Policy

SAICA
THE SOUTH AFRICAN INSTITUTE OF CHARTERED ACCOUNTANTS

Table of Contents

1 Introduction

1.1 The South African Institute of Chartered Accountants and its entities ("SAICA") recognises the fundamental rights and freedoms of natural persons, more specifically the right to privacy which includes the right to the protection against the unlawful collection, retention, dissemination and use of Personal Information and all other Processing activities by SAICA, subject to justifiable restrictions that are aimed at protecting other rights and important interests.

1.2 SAICA is committed to protect the Personal Information of SAICA's employees, its members and other stakeholders from unlawful and unfair Processing or damaging actions by SAICA, its employees, its stakeholders and/or third parties, either knowingly or unknowingly.

1.3 SAICA's Board and the CEO is committed to ensure alignment with the POPIA, PAIA and GDPR principles, standards and conditions, and addition thereto certain of these principles, standards and conditions are entrenched in SAICA's internal controls, policies and procedures governing its corporate conduct.

2 Objective of this Policy

2.1 SAICA intends to establish a culture of lawful, fair and transparent Processing of Personal Information and in addition thereto ensure that Personal Information is collected for specified, explicit and legitimate purposes, without imposing restrictions that are contrary to any of SAICA's Policies and/or its Regulatory Universe.

2.2 It is intended as a formal communication of SAICA's philosophy and approach to regulate the manner in which it processes Personal Information in accordance to the principles, standards and conditions that is prescribed for the lawful Processing of Personal Information.

2.3 It confirms the required designation of the DPO, its authority and Management's support thereof. It also assists in reducing risk by ensuring better preparedness for a compliance audit and identifying Personal Data Protection risks.

2.4 It outlines the data collection, retention, Anonymisation, Pseudonymisation, storage, access and accuracy procedures, as well as the objection against Processing, notification of data breaches, obtaining, recording and management of a consent and withdrawal of a consent by a Data Subject.

2.4.1 It further outlines the security measures required in terms of:

2.4.1.1 operators Processing Personal Information on behalf of the SAICA;

2.4.1.2 the retention and disposal of records and the retention and disposal of electronic documents;

2.4.1.3 integrity and confidentiality of Personal Information.

2.4.2 It is further intended to inform the Board, CEO, employees, members and all stakeholders of what is expected of them with regard to compliance matters with regard to Personal Information Protection, including but not limited to:

2.4.2.1 the key principles, standards and conditions, including the minimum principles, standards and conditions for compliance and management of SAICA's Compliance Risk in terms of Personal Information Protection;

2.4.2.2 the roles and responsibilities applicable throughout SAICA, which support the compliance processes in terms of Personal Data Protection; and

2.4.2.3 the reporting requirements established within the Personal Data Protection Process.

2.4.3 The principles, standards and conditions outlined in this document are to be applied at all levels of operation and functions, it thus applies to the CEO, Board and all employees.

2.4.4 Effective and efficient Personal Information protection and security is a team effort involving the participation and support of every SAICA employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these policies, procedures and guideline and to conduct their activities accordingly.

3 Interpretation and Definitions

In this Policy-

3.1 the headings are for convenience and shall be disregarded in construing this Policy;

3.2 unless the context indicates a contrary intention, the singular shall include plural and vice versa;

3.3 a natural person includes a juristic person and vice versa;

3.4 where any term is defined within a particular clause other than this **clause 3**, the term so defined shall bear the meaning ascribed to it in that clause wherever it is used in this Policy, unless it is clear from the clause in question that such a defined term has limited application to the relevant clause;

3.5 any reference to any statute, regulation or other legislation shall be a reference to that statute, regulation or other legislation as amended or substituted from time to time; and

3.6 unless the context clearly indicates a contrary intention, the following expressions shall bear the meanings set opposite them below and cognate expressions shall bear corresponding meanings:

3.6.1 **"Anonymisation"** means the irreversible removal of personal identifiers from information so that the Data Subject is no longer identifiable. Anonymised information therefore no longer falls within the definition of Personal Information;

3.6.2 **"AudCo**" means SAICA's Audit and Risk committee of the Board that is responsible for oversight of the Compliance Function, among other duties, in SAICA;

3.6.3 **"Board"** means the board of SAICA, including any other person/s with whom the ultimate responsibility for compliance may rest;

3.6.4 **"CEO"** means the Chief Executive Officer of SAICA who is accountable to the Board is ultimately responsible for regulatory compliance;

3.6.5 **"Compliance**" means the management and identification of the on-going obligations and requirements, exposures, risks and opportunities arising under –

3.6.5.1 legislation and regulations;

3.6.5.2 principles, standards, guidelines;

3.6.5.3 standard codes of practice and conduct (legal and voluntary); and

3.6.5.4 policies and procedures;

3.6.5.5 and then designing and implementing an effective assurance system and culture so that the obligations, risks and opportunities are properly met and managed;

3.6.6 **"Compliance Incident**" means an event or an occurrence which has resulted in SAICA being exposed or potentially exposed to a prospective or actual Compliance Risk;

3.6.7 **"Compliance Risk**" means the prospective or actual risk which SAICA is exposed to as a result of non-adherence and/or the inefficient and ineffectiveness of the procedures implemented by SAICA to ensure compliance to relevant statutory, regulatory, supervisory requirements, key internal and external stakeholder's expectations and the society as a whole;

3.6.8 **"Consent"** means a Data Subject's voluntary, specific, informed and unambiguous indication of its wishes by a statement or a clear affirmative action, signifies its agreement to the Processing of its Personal Information, as defined in Section 1 of the POPIA and Article 4 of the GDPR, whichever is applicable under the circumstances;

3.6.9 **"Constitution"** means the Constitution of the Republic of South Africa, 108 of 1996;

3.6.10 **"Controller"** means:

3.6.10.1 a Controller as defined in Article 4 of the GDPR; and

3.6.10.2 a Responsible Party, as defined in Section 1 of the POPIA;

whichever is applicable under the circumstances;

3.6.11 **"Data Protection Regulatory Framework"** means the legislation, regulations, standards and codes of good practices in SAICA's Regulatory Framework in relation to the protection of Personal Information of Data Subjects;

3.6.12 **"Data Retention"** means the continued storage of SAICA's information for compliance or business reasons. SAICA may retain data for various different reasons, including but not limited to, compliance with legislation, regulations, principles, standards, conditions and/or codes of good practice. SAICA should be able to recover business critical data in the event of a site-wide data loss;

3.6.13 **"Data Subject"** means the person to whom the Personal Information relates, as defined in Section 1 of the POPIA and Article 4 of the GDPR, whichever is applicable under the circumstances;

3.6.14 **"Division**" means a division of SAICA;

3.6.15 **"DPO"** means:

3.6.15.1 a Data Protection Officer, as defined in Articles 37 to 39 of the GDPR;

3.6.15.2 an Information Officer, as defined in section 1 of the POPIA;

whichever is applicable under the circumstances;

3.6.16 **"DTGC"** means the Digital Transformation Governance Committee of the Board that is responsible for assisting the Board in overseeing SAICA's strategic direction and investment in digital transformation and technology;

3.6.17 **"Employee"** means a permanent-, fixed-term or temporary employee of SAICA;

3.6.18 "**Enterprise Risk Management Framework**" means SAICA's approach to the management of all categories of risk, including policy and structure (people, systems and process);

3.6.19 **"GDPR"** means the General Data Protection Regulation (EU) 2016/679, which comes into effect on the 25th of May 2018;

3.6.20 **"Information Regulator"** means the Information Regulator established in terms of Section 39 of the POPIA;

2.1.1. **"ManCo"** means the Management Committee of SAICA**;**

2.1.2. **"Material Compliance Incident"** means a significant Compliance Incident which has impaired SAICA's integrity and has resulted in material damage to SAICA's reputation, financial loss, or any legal or regulatory sanctions imposed, due to a failure to comply with SAICA's regulatory universe;

2.1.3. **"MDS"** means a Minimum Data Set;

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

2.1.5. **"Personal Data/Information Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

2.1.6. **"Personal Information"** means information which relates to an identified or identifiable natural person, and where applicable, an identifiable, existing juristic person, in particular by reference to an identifier factor such as a name, identification number, location data, online identifiers or other specific factors such as physical, physiological, genetic, mental, economic, cultural or social identity of a natural person, as defined in Section 1 of the POPIA and Article 4 of the GDPR, whichever is applicable under the circumstances;

2.1.7. **"POPIA"** means the Protection of Personal Information Act, 4 of 2013 and its Regulations, which effective date is still to be determined;

2.1.8. **"Processing"** means any operation or set of operations performed on Personal Information or sets of Personal Information, as defined in Article 4 of the GDPR and Section 1 of the POPIA, whichever is applicable under the circumstances;

2.1.9. **"Processor"** means:

2.1.9.1. a Processor, as defined in Article 4 of the GDPR; and

2.1.9.2. an Operator, as defined in Section 1 of the POPIA;

whichever is applicable under the circumstances;

2.1.10. **"Pseudonymisation"** means the Processing of personal data in such manner that the Personal Information can no longer be attributed to a specific Data Subject, as defined in Article 4 of the GDPR;

2.1.11. **"Record of Processing Activities"** means Detailed records of the Personal Information Processing activities that a Data Controller or Processor is required to maintain and make available under the GDPR;

