SC WorkWealth Management Limited

RECORD KEEPING POLICY

Contents

1 Introduction

SC WorkWealth Management Limited ("the Company") is a company incorporated in Cyprus with incorporation number HE431951, a Cyprus Investment Firm licensed and regulated by the Cyprus Securities and Exchange Commission ("CySEC").

Pursuant to the Markets in Financial Instruments Directive (Directive 2014/65/EU) ("MiFID II") and Regulation 2014/600/EU ("MiFIR"), the Company is required to establish, implement and maintain effective and transparent policies and procedures for the prompt handling of clients / Company documents and records.

In this respect, the Company established, implemented and maintained an effective and transparent Record Keeping Policy ("the Policy"), which provides the required guidance regarding the documents (both in paper and electronic format) retention period, received or created during the provision of Investment Services and / or Ancillary Services to clients.

The Board of Directors ("BoD") has the responsibility of establishing this Policy, approving any subsequent amendments / revisions and ensuring that disciplinary measures are taken when the rules of this Policy are violated.

In cases where there are references in any of the internal policies and procedures of the Company in relation to issues covered by this Policy, which were approved prior to the approval of this Policy, the provisions of this Policy will prevail.

2 Purpose of this Policy

This Policy aims to establish a framework in order for the employees of the Company to clearly understand their responsibilities in relation to the requirements imposed by MiFID II with regards to the documentation, storage and retention period of certain Records. This Policy also provides guidelines on how long certain documents should be retained.

The provisions of this Policy apply at all times, unless:

- the Records under question are or could be subject to the future litigation;
- there is a dispute that could lead to litigation; or
- the Company is a party to a lawsuit; or
- an investigation is conducted by CySEC or any other competent judicial, governmental, supervisory or regulatory body,
- where, such Records must be preserved until the Head of Compliance/MLRO determines that are no longer needed.

3 Policy application

Applicability

The Policy applies to:

- All Records (both original documents and reproductions) created, received, provided or maintained by the Company's relevant employees;
- All the Company's departments involved in the provision of Investment and / or ancillary services; and
- All types of clients and / or counterparties to which the Company provides Investment and / or ancillary services.

All concerned staff members of the Company should be aware of the provisions of this Policy and understand the role and importance for the retention of Records pertaining to the offering of investment and / or ancillary services.

The Policy and any subsequent amendments are distributed to and are binding to all employees.

It is the Company's policy to maintain complete, accurate and high-quality records. Records are to be retained for the period set forth in "Record Retention Schedule" section of this document, unless longer retention is required for historical reference, contractual, legal or regulatory requirements or for any other purpose.

No employee or director of the Company shall knowingly destroy information or a document with the intention to obstruct or influence the investigation or proper administration of any matter within the Company's departments.

It is noted that records is defined as the following information / documentation, but not limited to: legal documentation, client data / statements, electronic mails, telephone conversations and electronic communications (e.g. instant messages (e.g. Bloomberg / Reuters), minutes of face-to-face meetings, telephone recordings), electronic documents (e.g. Microsoft Office Suite and PDF files) or other formatted files, regardless of the format or media (paper, electronic or other format), preserved about facts, events or transactions which are created or received by or on behalf of the Company for providing its investment and / or ancillary services / activities.

Regulatory Framework

The Policy has been prepared in accordance with the following laws, regulations, directives and guidelines:

- Law 87(I)/2017 regarding the provision of investment services, the exercise of investment activities and the operation of regulated markets of 2017;
- Regulation (EU) No. 600/2014 of the European Parliament and of the Council, of 15 May 2014 on Markets in Financial Instruments;
- Commission Delegated Regulation (EU) No. 2017/565 of 25 April 2016, supplementing Directive 2014/65/EU of the European Parliament and of the Council;

- Directive 2014/65/EU of the European Parliament and of the Council, of 15 May 2014 on Markets in Financial Instruments; and
- Other laws, directives and circulars issued by the European Securities and Markets Authority ("ESMA") and the Cyprus Securities and Exchange Commission ("CySEC") from time to time, applicable to this Policy.

4 Roles and responsibilities

The Company's Board of Directors is responsible for the approval of this "Document Retention Policy" and any subsequent amendments / revisions.

