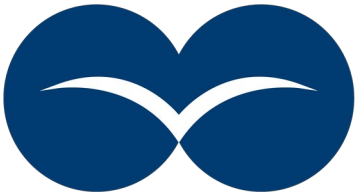

CONTROL OF RECORDS

Control of Records

Document Title	Control of Records
Document Ref	SM/INT/PRO/005
ISO Standard	ISO 9001:2015 / ISO 18788:2015 / ISO 28007:2015 / ISO 28000:2022 / ISO 45001:2018
Version	1.0
Classification	Internal
Effective Date	2 April 2026
Review Frequency	As per Document Register defined review date, or upon significant change
Owner	Group Compliance Director
Approved By	Pavel Shparber, CEO / Darren Watts, Group Compliance Director
Applicable Entities	Seagull Maritime FCZO, Seagull Maritime Malta, Seagull Maritime Nigeria, Seagull Maritime UK, Seagull Offshore

INTRODUCTION

This procedure defines the requirements for the identification, storage, protection, retrieval, retention and disposition of records across Seagull Maritime.

"Quality records" or "Security records" are those records which provide evidence of Seagull Maritime operating under the management system and meeting its contractual, statutory and regulatory requirements. This includes records from the Group Compliance Director (GCD), Quality Department, HR Department, Training Department, Security Department, Operations Department, and the Emergent Safety Reporting App (report.seagullmaritimeltd.com).

Records outside of this scope do not require control but may be controlled at the discretion of management where deemed necessary.

This procedure supersedes SOP-1002 (Control of Records Procedure) and SM/PRO/REC/001. It should be read in conjunction with SM/INT/PRO/002 (Control of Documents).

PROCEDURE

IDENTIFICATION

Seagull Maritime maintains records that are needed to provide evidence of conformity to requirements and the effective operation of the management system. These records are identified within the procedures and work instructions that generate them. Key records are listed in the Document Register (SM/INT/REG/001).

Control of Records

STORAGE

Softcopy records and data are stored on the company Google Drive which is subject to real-time backup and access controls managed by the GCD.

Personnel documentation for screening, recruitment and training is also stored on 1Clearview under the designated personnel module, and on the company online training platform for training records and certificates.

Incident and near-miss reports are recorded through the Seagull Safety Reporting App (report.seagullmaritimeltd.com), which provides a centralised, timestamped audit trail accessible to the GCD.

Hardcopy records should be avoided for environmental conservation, where possible, but where necessary they must be stored in appropriate filing that clearly identifies the records contained within.

PERSONAL DATA AND DATA PROTECTION

The Data Controller for the safe protection of Personal Data is the GCD who keeps all records pertaining to data protection controls.

The Personal Data relating to our security personnel is only kept for the purposes of conducting operations, meeting due diligence requirements, or as a legal requirement.

All Personal Data must be stored and managed in accordance with the European Union (EU) General Data Protection Regulation (GDPR) and any applicable local data protection legislation. Personal Data must be:

- ✓ used fairly and lawfully.
- ✓ used for limited, specifically stated purposes.
- ✓ used in a way that is adequate, relevant and not excessive.
- ✓ accurate.
- ✓ kept for no longer than is necessary.
- ✓ handled according to people's data protection rights.
- ✓ kept safe and secure (e.g. on Google Drive within limited access files).
- ✓ not transferred to 3rd Parties without adequate protection and/or approval of the individual concerned.

There is stronger legal protection for more sensitive personal data, which is never divulged to 3rd parties. This includes information about: ethnic background, political opinions, religious beliefs, health, sexual health, and criminal records.

RETENTION, RETRIEVAL AND DISPOSITION

Records shall be retained according to: legal and fiscal requirements, client requirements, shelf-life period, intended use of services and products, and need for trend analyses and verification.

The UK DPA and EU GDPR stipulate statutory retention periods for some HR records such as personnel files and pay records. Where applicable, these periods are observed as a minimum.

Accident Records must be kept for a minimum of 3 years.

All financial records must be kept for a minimum of 5 years, in accordance with Auditor requirements.

All checklists and forms after completion, and minutes of meetings, shall be filed and accessible for a period of no less than 5 years from the date of creation.

PCASP training records, firearms competency certifications, weapons handling and marksmanship records, weapons maintenance logs, and records relating to the operational use of firearms shall be retained for a minimum of 6 years from the date of the record. This retention period aligns with the limitation period for civil claims under the UK Limitation Act 1980 and is justified under GDPR Article 17(3)(e) (establishment, exercise or defence of legal claims) as an exception to data subject erasure requests within this retention window.

All other records should not be kept longer than necessary for the purpose for which they were processed. Once a record is no longer required, it shall be reviewed to determine whether it should be archived or destroyed.

Records that are discarded after retention shall be permanently destroyed by secure delete (soft copies) or shredding (hard copies).

As required by client contract or regulatory requirements, quality and information security records may be made available for evaluation by clients or their representatives for an agreed period.

PROTECTION

The relevant process managers shall be designated record "controllers" and must ensure their assigned records are stored in the correct location and are properly maintained.

Confidential records must be clearly marked as such and protected from accidental or intentional release. Access controls on Google Drive shall be used to restrict access to authorised personnel only.

The GCD is responsible for all Google Drive issues which might affect backup of data.

Where possible, individuals must work directly from Google Drive to ensure records are backed up in real time.

Staff should sync their required Google Drive folders to their workstations to ensure backed-up copies are available for offline working.

Entries made by hand on hardcopy forms shall be made in ink.

White-out or correction tape is not to be used on any quality or information security records. The original entry should be scored through with a single line, initialled and dated.

RELATED DOCUMENTS

Control of Documents (SM/INT/PRO/002)

Document Register (SM/INT/REG/001)

REVIEW

This procedure shall be reviewed at the frequency defined in the Document Register (SM/INT/REG/001), or earlier if a significant change occurs that affects records control practices within Seagull Maritime.