2.1.12. **"Regulatory Authority**" means an institution established to oversee the implementation of a particular Data Protection legislation. In terms of the GDPR an independent public authority has been established by the United Kingdom or another state to regulate compliance with data protection law by Controllers and Processors and take enforcement action in the case of non-compliance. In the UK the supervisory authority is the Information Commissioner's Office (ICO). In terms of the POPIA an Information Regulator has been established, in regards to Data Subjects situated within the Republic of South Africa;

2.1.13. **"Regulatory Framework"** means all applicable and prioritised legislation, regulations, standards, codes of good practices in terms of SAICA's operations, as set out in the SAICA Compliance Policy;

2.1.14. **"Regulatory Risk**" means the risk or potential risk that SAICA may be exposed to should it not comply with regulatory requirements or where it may exclude provisions of relevant regulatory requirements from its operational procedures;

2.1.15. **"Restriction"** means the marking of stored Personal Information with the aim of limiting their Processing in future, as defined in Section 1 of the POPIA and Article 4 of the GDPR, whichever is applicable under the circumstances;

2.1.16. "**SAICA**" means the South African Institute of Chartered Accountants and its entities;

2.1.17. **"SAICA's Founding Documents"** means the SAICA Constitution and its By-Laws;

2.1.18. "**Senior Executives**" means the Senior Executives of SAICA constituting ManCo; and

2.1.19. **"Special Personal Data Information"** means Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, as defined in Section 26 of the POPIA and Article 9 (1) of the GDPR, whichever is applicable under the circumstances. In addition, the SAICA's definition of High Risk Confidential Information includes the following personal data: Any other information that would cause significant damage or distress to an individual, i.e. it was disclosed without their consent, such as bank account and financial information, examination/assessment marks or grades; and

2.1.20. "**The/This Policy**" means this SAICA General Personal Data Protection and Retention Policy.

4 Policy Statement of Intent

4.1 SAICA

4.1.1 believes it is of the upmost importance that Personal Information it collects, retains, disseminate, use and process in order to perform its functions and reach its strategic objectives are done in compliance within the scope of its regulatory framework;

4.1.2 is committed to protecting the privacy of Personal Information and ensuring that the appropriate security measures and safeguards are put in place to effectively and efficiently respond to an actual or suspected data breach involving personal data held by SAICA and demonstrating compliance with the regulatory framework concerning the Processing of Personal Information;

4.1.3 recognises its accountability to its employees, members and stakeholders under the legal and regulatory requirements applicable to its operations. It is committed to high standards of integrity and fair dealing in the conduct of its operations, and also complying with both the spirit and the letter of applicable requirements and to always act with due skill, care and diligence;

4.1.4 is committed to the lawful and correct treatment of personal and commercial sensitive Personal Information, based on the fact that it is important for it to maintain the confidence in those it deals with, including its employees, members and any other stakeholder;

4.1.5 will only collect relevant factual Personal Information which it requires in order for it to carry out its operations, functions and to reach its strategic objectives. Only relevant factual information that SAICA requires to know will be captured and it will be clear on the purpose for the collection and use of such information within the MDS;

4.1.6 collects the Personal Information on paper, electronically via a computer or other digital material and deals with such appropriately, together with the necessary safeguards required in terms of the undermentioned Regulatory Framework;

4.1.7 details the procedures for the retention and disposal of information to ensure that SAICAC carries this out consistently and that it fully documents any actions taken, unless otherwise specified the retention and disposal refers to both hard and soft copy documents; and

4.1.8 ensures that it is compliant with the Regulatory Framework and that it has at least one legitimate reason for the Processing of the Personal Information, alternatively that a consent to process was obtained.

4.2 The Data Protection Regulatory Framework includes, but are not limited to:

4.2.1 the Constitution;

4.2.2 the POPIA;

4.2.3 the PAIA; and

4.2.4 the GDPR.

4.3 The interpretation of the Data Protection Regulatory Framework is supported by this Policy and its associate procedures and guidelines, and is designed to ensure that SAICA is compliant therewith. Should there be any possibility of ambiguity in interpretation, guidance is provided to minimise any risk and therefor protect the Data Subject as well as balance such with SAICA's ability to continue to perform its various operations and functions.

4.4 The principles, standards and conditions of the Data Protection Regulatory Framework further enhance the additional rights and freedoms Data Subjects can expect and it addresses the ever changing technology environment, which has various options for the collection, storage, sharing and use of Personal Information. It further includes new expectations with regard to a Data Subjects' consent to process its Personal Information and the necessity of such a consent to be clear on what basis such Personal Information can be processed.

4.5 The purpose of this Policy is to set out the processes, procedures and reporting lines in the event in which SAICA experiences and incident which affects Personal Information.

5 Data Protection by Design and Default

SAICA as a Controller shall:

5.1 at the time of determination of the means of Processing of Personal Information and at the time of the Processing itself, implement appropriate technical and organisational measures, such as Pseudonymisation, which are designed to implement data-protection principles, such as Anonymisation, in an effective manner and to integrate the necessary safeguards into the Processing in order to meet the requirements of the Data Protection Regulatory Framework, subject to the state of the art, the cost implementation and the nature, scope , context and purposes of Processing, and the varying likelihood of severity for the rights and freedoms of natural persons posed by Processing of Personal Information;

5.2 implement appropriate technical and organisational measures to ensure that, by default, only Personal Information which are necessary for each specific purpose of the Processing are processed, which applies to the amount of Personal Information collected, the extent of the Processing, the period of the storage and accessibility, more specifically such measures shall ensure that by default Personal Information is not made accessible without human intervention to any indefinite number of natural persons;

5.3 process Personal Information manner that uses technical or organisational measures to ensure appropriate security that protects the data against unauthorised or unlawful Processing and against accidental loss, destruction or damage. The Personal Information collected and processed by SAICA must be stored with the utmost confidentiality and secrecy, may not be used for purposes other than those that justified and permitted the collection thereof, and may not be disclosed or transferred to third parties other than in the cases permitted by applicable law.

5.4 SAICA as a Controller must further ensure that the Key Principles and Conditions of Personal Information, set out herein, are complied with at the time of the determination of the purpose and means of Processing and during the Processing of the Personal Information:

6 Key Principles and Conditions of Personal Information Protection

6.1 Lawfully, fairly and transparently

6.1.1 The Processing of Personal Information must be lawful and in a reasonable manner that does not infringe the privacy of the Data Subject, in that it has legitimate grounds for the processed of the Personal Information. Processing will only be lawful to the extent that one of the following applies:

6.1.1.1 consent by the Data Subject that his/her Personal Information can be processes for one of more purposes;

6.1.1.2 performance of an agreement to which the Data Subject is a party or to take steps on behalf of a Data Subject prior to entering the agreement;

6.1.1.3 compliance with a legal obligation to which SAICA is subject to;

6.1.1.4 protection of vital interest of the Data Subject or of another natural or juristic person;

6.1.1.5 performance of a task carried out in public interest or in an official authority vested in SAICA; and

6.1.1.6 purpose of the legitimate interest pursued by SAICA or a third person, unless such interest is trumped by the interest and fundamental rights of the Data Subject.

6.1.2 It is forbidden to purchase or obtain Personal Information from unlawful sources, from sources that do not sufficiently ensure the lawful origin of such information or from sources whose data has been collected or transferred in violation of the law.

6.1.3 Processing must be fair and reasonable in such a manner that it does not infringe the privacy rights of the Data Subject, subject to the restrictions.

6.1.4 SAICA must be transparent and take appropriate measures to provide information and any communication required, relating to the Processing and further Processing to the Data Subject in a concise, transparent, intelligle and easily accessible form, using clear and plain language. Should the Data Subject request the information, such information may be provided orally if sufficient proof of identity is provided by the Data Subject, it is however advisable that such a request for information is rather provided in writing in the form of **Annexure "A" (Data Subject Access Request Form).**

6.1.5 For the purpose of ensuring fair and transparent Processing, SAICA must inform Data Subjects whose Personal Information is to be collected of the circumstances relating to the Processing in accordance with applicable law. SAICA as a result shall inform Data Subject as follows:

6.1.5.1 On collection of Personal Information SAICA will explain to Data Subjects in a clear, concise and accessible way:

6.1.5.1.1 the identity and contact details of SAICA and its designated DPO;

6.1.5.1.2 that Personal Information we collect and for what purposes we collect and use their information;

6.1.5.1.3 that lawful conditions we rely on to process the Personal Information for each purpose and how this affects their rights;

6.1.5.1.4 whether we intend to process the Personal Information for other purposes and their rights to object;

6.1.5.1.5 the sources from which we obtain their information, where we have received the information from third parties;

6.1.5.1.6 whether we use automated decision making, including profiling, and if so the impact on Data Subjects and their rights to object;

6.1.5.1.7 whether they need to provide information to meet a statutory or contractual requirement and if so, the consequences of not providing the information;

6.1.5.1.8 our obligations to protect their Personal Information;

6.1.5.1.9 to whom we may disclose their Personal Information and why;

6.1.5.1.10 which other countries we may send their information to, why we need to do this and what safeguards apply in each case;

6.1.5.1.11 where relevant, what information we publish and why;

6.1.5.1.12 how Data Subjects can update the information that we hold;

6.1.5.1.13 how long we intend to retain their information; and

6.1.5.1.14 how to exercise their rights under data protection law.

6.1.5.2 We will publish this information on our website and where appropriate in printed formats. We will review the content of these Data Protection Notices regularly and inform our Data Subjects of any significant changes that may affect them.

6.1.5.3 We will provide simple and secure ways for our members, employees and other stakeholders to update the information that we hold about them.