In addition, the BoD has the responsibility, amongst others, to ensure:

- the overall implementation of the Policy;
- that the Policy is effectively communicated to all directors and employees of the Company;
- compliance with the provisions stipulated in the Policy;
- the timely and effective training and education of the concerned employees; and
- that disciplinary measures are taken and enforced when rules are not followed by employees.

The General Manager and Senior Management have the responsibility of:

- ensuring that an organisational structure / arrangement is in place securing the effective implementation of the provisions of this Policy;
- exercising effective oversight over the Company's document retention related arrangements and controls;
- undertaking training and education in connection with this Policy; and
- ensuring that disciplinary measures are taken and enforced when rules are not observed by employees.

The Compliance and AML Department has the responsibility to:

- ensure that the provisions stipulated in this Policy are followed at all times;
- periodically evaluate the effectiveness of the Policy and adopt any alternative or additional measures as are necessary and appropriate;
- periodically review and check whether the Records are kept for the appropriate period of time;
- providing advice in relation to the implementation of this Policy; and
- make available the above information to the relevant Competent Authority, if requested.

The IT Department has the responsibility to:

- oversee the development and periodic review of document retention arrangements in order to ensure compliance with its relevant obligations;
- ensure that all means of Records are properly stored, readily accessible, are of good quality and have not been altered;
- monitor on an on-going basis the Company's compliance in relation to the IT provisions stipulated in this Policy.

The Internal Audit Function has the responsibility to perform an audit, at least on an annual basis, in order to assess the compliance level of the employees/departments, as well as the Company as a whole, in connection with the provisions stipulated in this Policy.

5 Document Retention Obligation

Pursuant to MiFID II, the Company should establish and implement adequate arrangements / mechanisms in order to ensure that Records regarding:

- Investment and / or Ancillary Services / Activities provided by the Company to its clients / counterparties; and
- transactions concluded between the Company and its clients / counterparties,

are adequately stored and maintained for the required retention period.

Records shall be stored in a durable medium, which allows them to be replayed or copied and must be retained in a format that does not allow them to be altered or deleted. In addition, all Records should be readily accessible for the relevant persons and available to clients and / or the Competent Authority upon request.

The records shall be retained in a medium that it allows the storage of information in a way accessible for future reference and in such a form and manner that the following conditions are met:

- the Competent Authority is able to access them readily and to reconstitute each key stage of the processing of each transaction;
- it is possible for any corrections or other amendments and the content of the Records, prior to such corrections or amendments, to be easily ascertained;
- it is not possible for the records otherwise to be manipulated or altered;
- it allows the Head of Information Technology or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and

- the Company's arrangements comply with the record keeping requirements irrespective of the technology used and are adequate to mitigate any shortcomings or limitations of the record-keeping arrangements.

Further to the records described this Policy, the Company is also obliged to keep all policies and procedures required by MiFID II, the Markets in Financial Instruments Regulation (EU) No 600/2014, the Regulation (EU) No 596/2014 on market abuse ("MAR") as well as the Directive 2014/57/EU on criminal sanctions for market abuse ("CSMAD"), in order to ascertain that the Company has complied with the relevant obligations.

It is also noted that the Competent Authority may require the Company to keep additional records to those identified in this Policy.

6 Lifecycle of a record

The principle around Records retention is to ensure that Records are maintained properly and in line with the provisions of MiFID II throughout their lifecycle.

In particular, a record's lifecycle consists of the following stages:

No	Stage	Description
1	**Creation of Records**	This is the point in time where information and Records are created by the Company or received from clients / counterparties in different forms or format, such as written form, electronic form, etc. Each concerned department should keep accurate and complete Records, relating to the investment and / or ancillary services offered as well as transactions undertaken with its clients / counterparties.
2	**Use and Maintenance**	Each concerned department is responsible for the maintenance of its own Records and shall maintain and safeguard the integrity of those Records for the required retention period.
3	**Access**	The access to specific Records may be restricted due to the information contained in such Records (e.g. personal, commercial or operationally sensitive information). Each of the Company's departments shall liaise with the IT Department and establish / implement the necessary arrangements (e.g. access rights, passwords or system access restrictions) in order to safeguard such information. For example, electronic Records shall generally be stored in shared drives (with appropriate confidentiality protection) or in case of hard copies, secured / fireproof cabinets shall be used.

No	Stage	Description
4	**Storage and Retention**	Records should be stored in a searchable format and in such a medium that ensures their usability, reliability, authenticity and preservation for a period at least equal to the required retention period.
5	**Retrieval of Records**	Records shall be retrieved at any point in time without undue delay. Records must be stored in searchable format, allowing the Company to deliver such Records to the Competent Authority and / or Clients within a reasonable period of time. All encrypted data will be converted to an unencrypted format before making available a copy of such Records.
6	**Disposal of the Records**	Records could be disposed of after the expiration of the retention period, provided there is no legal hold or administrative value to keep such Records. Records authorised for disposal must be destroyed safely and securely, in a manner that ensures that the information cannot be reconstructed, in line with the applicable laws and regulations imposed by the Competent Authority from time to time.

7 Type of records

The Company shall provide clients, or potential clients, in good time and before the provision of investment and / or ancillary services with, but not limited to, information / documentation described below.

Information to clients

- General information:
  - General information about the Company as well as the Investment and /or Ancillary Services which the Company is authorised to provide;
  - Information about the nature and risks of Financial Instruments (risk disclosures on Financial Instruments).
- Information concerning Client categorisation, Appropriateness, Target Market Assessment and Investment Advice:
  - Client Categorisation / Re-categorisation letters;
  - Client Consent letters / Warning letters;
  - Client Questionnaire;

- Records regarding the appropriateness /suitability assessments performed by the Company / results of the appropriateness /suitability assessments ensuring that arrangements are designed to enable the detection of failures regarding the suitability assessment (such as mis-selling). Regarding the suitability assessment, relevant information about the client should be recorded (including how that information is used and interpreted to define the client's risk profile), and information about financial instruments recommended to the client or purchased on the client's behalf. Specifically:
  - any changes made by the Company regarding the suitability assessment, in particular any change to the client's investment risk profile;
  - the types of financial instruments that fit that profile and the rationale for such an assessment, as well as any changes and the reasons for them.
- Record regarding any investment advice provided and all investments (and disinvestments) made;
- Warning letters given to clients in cases where the Investment Service or product was assessed as non-appropriate for the Client;
- Warning letters given to clients in cases where the Client did not provide sufficient information to enable the Company to undertake a proper appropriateness assessment;
- Target market assessment related documentation (e.g. European MiFID Template);
- Other Client informative related documentation (e.g. license, financial statements, KYC related documents).

- Information on costs and charges:
  - Information about all costs and charges related to both the financial instrument(s) and Investment / Ancillary Service(s) provided to the Company's clients;
  - Information regarding the itemised breakdown of cost and charges, upon Client's request;
  - Illustration showing the cumulative effect of costs on return when providing Investment Services.
- Marketing communication:
  - All marketing communication related information that the Company disseminates in such a way that is likely to be received by clients or potential clients.

Client agreements

All clients' agreements, which set out the respective rights and obligation of the Company and the client, irrespective of the Client categorisation, should be stored at least during the period of the client relationship. Client agreements related documentation should include, among others, the following:

- Terms and Conditions;
- Investment Advice Agreement;

- Any other Agreement signed between the two parties.

Complaints handling records

The following Records shall be established / documented and maintained by the Company in relation to Complaints handling requirements:

- "Client Complaint Form" received from clients or potential clients;
- Complaints Register for recording clients' complaints;
- Documentation related to the reporting of clients' Complaints to CySEC; and
- Other related documentation (e.g. letters to clients, documentation of Complaints' internal assessment).

Regulatory / Internal related reports / documents

This sub-section describes all reports that demonstrate the Company's compliance with the applicable regulatory framework governing the Investment and /or Ancillary Services / Activities offered to its clients. Such reports / documents are prepared, maintained and communicated to the Company's Senior Executive Management, the Board of Directors as well as the Competent Authority.

Such reports / documents include, among others, the following:

- Compliance / Risk Management / Internal Audit reports submitted to the Company's Board of Directors on the implementation and effectiveness of the overall control environment for Investment Services and Activities, on the risks that have been identified and on the complaints-handling reporting as well as remedies undertaken or to be undertaken;
- Anti – Money Laundering reports;
- Conflicts of Interest Register;
- Records regarding personal transactions;
- Other Records required by MiFID II / the Law and described in the Company's Compliance Monitoring Program.

Policies and Procedures

The Company should keep records in a sufficient way in order to enable the Competent Authority to fulfil its supervisory tasks and to perform the enforcement actions under MiFID II and Market Abuse Regulation (MAR), and in particular to ascertain that the Company has complied with all relevant obligations, including those with respect to clients or potential clients and to the integrity of the market.