6.1.5.4 Where we process Personal Information to keep people informed about SAICA's activities and events we will provide in each communication a simple way of opting out of receiving further marketing communications.

6.1.6 In these ways we will provide accountability for our use of Personal Information and demonstrate that we will manage Data Subject's Personal Information in accordance with their rights and expectations.

6.1.7 Should the Data Subject already have knowledge of the information or it is impossible to or such would seriously impair the achievement of the objectives of the Processing, SAICA would not be required to give notice of such to the Data Subject.

6.2 Collect for a specified, explicit and legitimate purpose

6.2.1 The Personal Information must not be processed for a purpose other than the purpose for which it was initially collected for, unless such Processing is in public interest, scientific or historical research purposes or statistical purposes.

6.2.2 It must be clear from the outset on the purpose of the collection of the Personal Information and should further Processing be required for a different purpose SAICA must provide the Data Subject with such information to ensure fair and transparent Processing.

6.3 Minimise the Personal Information to be collected to adequate and relevant information, in conjunction with the purpose of the collection and process of the information

6.3.1 The Personal Information collected and held by SAICA must be sufficient, adequate, relevant and not excessive for the purpose it collects or holds it for.

6.3.2 The minimum required Personal Information will be collected and held by SAICA and SAICA will determine a MDS in terms of the different purposes Personal Information is collected for.

6.4 Accurate, where necessary, and keep Personal Information up to date

6.4.1 Ensure that Personal Information is complete, accurate, where necessary kept up to date and not misleading.

6.4.2 Further ensure that every reasonable step is taken to ensure that the Personal Information that is inaccurate in terms of the purpose it is processed, are erased or rectified without delay.

6.5 Keep Personal Information for the period required in terms of the purpose

6.5.1 The time period for which Personal Information will be held, would be considered in conjunction to the purpose for which it is held.

6.5.2 Data will be held for a period merely required in accordance to the purpose and longer should it be legally required from SAICA to do so or solely for archiving purposes which are in public interest, scientific or historical research purposes or statistical purposes, subject to it implementing appropriate technical and organisational measures in order to safeguard the rights and freedoms of Data Subjects.

6.5.3 Should the purpose for Processing be fulfilled and further Processing is required for another purpose, it is necessary to determine whether such a purpose is compatible with the initial purpose by determining whether there is a link between the purposes; the context under which the data was collected, more specifically the relationship between the Data Subject and SAICA; the nature of the Personal Information, whether such is special Personal Information or criminal convictions or offences; possible consequences of the intended further Processing for the Data Subject; and the existence of appropriate safeguards, which may include Encryption and Pseudonymisation.

6.6 Principle of proactive responsibility (accountability)

6.6.1 SAICA shall be responsible for complying with the principles set forth in this Policy and those required by applicable law and must be able to demonstrate compliance when so required by applicable law.

6.6.2 SAICA must perform a risk assessment of the Processing that it carries out in order to identify the measures to apply to ensure that Personal Information are processed in accordance with legal requirements. When so required by law, SAICA shall perform a prior assessment to the risks that new products, services or IT system may imply for personal data protection and shall adopt the necessary measures to eliminate or mitigate them.

6.6.3 SAICA shall retain a record of activities in which the Personal Information Processing that is carried out by SAICA in the course of its activities, is described. In the event of an incident causing the accidental or unlawful destruction, loss or alternation of Personal Information, or the disclosure or unauthorised access to such data, the internal protocols established for such purpose by the SAICA ("IT") and the Legal and Governance Division, and those established by the applicable law must be followed. Such incidents must be documented and measures shall be adopted to resolve and mitigate potential adverse effects for Data Subjects. In the cases provided for by law, DPO shall be designated in order to ensure that SAICA complies with the legal provisions on data protection.

6.7 Processing will be done in accordance to the Data Subject's rights

6.7.1 SAICA will respect a Data Subjects rights to:

6.7.1.1 access to a copy of the Personal Information held by SAICA;

6.7.1.2 object to Processing that could possibly cause or is causing damage or distress to the Data Subject;

6.7.1.3 prevent Processing of their data for direct marketing;

6.7.1.4 object to automated decision making;

6.7.1.5 have inaccurate Personal Information rectified, blocked, erased or destroyed;

6.7.1.6 claim compensation for damages caused by a breach of the Data Protection legislation;

6.7.1.7 have their Personal Information erased when it is no longer needed, if the data has been unlawfully processed or if the Data Subject withdraws their consent, unless there is an overriding legal or public interest in continuing to process the data;

6.7.1.8 restrict the Processing of their Personal Information until a dispute about the data's accuracy or use has been resolved, or when SAICA no longer needs to keep the Personal Information but the Data Subject needs the data for a legal claim;

6.7.1.9 data portability: where a Data Subject has provided Personal Information to SAICA by consent or contract for automated Processing and asks for a machine readable copy or have it sent to another Controller;

6.7.1.10 object to and prevent further Processing of their Personal Information for SAICA's legitimate interests or public interest unless SAICA can demonstrate compelling lawful grounds for continuing; and

6.7.1.11 stop SAICA from Processing the Personal Information obtained for online services such as social media, where consent for the Processing was previously given by or on behalf of a child, who withdraws their consent.

6.8 Personal Information will be kept secure by SAICA and any Processor

6.8.1 Appropriate technical and other measures will be taken by SAICA to prevent unauthorised or unlawful Processing or accidental loss or destruction of, or damage to, Personal Information.

6.8.2 In the event in which SAICA contracts with a Processor or third party, whose service or goods would include the Processing of the Personal Information collected and held by SAICA, it is mandatory that such a Processor or Third Party:

6.8.2.1 enter into a written agreement with SAICA, as well as in electronic form;

6.8.2.2 must undertake to only process Personal Information on instruction of SAICA and with its knowledge;

6.8.2.3 treat Personal Information as confidential and will not disclose such unless it is required by law or in the course of its duties of the agreement;

6.8.2.4 that it designs and organises data protection security consistent to the nature of the relevant Personal Information to be processed and the risks associated with a data breach in terms thereof, and assist SAICA in terms of its obligation to perform Data Protection Impact Assessments;

6.8.2.5 ensure that it has the necessary physical and technical security, which is backed up by a robust policies and procedures, and also that it has reliable and experienced staff;

6.8.2.6 assist SAICA through appropriate technical and organisational measures for the fulfilment of SAICA obligation to respond to request from Data Subjects in terms of their rights;

6.8.2.7 ensure that it is able to respond to any data breaches swiftly and effectively;

6.8.2.8 ensure that it deletes or returns all Personal Information to the Controller after the end of the services relating to the Processing, and deletes existing copies on request of SAICA, unless it is required by law to storage thereof;

6.8.2.9 provide SAICA with all information necessary to demonstrate compliance with the Data Protection Regulatory Framework and allow for and contribute to audits, including inspections, conducted by SAICA or another auditor mandated by SAICA;

6.8.2.10 designate a person who will be responsible for ensuring its Personal Information security, who has undertaken to commit him/herself to confidentiality;

6.8.2.11 shall without undue delay notify SAICA of a data breach; and

6.8.2.12 ensure that should SAICA transfer Personal Information to a Processor or third party across border that it is subject to law or a binding agreement that provides for adequate protection of upholding the principles of reasonable Processing and are substantially similar to the principles and conditions relating to the Data Protection Regulatory Framework.

6.9 No transfer of personal information shall be made cross-border

6.9.1 Personal Information of Data Subjects will not be transferred cross-border, unless:

6.9.1.1 such a country ensures an adequate level of protection of the rights and freedoms of Data Subjects in regard to the Processing of their Personal Information;

6.9.1.2 the Data Subject consents to the transfer;

6.9.1.3 the transfer is necessary for the performance of a contract between the Data Subject and SAICA or for the implementation of pre-contractual measures in response to a Data Subject's request;

6.9.1.4 the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject; or

6.9.1.5 it is not reasonably practicable to obtain the consent from the Data Subject, and if it was reasonably practicable to obtain such consent, the Data Subject would be likely to give same.

7 Retention of Personal Information

7.1 The main principle of the Retention of Personal Information, is that Personal Information should not be held for more than 5 (five) years after it ceases to be current, unless there is a specific reason for doing so for example legislative requirements would take precedence if the retention period is greater than 5 (five) years.

7.2 This applies to all data stored on SAICA owned, leased and otherwise provided systems and media, regardless of location.

7.3 SAICA shall attend to an examination and review of closed records to determine whether they should be destroyed, retained for a further period or transferred to an archive for permanent preservation.

7.4 SAICA's Information Communications Technology Draft Policy requires that all information on all business critical servers to be backed up on a daily basis, as per the backup schedule, and backup tapes must be kept off-site. It further requires that:

7.4.1 backup tapes shall be rotated weekly in a (four) week cycle for daily backups;

7.4.2 a weekly backup shall be rotated monthly;

7.4.3 a monthly backup shall be done at the end of every month and retained for a year; and

7.4.4 annual backups shall be kept for 5 (five) years, this applies to all business records (the December month backup becomes the annual backup and shall be kept for 5 (five) years.

7.5 SAICA has an approved **Record Retention Schedule**, attached hereto and marked as **Annexure "B".** This Schedule acts as the initial maintenance, retention and disposal schedule for physical record of SAICA and the retention and disposal schedule of electronic documents.

7.6 The Senior Executive: Legal & Governance (the "Administrator") is the officer in charge of the administration of this Policy and the implementation of processes and procedures to ensure that the Record Retention Schedule is followed. The Administrator is also authorised to: make modifications to the Record Retention Schedule from time to time to ensure that it is in compliance with the relevant laws and includes the appropriate document and record categories for the company; monitor relevant laws affecting record retention; annually review the record retention and disposal program; and monitor compliance with this policy.

7.7 In the event in which SAICA is served with any subpoena or request for documents or any employee becomes aware of a governmental investigation or audit concerning SAICA or the commencement of any litigation against or concerning SAICA, such employee shall inform the Administrator and any further disposal of documents shall be suspended until such time as the Administrator determines otherwise. The Administrator shall take such steps as are necessary to promptly inform all staff of any suspension in the further disposal of documents.

7.8 Records can be destroyed in the following ways:

7.8.1 non-sensitive information – can be placed in a normal rubbish bin;

7.8.2 confidential information – cross cut shredded and pulped or burnt;

7.8.3 electronic equipment containing information - destroyed using kill disc and for individual folders, they will be permanently deleted from the system.

7.9 Destruction of electronic records should render them non-recoverable even using forensic data recovery techniques.

8 Key Requirements and Controls

8.1 SAICA shall ensure that the appropriate actions are taken to ensure compliance with the Data Protection Regulatory Framework, more specifically the Principles and Conditions set out in this Policy, by the application of the necessary controls.

8.2 SAICA will:

8.2.1 identify and specify the purposes for which Personal Information is collected and processed, and ensure that such purposes are legitimate;

8.2.2 observe the conditions surrounding fair data collection and Processing;

8.2.3 collect and process appropriate information and only to the extent that is needed to fulfil any operational needs or to comply with any legal requirements;

8.2.4 ensure quality and accuracy of Personal Information collected and processed;

8.2.5 ensure rights of Data Subjects can be exercised in full, including but not limited to:

8.2.5.1 informed when Personal Information is collected and processed;

8.2.5.2 access to its Personal Information;

8.2.5.3 prevent Processing under certain circumstances; and

8.2.5.4 correct, rectify, block or erase information which is regards as incorrect or wrong information.

8.2.6 take appropriate technical and organisational security measures to safeguard Personal Information;

8.2.7 ensure that Personal Information is not transferred cross-border without suitable safeguards;

8.2.8 treat Data Subjects just and fair whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information; and

8.2.9 set in place clear processes and procedures to respond to Data Subject requests for information.

8.3 The relevant Policies and procedures relating to these controls have been set out under the scope and applicability of this Policy. The Board, CEO and employees are required to implement and comply with these policies and procedures to enable them to validate their fulfilment of the Principles and Conditions set out in this Policy.

8.4 It should be noted that should the Board, CEO and employees fail to adhered to this Policy, that such conduct may lead to disciplinary action being taken in accordance to SAICA's Disciplinary Procedures.

9 Key Roles and Responsibilities

9.1 All users of SAICA information are responsible for:

9.1.1 completing relevant training and awareness activities provided by the SAICA to support compliance with this Policy;

9.1.2 taking all necessary steps to ensure that no breaches of information security result from their actions;

9.1.3 reporting all suspected information security breaches or incidents promptly to GDPRcompliance@saica.co.za so that appropriate action can be taken to minimise harm;

9.1.4 informing SAICA of any changes to the information that they have provided to SAICA in connection with their employment, membership or other, for example changes to address or bank account details;

9.2 The CEO has ultimate accountability for SAICA's compliance with data protection law and is responsible for ensuring that centrally managed IT systems and services embed privacy by design and default and for promoting good practice in IT security among staff.

9.3 The ManCo is accountable for information governance and for ensuring that the DPO is given sufficient autonomy and resources to carry out his/her tasks effectively and efficiently.

9.4 The Senior Executive of Legal and Governance has senior management responsibility for information governance within SAICA.

9.5 The DPO is responsible for:

9.5.1.1 informing and advising ManCo and all members of the SAICA of their obligations under data protection law;

9.5.1.2 promoting a culture of data protection, e.g, through training and awareness activities;

9.5.1.3 reviewing and recommending policies, procedures, standards, and controls to maintain and demonstrate compliance with data protection law and embed privacy by design and default across the SAICA;

9.5.1.4 advising on data protection impact assessment and monitoring its performance;

9.5.1.5 monitoring and reporting on compliance to the Board, CEO, the Audit and Risk Committee and other relevant committees and boards;

9.5.1.6 maintaining Records of Processing Activities;

9.5.1.7 providing a point of contact for Data Subjects with regard to all issues related to their rights under data protection law;

9.5.1.8 investigating personal data breaches, recommending actions to reduce their impact and likelihood of recurrence; and

9.5.1.9 acting as the contact point for and co-operating with the Regulatory Authority on issues relating to Processing;

9.5.2 Senior Management is responsible for implementing the policy within their business areas, and for adherence thereto by their staff. This includes:

9.5.2.1 assigning generic and specific responsibilities for data protection management;

9.5.2.2 managing access rights for information assets and systems to ensure that staff, contractors and agents have access only to such Personal Information as is necessary for them to fulfil their duties;

9.5.2.3 ensuring that all staff in their areas of responsibility undertake relevant training provided by the SAICA and are aware of their responsibilities for data protection;

9.5.2.4 ensuring that staff responsible for managing IT put in place equivalent IT security controls; and

9.5.2.5 assisting the Data Protection Officer in maintaining accurate and up to date records of all data Processing activities.

9.6 The Senior Executive of Human Resources Development is responsible for maintaining relevant human resources policies and procedures, to support compliance with data protection law.

9.7 The Senior Executive of Membership and Global Alliances is responsible for maintaining relevant membership, administration policies and procedures and for oversight of the management of member records and associated Personal Information across the SAICA in compliance with data protection law.

9.8 The Senior Executive of Risk, Audit and Research is responsible for ensuring that data protection and wider Information Security controls are integrated within project management, risk, business continuity management and audit programmes.

9.9 The Head of Procurement Services is responsible for ensuring that supply chain due diligence and procurement processes embed information risk and data protection impact assessment and privacy by design.

9.10 The Facilities Division is responsible for ensuring that controls to manage the physical security of the SAICA take account of relevant data protection risks and are integrated into its systems.

9.11 The DTGC is responsible for reviewing the effectiveness of data protection policies and procedures as part of its wider oversight of information security management, as set out in the Information Security Policy Framework.

10 Appointment of Regulatory Authority

10.1 SAICA shall identify the authorities, regulators and/or supervisory authorities in relation to the regulation of the Data Protection Regulatory Framework and cooperate on request with the relevant authorities, regulators and/or supervisory authorities applicable.

11 Scope and Applicability of this Policy

11.1 This Policy applies to the Board, CEO, all employees, its Members and all other relevant stakeholders.

11.2 The principles, standards and conditions of Personal Data Protection are directly linked to the following SAICA Policies and Procedures:

11.2.1 SAICA Founding Documents;

11.2.2 SAICA Compliance Draft Policy;

11.2.3 SAICA Anonymisation and Pseudominisation Draft Policy;

11.2.4 SAICA Disciplinary Code and Procedure;

11.2.5 SAICA Information Communication Technology Draft Policy;

11.2.6 SAICA Data Impact Assessment Draft Procedure;

11.2.7 SAICA Data Security Incident Response Policy/ Incident Management Draft Policy;

11.2.8 SAICA Staff Training Draft Policy – Data Protection; and

11.2.9 SAICA Data Subject Rights Draft Policy.

12 Collection of Personal Information

12.1 SAICA will ensure that the Personal Information collected is within the boundaries of this Policy, in any location used by SAICA staff or contractors related to SAICA's operations, which includes Personal Information collected directly from the Data Subject, by completing a form or electronically.

12.2 SAICA will ensure, as far as reasonably possible, that a fair Processing notice is in place and that the Data Subject:

12.2.1 is informed as to why the collection of the Personal Information is required;

12.2.2 clearly understands what the legitimate purpose for the collection and Processing is, and should the legitimate purpose be based on a consent by the Data Subject only, what the consequences would be in the event in which the Data Subject refuse to give consent to Processing his/her Personal Information;

12.2.3 understand as to whom the Personal Information may be shared with and why;

12.2.4 is aware of the option to agree to the sharing of his/her Personal Information, and that he/she may grant explicit written or verbal consent to collect and share special Personal Information where necessary;

12.2.5 may give explicit consent to be contacted via email or telephone; and

12.2.6 is competent to give consent and has given such consent freely without any duress.

13 Storage of Personal Information

13.1 Personal Information and records relating to Data Subjects shall be stored securely and only authorised staff and where applicable authorised Processors and Third Parties will have access thereto.

13.2 SAICA will store such Personal Information for the period required or longer as required by the Regulatory Framework or legal obligation and in accordance to the SAICA Data Retention Policy, archiving, and destruction procedures.

13.3 SAICA is responsible to ensure that all Personal Information and company data is non-recoverable from any computer or similar devices previously used by SAICA which has been passed on or sold to a third party.

14 Access to and Accuracy of Personal Information

14.1 All Data Subjects have the right to access his/her Personal Information held by SAICA. SAICA shall ensure that the Personal Information is as far as reasonably possible accurate and up to date, by requesting Data Subjects to give notice to SAICA of any changes, alternatively will request the Data Subjects to update same on an annual basis via SAICA's website.

14.2 All SAICA employees are to ensure that Personal Information stored in terms of a Data Subject is factual and not subjective.