In this respect, the Company shall maintain all the policies, procedures as well as other relevant documents (e.g. departmental procedures, transactions) in relation to MiFID II and MAR.

Record retention schedule

Nature of obligation	Type of Record	Retention Period	Storage Location
Client assessment			
	Information to clients	• Duration of Client relationship; and • five (5) years after its termination.	Physical (paper arquived in ofiice) Local Drive and Cloud
	Client agreements	• Duration of Client relationship; and • five (5) years after its termination.	Physical (paper arquived in ofiice) Local Drive and Cloud
	Appropriateness assessment	• Five (5) years, 7 years if requested by CySEC.	Physical (paper arquived in ofiice) Local Drive and Cloud
Reporting to Clients			
	Obligation in respect of services provided to clients	• Duration of Client relationship; and • five (5) years after its termination.	Physical (paper arquived in ofiice) Local Drive and Cloud
Communication with Clients			
	Information about Costs and associated charges	• Five (5) years, 7 years if requested by CySEC.	Physical (paper arquived in ofiice) Local Drive and Cloud
	Information about the investment firm and its services, financial instruments and safeguarding of client assets	• Five (5) years, 7 years if requested by CySEC.	Physical (paper arquived in ofiice) Local Drive and Cloud

Nature of obligation	Type of Record	Retention Period	Storage Location
	Information to clients	• Five (5) years, 7 years if requested by CySEC.	Physical (paper arquived in ofiice) Local Drive and Cloud
	Marketing communications (except in oral form)	• Five (5) years, 7 years if requested by CySEC.	Physical (paper arquived in ofiice) Local Drive and Cloud

Nature of obligation	Type of Record	Retention Period	Storage Location
Organisational requirements			
	The firm's business and internal organisation	• Five (5) years, 7 years if requested by CySEC.	Physical (paper arquived in ofiice) Local Drive and Cloud
	Compliance reports	• Five (5) years, 7 years if requested by CySEC.	Physical (paper arquived in ofiice) Local Drive and Cloud
	Conflict of Interest record	• Five (5) years, 7 years if requested by CySEC.	Physical (paper arquived in ofiice) Local Drive and Cloud
	Risk Management reports	• Five (5) years, 7 years if requested by CySEC.	Physical (paper arquived in ofiice) Local Drive and Cloud
	Internal Audit reports	• Five (5) years, 7 years if requested by CySEC.	Physical (paper arquived in ofiice) Local Drive and Cloud
	Complaints-handling Records	• Five (5) years, 7 years if requested by CySEC.	Physical (paper arquived in ofiice) Local Drive and Cloud

8 Update of the Policy

The Company acknowledges its responsibility to establish, implement and maintain an effective written Document Retention Policy.

This Policy is created, owned and maintained by the Compliance Department, which is responsible for maintaining version series, original requests, and supporting documentation with all relevant approvals of this Policy. The Company's Policy is assessed and periodically reviewed, at least on an annual basis, or more frequently, should the need arise.

The following circumstances, amongst others, can trigger the review process at an earlier stage:

- Change in the service and product mix of the Company;
- Identification of situations that are not adequately captured in the Policy;
- The applicable legislation requires the update of the Policy.

The Compliance Department will use all reasonable endeavours to ensure that the Policy remains current and applicable to the existing business as well as any new business of the Company. The Compliance Department will also use all reasonable endeavours to ensure that the Policy remains appropriate to the structure and size of the Company as well as the nature, scale and complexity of the Company's business model.

Any amendment or the abolition of this Policy shall be approved by the Compliance Department and by the Board of Directors.

9 Training

The Company provides and expects all employees to attend trainings on document retention related requirements. Such training sessions are critical for ensuring that employees are able to understand the restrictions imposed by this Policy, identify and escalate potential breaches.

10 Policy violations

Where an allegation is made to the effect that an employee has violated this Policy, whether or not this is intentional, the matter shall be dealt with under the Company's internal rules. Where, after an internal investigation and subsequent disciplinary hearing, the allegation is upheld, the employee will be subject to a disciplinary action / penalty, which can include termination of employment.

Remedial and / or disciplinary action (where applicable) against employees and members of management and third parties may also include reimbursement or litigation, depending on the severity of the incident.