14.3 In addition to the above, SAICA will ensure that:

14.3.1 it clearly describes its processes and procedures on handling Personal Information;

14.3.2 it regularly review and audit the manner in which it collects, hold, manages and process Personal Information;

14.3.3 it regularly assess and evaluate its methods and performance in relation to handling Personal Information;

14.3.4 a DPO is appointed with the specific responsibility to ensure compliance with the Data Protection Framework;

14.3.5 the Board, CEO and all SAICA employees who processes Personal Information understand that they are contractually responsible for following good data protection practices;

14.3.6 all Board members and SAICA employees who process Personal Information are appropriately trained, supervised and will report any suspected or actual breaches of data (such breaches must be reported via the Data Protection Breach Reporting procedure);

14.3.7 the Data Protection Officer any other authorised employees who deals with enquiries from Data Subjects on access, rectifications, blocking or destruction of Personal Information are appropriately trained, experienced and handle such enquiries promptly and courteously;

14.3.8 the Board members and SAICA employees understand that a breach of the principles and conditions identified in this Policy may lead to disciplinary action being taken against them.

15 Record of Processing Activities

15.1 SAICA shall maintain written records of all Processing activities related to the Processing of Personal Information and shall include the necessary information.

15.2 SAICA will further ensure that the Processor mandated by it, shall provide a guarantee that it shall maintain a record of all categories of Processing activities carried out on behalf of SAICA and that all necessary information shall be included.

15.3 The abovementioned records shall be held in written and electronic form. Should the supervisory authority request such records, it shall be made available.

16 Data Breach Response

16.1 SAICA shall without undue delay, if feasible, within a period of 72 (seventy-two) hours after becoming aware of the breach, notify the breach to the relevant Regulatory Authority including the necessary information, unless the breach is unlikely to result in a risk to the rights and freedoms of the Data Subject.

16.2 Should the notification be delayed beyond the 72 (seventy-two) hours, such must be accompanied by reasons for the delay. Should it not be possible to provide all necessary information simultaneously, the information shall be provided in phases without undue delay.

16.3 SAICA shall keep record and document any personal data breaches, including the relevant facts, the effect thereof and the remedial action taken, and such record shall be in a form that will enable to the authorities, regulator and/or supervisory authority to verify compliance with the Data Protection Regulatory Framework.

16.4 In the event in which the data breach is likely to result in a high risk to the rights and freedoms of the Data Subject, SAICA shall communicate the breach to the Data Subject without undue delay, and shall include the nature of the breach, and all other necessary information.

17 Remedial Action and Lessons Learned

17.1 SAICA employees shall:

17.2 immediately report any material data protection compliance incidents the head of the Compliance Function, being the Senior Executive of Legal and Governance and the DPO, who shall:

17.2.1 initiate and support the appropriate remedial action to be taken by the responsible parties;

17.2.2 ensure, in case of suspected misconduct, that an investigation takes place, and, where and when appropriate recommended corrective or disciplinary action to Senior Executive: Human Resources, the relevant Senior Executive over the Division and ManCo;

17.2.3 develop a Lessons Learned Schedule to ensure that SAICA can learn from previous experiences and is able to properly implement the controls which are necessary to avoid a reoccurrence of such an incident;

17.2.4 initiate appropriate discussion of material compliance incidents in the AudCo;

17.2.5 encourage reporting of data protection compliance breaches or violations across SAICA; and

17.2.6 make use of existing incident reporting processes, as far as possibly, but remains fully responsible for quality of compliance incident reporting process.

17.3 Breaches of the applicable data protection compliance laws, rules and standards will be seen in a very serious light. Employees who do not comply with this policy or high level compliance standards may be subject to disciplinary action in terms of the applicable SAICA processes and procedures.

17.4 As set out in the SAICA Compliance Draft Policy, any person who fails to comply with its internal policies, procedures and any other requirements, or who fails to actively comply with the letter and spirit of the regulatory requirements will be subject to disciplinary procedures that could ultimately lead to their dismissal.

18 Implementation and Review of Policy

18.1 This Policy will be monitored by the Legal and Governance Division who is the owner of the Policy on an ongoing basis to ensure that all Business Units in SAICA are complying with and applying the Policy as well as the principles outlined in the policy.

18.2 Executive Directors are responsible for the implementation of this Policy into their Business Units / areas and every staff member is required to apply the policy in their normal day to day operations.

18.3 This Policy will be reviewed on an annual basis by the Policy Owner or earlier if required. The Policy Owner will communicate any changes to this Policy to SAICA so that they can respond to them.

19 Policy Communication

This Policy shall be communicated to all applicable users by means of awareness campaigns as well as the Intranet. All users (including contractors and third parties) are required to sign this Policy before gaining access to SAICA's network.

20 Effective Date

The policy shall come into effect on the date effectiveness of any legislation relevant to personal data protection and shall repeal any previous SAICA Policy/s which are related to Personal Data Protection.

Annexure "A"

DATA SUBJECT ACCESS REQUEST

GDPR DATA SUBJECT ACCESS REQUEST FORM

Should SAICA hold your Personal Information, you are currently entitled to request access to such information in accordance to the provisions of the Protection of Personal Information Act, 4 of 2013 (not effective as yet) and the General Data Protection Regulation (EU) 2016/679 ("GDPR") (which comes into effect on the 25th of May 2018) of the European Union ("EU"), where applicable.

Should you require access to your aforesaid information, you are required to complete this Form to enable us to provide you with the relevant information.

We will endeavour to respond to your request promptly, but in at least 30 (thirty) days, as follows:

- our confirmation of receipt of your request; or
- our receipt of any further information we may require from you to enable us to comply with your request.

Please note that, depending on the complexity and number of request we may extend the period by a further 2 (two) months, of which we will inform you of such extension within 1 (one) month of your request.

Note that the information you provide in this form will merely be used for the purpose of identifying you and the personal information you are requesting and enabling us to respond to your request. The completion of this form is not mandatory for you to make your request, such will however assist us in processing your request efficiently.

Section A: Details of Person Requesting Information

Full Name and Surname:	
Identity Number:	
Contact Telephone Number:	
Email Address:	
Physical Address:	

Member Number (if applicable):	

Section B: Are you the Data Subject:

Please tick the appropriate box and peruse the instructions.

☐ **Yes, I am the Data Subject.** I enclose herewith proof of my identity and physical address, please tick the boxes in terms of the proof:

Identification document ☐

Passport ☐

Driver's License ☐

Birth Certificate ☐

Utility Bill or Bank Statement, not older than 3 (three) months ☐

TV License or Local Authority Tax Bill reflecting my physical address, not older than 1 (one) year ☐

☐ **No, I am not the Data Subject.** I am acting on behalf of the Data Subject and enclose hereto proof of my identity, as well as the Data Subject, and a copy of the Data Subject's written authority. (Please complete **Section C** hereof)

My Documentation:

Identification document ☐

Passport

Driver's License ☐

Birth Certificate ☐

Utility Bill or Bank Statement, not older than 3 (three) months ☐

TV License or Local Authority Tax Bill reflecting my physical address, not older than 1 (one) year ☐

Written Mandate Signed by Data Subject ☐

Data Subject's Documentation:

Identification document

Passport ☐

☐

Driver's License

Birth Certificate ☐

Utility Bill or Bank Statement, not older than 3 (three) months ☐

TV License or Local Authority Tax Bill reflecting my physical address, not older than 1 (one) year ☐

We need to ensure that we are releasing the information to the correct person and thus we require proof of your identity and your physical address. Please provide us with a certified photocopy of scanned image of one of both of the following:

- **Proof of Identity**
  Identity Document, Passport, Driving License or Birth Certificate.
- **Proof of Physical Address**
  Utility Bill or Bank Statement, not older than 3 (three) months; TV Licence or Local Authority Tax Bill reflecting your physical address, not older than 1 (one) year.

In the event in which we are not satisfied that you have proven your identity, we reserve the right to refuse to grant your request.

Section C: Details of Data Subject (if different from Section A)

Full Name and Surname:	
Identity Number:	
Contact Telephone Number:	
Email Address:	
Physical Address:	
Member Number (if applicable):	

Section D: Describe what Information you require

Please provide any relevant details you are of opinion would assist us in identifying the information you require.

It is important to note, that should the information provided above reveal information directly or indirectly related to another person we will require such person's consent prior to us providing you with the information. In certain circumstances, where the information requested would adversely affect the rights and freedoms of others, we may not be able to disclose the information to you, in which case you will be informed promptly and provided with reasons for our decision.

While in most cases we will be happy to provide you with the information you request, we nevertheless reserve the following rights, in accordance to:

- Article 12 (5) to charge a reasonable fee or refuse your request if is considered as being manifestly unfounded, excessive or repetitive;
- Article 14 (5) of the GDPR to refuse your request due to the fact that you already have such information or providing such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in

the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguard referred to in article 89 (1) of the GDPR; or

- In terms of Article 14 (1) it is likely to render impossible or it would seriously impair the achievement of the objectives of that processing.

We will however make every effort possible to provide you with a satisfactory form of access or summary of the information, if suitable.

Section E: Information about the Collection and Processing of Personal Information

Should you require information about any of the following, please tick the relevant boxes:

- Why SAICA is processing your Personal Information ☐
- To whom your Personal Information are disclosed ☐
- The Source of your Personal Information ☐

Section F: Disclosure of CCTV images

Should the information you require be in the form of video images captured by our CCTV Security Cameras, would you be satisfied with viewing these images?

Yes ☐ No ☐

Section G: Declaration

Please note: any attempt to mislead SAICA may result in prosecution.

I, undersigned

_____

(Name and Surname)

do hereby,

1. confirm that I have read and understood the terms of this Data Subject Access Request Form;

2. consent to the processing of the personal information that I am submitting in this form and any personal information I may submit in further correspondence for purposes of processing this request, and where necessary my details may be shared with the supervisory authority;

3. certify that the information provided in this application is true, correct and within my personal knowledge, and that I'm authorised to submit this request;

4. understand that it is necessary to confirm my identify, and where applicable also the Data Subject's Identity on whose behalf I am acting; and

5. it might be necessary to obtain more detailed information in order to locate the correct personal information;

6. confirm that I understand that SAICA will not be able to process my request if this Form is not properly completed or incomplete.

_____ _____

Signature Date:

Supplementary Documentation Mandatory to this Data Subject Access Request Form:

- **Proof of your Identity (refer to Section B hereof);**
- **Proof of the Data Subject's Identity (if different to the above);**
- **If applicable, authority from the Data Subject wherein you are mandated to act on his/her behalf.**

Please address and return your completed form, together with the mandatory documentation to:

The SAICA Data Protection Officer

Physical Address:

The South African Institute of Chartered Accountants

17 Fricker Road

Illovo

Sandton

Johannesburg

2196

Email: GDPRcompliance@saica.co.za

Telephone Number: +2711 621 6710 / 6979

Important:

Should you on receipt of the Information requested believe that:

- the information is inaccurate or out of date;
- we should no longer be holding your information;
- we are using your information for a purpose of which you are unaware;
- we may have passed inaccurate information about you to someone else;

then you could notify the SAICA's Data Protection Officer immediately

Annexure "B"

RECORD RETENTION SCHEDULE

1 Protection of Personal Information Act, 4 of 2013

The Protection of Personal Information Act, No 4 of 2013, aims to give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations.

Section 14 of the Protection of Personal Information Act states that personal information must not be retained for any longer than is necessary to achieve the purpose for its collection. If there is no legal requirement to keep the information, it should be deleted. The Act therefore places an obligation on the person collecting the data to delete or remove it at a certain time.

Records of personal information must 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.

Number	Document details	Retention period	Action post retention	Compliance with Legislation	Compliance with Internal Policy	Responsible party
2 Companies Act, No 71 of 2008 The **Companies Act, No 71 of 2008,** consolidates and amends the law that relates to companies. This Act became effective on 1 May 2011 and should be read with the Companies Amendment Act, No 3 of 2011, and the Companies Regulations, 2011. The Act expressly provides that records must be kept "in written form, or other form or manner that allows that information to be converted into written form within a reasonable time						
2.1	General rule for company records: Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act and other public regulation	7 years or longer (as specified in other public regulation)	Destroy	**Reference: Section 24**		
2.2	Notice of Incorporation (Registration certificate)	Indefinite				
2.3	Memorandum of Incorporation and alterations or amendments	Indefinite				
2.4	Rules/By-laws	Indefinite Current and previous versions				
2.5	Register of company secretary and auditors	Indefinite				
2.6	Regulated companies (companies to which chapter 5, part B, C and Takeover Regulations apply) - Register of disclosures of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued	Indefinite				
2.7	Notice and minutes of all shareholders meeting including: - Resolutions adopted - Document made available to holders of securities	Permanent				
2.8	Copies of reports presented at the annual general meeting of the company	7 years	Destroy			
2.9	Copies of annual financial statements required by the Act	7 years	Destroy			
2.10	Copies of accounting records as required by the Act	7 years	Destroy			
2.11	Record of directors and past directors, after the director has retired from the company	7 years	Destroy			

2.12	Written communication to holders of securities	7 years	Destroy			
2.13	Minutes and resolutions of directors' meetings, audit committee and directors' committees	Permanent				
2.14	Securities register and uncertificated securities register	Indefinite		**Reference: Section 50**		
3 **Electronic Communication and Transaction Act, No 25 of 2002** The **Electronic Communication and Transaction Act, No 25 of 2002,** regulates electronic communication and prohibits the abuse of information. Certain principles are stated for the electronic collection of personal information and also the timeframe in which this information must be kept.						
3.1	Personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information	As long as information is used, and at least 1 year thereafter.	Destroy	**Reference: Section 51(5), (7) and (8)**	**IT Policies**	
3.2	A record of any third party to whom the information was disclosed must be kept for as long as the information is used	As long as information is used and at least 1 year thereafter.	Destroy		**IT Policies**	
3.3	All personal data which has become obsolete		Destroy			
4 **Consumer Protection Act, No 68 of 2008** The **Consumer Protection Act, No 68 of 2008,** seeks to promote a fair, accessible and sustainable marketplace, to provide for improved standards of consumer information and to prohibit certain unfair marketing and business practices. The Act became effective on 31 March 2011 and should be read with the Consumer Protection Act Regulations. There are specific requirements for information to be kept by intermediaries, for auctions and promotional competitions						
4.1	Information provided to a consumer by an intermediary - - Full names, physical address, postal address and contact details; - Id number and registration number; - Contact details of public officer in case of a juristic person; - Service rendered; - Intermediary fee;	3 years	Destroy	**Reference: Section 27(3)(b) and Regulation 10 Disclosure by intermediary**		

	- Cost to be recovered from the consumer; - Frequency of accounting to the consumer; - Amounts, sums, values, charges, fees or remuneration specified in monetary terms					
4.2	Disclosure in writing of a conflict of interest by the intermediary in relevance to goods or service to be provided	3 years	Destroy			
4.3	Record of advice furnished to the consumer reflecting the basis on which the advice was given	3 years	Destroy			
4.4	Written instruction sent by intermediary to the consumer	3 years	Destroy			
4.5	A person who conducts a promotional competition must retain: - full details, including identity or registration numbers, addresses and contact numbers of the promoter; - rules of promotional competition; - copy of offer to participate in promotional competition; - names and identity numbers of persons responsible for conducting the promotional competition; - full list of prizes offered in promotional competition; - a representative selection of materials marketing the promotional competition; - list of all instances when the promotional competition was marketed, including dates, medium used and places where marketing took place; - names and identity numbers of persons responsible for conducting the selection of prize winners in the promotional competition; - acknowledgement of receipt, identity number and the date of receipt of the prize by the prize winner; - declarations or affirmation that prize winners are not employees, directors, agents, or consultants who directly or indirectly controls or is controlled by the promoter or marketing service provider in respect of	3 years	Destroy	**Reference: Section 36(11)(b) and Regulation 11(6)** **Promotional competitions**		

	the promotional competition, or the spouses, life partners, business partners or immediate family members; - basis of determining the prize winners; - summary describing the proceedings to determine the winners; - whether an independent person oversaw the determination of the prize winners; - the means by which the prize winners were announced and frequency; - list of names and identity numbers of prize winners; - list of dates when prizes were handed over to the prize winners; - steps taken by the promoter to contact the winner; - reasons for prize winner not receiving or accepting the prize and steps taken by promoter to hand over the prize					
4.6	Written agreement that contains the terms and conditions upon which the auctioneer accepts the goods for sale.	3 years	Destroy	**Document Section 45 and Regulation 31 Auctions**		
5 **National Credit Act, No 34 of 2005** The public is protected by the National Credit Act, No 34 of 2005 ("NCA"), which aims to promote and advance the social and economic welfare of consumers by promoting a fair and transparent credit industry and assisting consumers to make more informed decisions before buying goods and services on credit. To ensure that this process occurs, certain documents must be retained.						
5.1	Records of registered activities to be retained by Credit Providers, in respect of each consumer: - application for credit; - application for credit declined; - reasons for decline of application for credit; - pre-agreement statement and quote; - documentation in support of steps taken in terms of section 81(2) of the Act; - record of payments made; and	3 years from the earliest of the dates on which the registrant created, signed or received the document	Destroy	**Reference: National Credit Regulations, Regulation 55(1)(b)**		

	- documentation in support of any steps taken after default by consumer.					
5.2	Records of registered activities to be retained by Credit Providers, in respect of operations: - record of income, expenses and cash flow; - credit transaction flows; and - management accounts and financial statements.	3 years from the earliest of the dates on which the registrant created, signed or received the document	Destroy	**Reference: National Credit Regulations, Regulation 55(1)(c)**		
5.3	Details and results of disputes lodged by the consumers	6 months	Destroy	**Reference: National Credit Regulations, Regulation 17(1) Retention period applicable to credit bureau information**		
5.4	Enquiries	1 year	Destroy			
5.5	Payment Profile	5 years	Destroy			
5.6	Adverse classification of enforcement action	1 year	Destroy			
5.7	Adverse classification of consumer behavior	1 year	Destroy			
5.8	Debt restructuring	Until a clearance certificate is issued	Destroy			
5.9	Civil court judgments	The earlier of 5 years or until the judgment is rescinded by a court or abandoned by the credit provider in terms of section 86 of the Magistrate's Court Act, 32 of 1944	Destroy			
5.10	Maintenance judgments	Until the judgment is rescinded by a court	Destroy			
5.11	Administration orders	5 years or until order is rescinded by court	Destroy			

5.12	Sequestration order	5 years or until rehabilitation order is granted	Destroy			
5.13	Rehabilitation orders	5 years	Destroy			
5.14	Records of registered activities to be retained by Credit Bureaux, 1. All documents relating to disputes, inclusive of but not limited to: - documents from the consumer; - documents from the entity responsible for disputed information; - documents pertaining to the investigation of the dispute; 2. Correspondence addressed to and received from sources of information as set out in section 70(2) of the Act and Regulation 18(7) pertaining to issues of disputed information.	3 years from the earliest of the dates on which the registrant created, signed or received the document	Destroy	**Reference: National Credit Regulations, Regulation 55(1)(d)**		
5.15	Records of registered activities to be retained by Debt Counsellors, in respect of each consumer - application for debt review; - copy of all documents submitted by the consumer; - copy of rejection letter (if applicable); - debt restructuring proposal; - copy of any order made by the tribunal and/or the court; and - copy of clearance certificate.	3 years from the earliest of the dates on which the registrant created, signed or received the document	Destroy	**Reference: National Credit Regulations, Regulation 55(1)(a)**		

5.16	Records to be kept in terms of section 170 of the Act in respect of each consumer: - records of all applications for credit, credit agreements and credit accounts	3 years from the date of termination of the credit agreement; or, in the case of an application for credit that is refused or not granted for any reason, from the date of receipt of the application	Destroy	**Reference: National Credit Regulations, Regulation 56**		
6 **Compensation for Occupational Injuries and Diseases Act, No 130 of 1993** The **Compensation for Occupational Injuries and Diseases Act, No 130 of 1993,** provides for compensation for disablement caused by occupational injuries or diseases sustained or contracted by employees in the course of their employment or for death by these injuries at their place of work. The Act states that certain records that relate to the earnings should be retained.						
6.1	A register or other record of the earnings and other prescribed particulars of all the employees	4 years after the date of the last entry in that register or record	Destroy	**Reference: Section 81(1) and (2)**		
7 **Occupational Health and Safety Act, No 85 of 1993** The **Occupational Health and Safety Act, No 85 of 1993,** was enacted to provide for the health and safety of employees at work and for people using plant and machinery and working in other hazardous employment conditions. Certain documents have to be kept based on the Administrative Regulations.						
7.1	An employer or user shall keep at a workplace or section of a workplace, as the case may be, a record in the form of Annexure 1 for a period of at least three years, which record shall be open for inspection by an inspector, of all incidents which he or she is required to report in terms of section 24 of the Act and also of any other incident which resulted in the person concerned having had to receive medical treatment other than first aid.	3 years	Destroy	**Reference: General Administration Regulations 2003, 9(1) and 5(1)**		

7.2	A health and safety committee shall keep record of each recommendation made to an employer in terms of issues affecting the health of employees and of any report made to an inspector as contemplated in section 20(2) of the Act	3 years	Destroy			
7.3	**Reference: Asbestos Regulations, 2001, Regulation 16(e) and (f)**		Destroy			
7.4	Records of assessments and air monitoring, and the asbestos inventory	Min of 40 years	Destroy			
7.5	Medical surveillance records	Min of 40 years	Destroy			
7.6	**Reference: Hazardous Biological Agents Regulations, 2001, Regulation 9(1) and (2)**		Destroy			
7.7	Records of risk assessments and air monitoring results	40 years	Destroy			
7.8	Medical surveillance records	40 years	Destroy			
7.9	**Reference: Hazardous Chemical Substance Regulations, 1995, Regulation 9**		Destroy			
7.10	Records of assessments and air monitoring	30 years	Destroy			
7.11	Medical surveillance records	30 years	Destroy			
7.12	**Reference: Lead regulations, 2001, Regulation 10**		Destroy			
7.13	Records of assessments and air monitoring	40 years	Destroy			
7.14	Medical surveillance records	40 years	Destroy			
7.15	All records of assessments and noise monitoring	40 years	Destroy	**Reference: Noise Regulations (MOSA) Regulation 11**		
7.16	All medical surveillance records, including the baseline audiogram of every employee	40 years	Destroy			
8 **Basic Conditions of Employment Act, No 75 of 1997**						

The **Basic Conditions of Employment Act, No 75 of 1997,** states that various documents relating to employees should be kept for future reference. (Note: A reference exists that an employer who keeps records in terms of this section is not required to keep any other record of time worked and remuneration paid as required by any other employment law.)						
8.1	Written particulars of employee must be kept after termination of employment	3 years after the termination of employment.	Destroy	Basic Conditions of Employment Act, No 75 of 1997 Reference: Section 29(4)		
8.2	Employee's name and occupation	3 years from the date of the last entry in the record.	Destroy	**Reference: Section 31**		
8.3	Time worked by each employee					
8.4	Remuneration paid to each employee					
8.5	Date of birth of any employee under 18 years of age					
8.6	Any other prescribed information					
8.7	An employer must establish and maintain records in respect of its workforce, its employment equity plan and other records relevant to its compliance with this Act.	5 years after expiry of the plan	Destroy	**Reference: Section 26**		
8.8	A designated employer must retain their Employment Equity Plan	5 years after expiry of the plan	Destroy	**Reference: Regulation 9(3)**A		
8.9	A designated employer must submit a report to the Director General once every year. This report should be retained after submission to the Director General	5 years after it has been submitted to the Director-General.	Destroy	**Reference: Regulation 10(9**		
8.10	Employers must maintain personal records of each of their current employees in terms of - names; - identification numbers; - monthly remuneration; and - address where the employee is employed	In addition to the 5-year rule, records must therefore be retained until the base cost calculation must be proved to SARS in the event of a	Destroy			

		capital gain or capital loss				
9 Labour Relations Act, No 66 of 1995 The **Labour Relations Act, No 66 of 1995,** applies to employees, employers, trade unions and employers' organisations and provides a framework where the parties can collectively bargain regarding remuneration, basic conditions of service and other matters of importance. Various records relating to the structures created in this Act have to be kept for future reference						
9.1	Every Council must preserve the following documents in original or reproduced form: - books of account - supporting vouchers - income and expenditure statements - balance sheets - auditor's reports minutes of its meetings (Reference: Section 54)	3 years from the end of the financial year to which they relate	Destroy	**Reference: Section 53(4)**		
9.2	Registered trade unions and registered employers' organisation must preserve the following documents in original or reproduced form: - books of account - supporting vouchers - records of subscriptions or levies paid by its members - income and expenditure statements - balance sheets auditor's reports	3 years from the end of the financial year to which they relate.	Destroy	**Reference: Section 98(4)**		
9.3	Registered trade unions and registered employers' organisation must keep a list of its members	Indefinite		**Reference: Section 99**		
9.4	Minutes of its meetings, in an original or reproduced form from the end of the financial year to which they relate	3 Years	Destroy			
9.5	Registered trade unions and registered employers' organisation must keep the ballot papers for a period of three years from the date of every ballot	3 Years	Destroy			
9.6	Every employer must keep the records in their original form or a reproduced form that an employer is required to keep in compliance with any applicable:	3 years from the date of the event or end of the	Destroy	**Reference: Section 205(1) and (2)**		

	- collective agreement; - arbitration award; - determination made in terms of the Wage Act	period to which they relate				
9.7	Employer must keep prescribed details of any strike, lock-out or protest action involving its employees	Indefinite	Destroy	**Reference: Section 205(3)**		
9.8	Employers should keep records for each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions	Indefinite	Destroy	**Schedule 8, Section 5**		
9.9	The Commission must keep the following records: Books of accounts Records of income, expenditure, assets and liabilities	Indefinite	Destroy	**Schedule 3, Section 8(a)**		

10 Unemployment Insurance Act, No 63 of 2002

The **Unemployment Insurance Act, No 63 of 2002,** applies to all employers and workers, but not to –

- Workers working less than 24 hours a month for an employer;
- Learners;
- Public servants;
- Foreigners working on contract;
- Workers who get a monthly State (old age) pension; or
- Workers who only earn commission.

Domestic employers and their workers have also been included under the scope of the Act since 1 April 2003.

10.1	Employers must maintain personal records of each of their current employees in terms of - names; - identification numbers; - monthly remuneration; and - address where the employee is employed	Refer to 13.6 under Income Tax Act	Destroy	Unemployment Insurance Act, No 63 of 2002 **Reference: Section 56(2)(c)**		
TAX	The **Income Tax Act, No 58 of 1962,** is the Act that governs all the laws relating to income taxes and donations and the **Value Added Tax Act, No 89 of 1991,** provides for the taxation of the supply of goods and services as well as the importation of goods. The **Tax Administration Act, No 28 of 2011**, has been effective from 1 October 2012. This Act has not removed the retention of documentation requirements from the Income Tax Act and the Value Added Tax Act and has included the requirements for document keeping in the Act.					

11 Income Tax Act, No 58 of 1962						
11.1	In addition to the records required in section 29 TAA, in respect of each employee the employer shall keep a record showing (para 14(1)(a)(-(d)): 12. amount of remuneration paid or due by him to the employee; 13. the amount of employees' tax deducted or withheld from the remuneration paid or due; 14. the income tax reference number of that employee; 15. any further prescribed information	5 years from the date of submission of the return evidencing payment (i.e. EMP201)	Destroy	**Reference: 4th Schedule, para 14(1)**		
11.2	In addition to the records required in section 29 Tax Administration Act, in respect of each employee the employer shall keep a record showing (para 14(1)(a)(-(d)): 16. amount of remuneration paid or due by him to the employee; 17. the amount of employees' tax deducted or withheld from the remuneration paid or due; 18. the income tax reference number of that employee; 19. any further prescribed information;	5 years from the date of submission of the return required by gazette (i.e. EMP501)	Destroy	**Reference: 4th Schedule, para 14(3**		
12 Value Added Tax Act, No 89 of 1991 In addition to the records required in Chapter 4, part A of the Tax Administration Act, every vendor must keep the records as indicated below.						
12.1	Where the zero rate is applied by any vendor documentary proof must be obtained and retained to substantiate the entitlement to the zero rate	5 years from the date of submission of the return	Destroy	Value Added Tax Act, No 89 of 1991 **Reference: Section 11(3)**		
12.2	Where a vendor's basis of accounting is changed, the vendor shall prepare lists of debtors and creditors showing the amounts owing by the debtors and owing to the creditors at the end of the tax period immediately preceding the changeover period.	5 years from date of submission of the return	Destroy	Value Added Tax Act, No 89 of 1991 **Reference: Section 15(9)**		
12.3	Records of importation of goods and documents - bill of entry, or - other documents prescribed by the Custom and Excise Act;	5 years from date of submission of the return	Destroy	Value Added Tax Act, No 89 of 1991 **Reference: Section 16(2)**		

	- proof, by virtue of retention of the receipt of payment, that the VAT charge has been paid to SARS - Records must be maintained as referred to in section 20(8) where the supply is a supply of second hand goods or a supply contemplated in section 8(10) - statements as contemplated in section 54 (2A and 54(3)(a) of the Customs & Excise Act must be retained A ruling (requested no later than two months before expiry of the five year period and such documents to which the ruling relates Section 16 refers to Section 55 of the VAT Act and Part A of Chapter 4 of the TAA insofar that even if provided to SARS, the Commissioner may disallow a deduction for input tax unless the bill of entry or document concerned is retained by the taxpayer in accordance with these provisions.					
12.4	Vendors are obliged to keep the following records in addition to those required under Part A of Chapter 4 of the TAA: - record of all goods and services supplied by and to the vendor showing the goods and services, the rate of tax applicable to the supply and the suppliers or their agents, in sufficient detail to enable the goods and services, the rate of tax, the suppliers or the agents to be readily identified by the Commissioner and all invoices, tax invoices, credit notes, debit notes, bank statements, deposit slips, stock lists and paid cheques - a record of all importation of goods required to be obtained relating thereto in terms of section 16(2)(d) - documentary proof required to be obtained and retained in terms of section 16(2)(f) and (g) - the charts and codes of account, the accounting instruction manuals and the system and programme documentation which describes the accounting	5 years from date of submission of the return	Destroy	Value Added Tax Act, No 89 of 1991 **Reference: Section 55(1)(a)**		

	system used for each tax period in the supply of goods and services; - any list required to be prepared in accordance with section 15(9) - any documentary proof required to be obtained and retained in accordance with section 11(3)					
12.5	Documentary proof substantiating the zero rating of supplies	5 years from date of submission of the return	Destroy	Value Added Tax Act, No 89 of 1991 **Reference: Interpretation Note 31 – 30 March 2013**		
12.6	Where a tax invoice or credit or debit note has been issued in relation to a supply by an agent or to an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.	5 years from date of submission of the return	Destroy	Value Added Tax Act, No 89 of 1991 **Reference: Interpretation Note 31 – 30 March 2013**		
13 Securities Transfer Tax Administration Act, No. 26 of 2007 In addition to the records required to be kept under section 29 of the Tax Administration Act, the below-mentioned persons must retain sufficient record of a security transfer in order to enable that person to observe the requirements of this Act and satisfy the Commissioner that the requirements of this Act have been met.						
13.1	Any member, participant or person to whom a listed security is transferred must keep, for a period of five years, such record of every transfer which has been effected by the member, participant or person to whom the security has been transferred as may be required to enable the member, participant or person to whom the security has been transferred, as the case may be, to observe the requirements of this Act and to enable the Commissioner to be satisfied that those requirements have been observed	5 years from date of transfer of the security	Destroy	**Reference: Section 13(1)**		
13.2	A company or close corporation that issued an unlisted security must keep records of every transfer of an unlisted security issued by itas may be required to enable the company to observe the requirements of this Act and to	5 years from date of transfer of the security	Destroy	**Reference: Section 13(2)**		

	enable the Commissioner to be satisfied that those requirements have been observed. These records must be obtained from a person to whom an unlisted security is transferred, who is required to inform the aforementioned company of the transfer.					
Document Retention not governed by specific legislation						
14 **PROFESSIONAL DEVELOPMENT**						
14.1	Training related documentation	Indefinite				**Prof Dev**
15 **PROPERTY RECORDS**						
15.1	Correspondence, Property Deeds, Assessments, Licenses, Rights of Way	Permanent				
15.2	Original Purchase/Sale/Lease Agreement					
15.3	Property Insurance Policies					
15.4	Resource Management	Current Financial Year + 2	Destroy			
15.5	Legal Documentation	Permanent	Archive			
15.6	Business Continuity Plan	Active	Archive			
15.7	Security Information	Current Academic Year + 5	Destroy			
15.8	Leased Property Files	End of lease + 5	Destroy			
15.9	Property Files	Current Financial Year + 5	Destroy			
15.10	Leases	End of lease + 5	Destroy			

15.11	CCTV recordings	28 days	Destroy unless legally required			
16 **Miscellaneous**						
16.1	Consultant's Reports	2 years				
16.2	Material of Historical Value (including pictures, publications)	Permanent				
16.3	Policy and Procedures Manuals – Original	Current version with revision history				
16.4	Policy and Procedures Manuals - Copies	Retain current version only				
16.5	Terms of Reference	Current version with revision history				
16.6	Annual Integrated Reports	Permanent				
16.7	Licences and Permits	Permanent				
16.8	Web Page Files: Internet Cookies	All workstations: Internet Explorer should be scheduled to delete Internet cookies once per month.				
16.9	Correspondence or memoranda that do not pertain to documents having a prescribed retention period should generally be discarded sooner.	discarded *within two years.*				

	Those pertaining to routine matters and having no significant, lasting consequences should be Some examples include: • Routine letters and notes that require no acknowledgment or follow-up, such as notes of appreciation, congratulations, letters of transmittal, and plans for meetings. • Form letters that require no follow-up. • Letters of general inquiry and replies that complete a cycle of correspondence. • Letters or complaints requesting specific action that have no further value after changes are made or action taken (such as name or address change). • Other letters of inconsequential subject matter or that definitely close correspondence to which no further reference will be necessary. • Chronological correspondence files. Please note that copies of interoffice correspondence and documents where a copy will be in the originating department file should be read and destroyed, unless that information provides reference to or direction to other documents and must be kept for project traceability.					

16.10	Correspondence pertaining to non-routine matters or having significant lasting consequences.	permanently				
17 **LEGAL FILES AND PAPERS**						
17.1	Legal Memoranda and Opinions (including all subject matter files)	10 years after close of matter				
17.2	Litigation Files	10 year after expiration of appeals or time for filing appeals				
17.3	Disciplinary matters	10 years after close of matter				
17.4	Court Orders	Permanent				
17.5	Requests for Departure from Records Retention Plan	10 years				
17.6	CCMA documentation	10 year after expiration of appeals or time for filing appeals				
17.7	Workmen's compensation claims	10 years after the matter is closed.				
18 **COMPANY / ORGANISATION**						
18.1	Company Records/ Governance (minute books, signed minutes of the Board and all committees, corporate seals, articles of incorporation,	Permanent				

	bylaws, regulations, code of professional conduct, annual corporate reports; trademarks; MOI; Articles of Association; declarations of interest)					
18.2	Accreditation documentation	Permanent				
18.3	Licenses and Permits	Permanent				
19 **CONTRACTS**						
19.1	Contracts and Related Correspondence (including any proposal that resulted in the contract and all other supportive documentation)	7 years after expiration or termination				
20 **ACCOUNTS AND FINANCE**						
20.1	Accounts Payable ledgers and schedules	7 years	Destroy			
20.2	Accounts Receivable ledgers and schedules	7 years	Destroy			
20.3	Annual Audit Reports and Financial Statements	Permanent	Archive			
20.4	Annual Audit Records, including work papers and other documents that relate to the audit	7 years after completion of audit	Destroy			
20.5	Annual Plans and Budgets	2 years	Destroy			
20.6	Bank Statements and Cancelled Checks	7 years	Destroy			
20.7	Cheque reconciliations	6 years post audit	Destroy			
20.8	Employee Expense Reports	7 years	Destroy			
20.9	General Ledgers	Permanent	Archive			

20.10	Interim Financial Statements	7 years	Destroy			
20.11	Notes Receivable ledgers and schedules	7 years	Destroy			
20.12	Investment Records	7 years after sale of investment	Destroy			
20.13	Internal Audit work papers and findings	7 years after completion	Destroy			
20.14	Annual Financial Statements/ Integrated Report	Permanent	Archive			
20.15	Student related costs	Current tax Year + 5	Destroy			
20.16	Legal Costs	Current Tax Year + 5	Destroy			
20.17	Invoices	Current Tax Year + 5	Destroy			
20.18	Orders	Current Tax Year + 5	Destroy			
20.19	Purchase Records	Current Tax Year + 5	Destroy			
21 **SEMINARS AND EVENTS**						
21.1	All seminar and event related documents (members)	Permanent				
21.2	All seminar and event related documents (non-members)	Current year + 5 (depending on consent)	Destroy			
22 **ASA**						
22.1	Database of subscribers (members)	Permanent				
22.2	Database of subscribers (non-members)	7 years post cancellation of subscription subject to consent	Delete			

22.3	Articles rejected for publication	2 years post final communication with author.	Destroy			
23 **MEMBERSHIP**						
23.1	Membership records (including applications and supporting documents, disciplinary findings, terminations etc.)	Permanent				