



## **DATA RETENTION POLICY**



# Contents

- 1. PURPOSE AND POLICY STATEMENT ..... 3**
- 2. SCOPE OF APPLICATION ..... 3**
- 3. DEFINITIONS ..... 3**
- 4. EXCEPTIONS ..... 4**
- 5. RETENTION PERIOD ..... 4**
  - 5.1 Retention schedule: Governance and management records.....5
  - 5.2 Retention schedule: Finance, accounting, and taxation records .....6
  - 5.3 Retention schedule: Commercial, Business development and Procurement records.....7
  - 5.4 Retention schedule: Operational and technical data .....8
  - 5.5 Retention schedule: HR records .....9
  - 5.6 Retention schedule: HSE/HSSE records.....9
- 6. DISPOSAL..... 9**
- 7. RESPONSIBILITIES ..... 9**
- 8. SPEAK UP ..... 10**
- 9. DISCIPLINARY ACTION..... 10**
- 10. REVIEW PROCESS..... 10**

## 1. PURPOSE AND POLICY STATEMENT

We at QTerminals generate, collect, and process considerable volumes of data and documents in carrying out our business activities. Retaining records of this data and documents is necessary to ensure business continuity and to comply with our business, contractual and regulatory obligations. However, eventual disposal of the data records and documents is necessary to reduce costs and administrative burdens of storing them, as well as to ensure confidential and compliant treatment of various types of data and documents.

QTerminals considers responsible handling and retention of our records to be an integral part of our social responsibility. With the Data Retention Policy (hereinafter “Policy”), we provide guidelines on record management and handling, retention, and disposal practices, which allow us to ensure compliance with legal requirements, improve business continuity, and reduce costs of maintaining and storing our records.

## 2. SCOPE OF APPLICATION

The Policy applies globally to all Employees. This Policy does not replace any national or international law. In case of any conflict, legislation must take precedence over this Policy. Employees are requested to promptly notify Compliance team in case such conflict has been identified.

The Policy applies to data in all forms, including soft (electronical) and hard (on paper) copies, regardless of a format (e.g., text, picture), location, media, and communication device.

## 3. DEFINITIONS

**Employees** means all QTerminals’ employees (including contracted workers), officers, and directors.

**Ethics Review Panel (ERP)** means a multidisciplinary body within QTerminals committed to reviewing all reported alleged unethical matters, misconduct and wrongdoings in a timely manner and deciding on the respective disciplinary action. ERP members are selected on the case-by-case basis by the Group Legal and Compliance Director, depending on the nature and criticality of the alleged misconduct and/or wrongdoing.

**Line Manager** is a person with direct managerial responsibility for a particular Employee.

**QTerminals or Company** means QTerminals W.L.L. and its controlled subsidiaries, affiliates, and joint ventures.

**Third Party** is any customer, client, business partner, supplier, service provider, consultant and other representatives with whom QTerminals has a business relationship.

## 4. EXCEPTIONS

In case a record contains personal information, Data Protection Policy should take precedence over Data Retention Policy in relation to management, retention, and disposal of records. Please refer to Data Protection Policy for detailed guidance. In addition, records cannot be disposed and must be retained regardless of the retention schedule under the following circumstances:

- **Legal hold:** Pending or reasonably foreseeable legal claim, litigation, investigation, or similar legal actions that relate to given records. In case of a legal hold, Legal department should notify responsible Employees

and specify which records must be retained until further notice. Disposal of these records is possible only after the end of legal proceedings and upon approval from the Legal department.

- **Concession agreements and other contractual obligation:** In case contract requires longer retention period than stated in this Policy, contract should take precedence and record's retention period should be adjusted accordingly.
- **Business continuity requirement:** In case process owner requests to extend the retention of a record in order to ensure business continuity and support completion of business processes, the retention period can be adjusted after the approval of Compliance team.

## 5. RETENTION PERIOD

Tables with retention schedules below set the minimum time period for retention of records depending on the information it contains. Retention period is determined solely based on content of the record, irrespective of its format or form. Thus, retention periods apply equally to electronic records and hard copies. Generally, it shall not be required to retain both electronic and paper versions of the same record. However, if a paper record contains physical signatures or stamps, it must be retained as a hard copy and cannot be disposed even if an electronic version of the same record exists.

Retention tables below provide general guidance on the retention period for various types of records. However, responsible Employee should review applicable legal and contractual obligations (e.g., Concession agreements) in each business unit as they take precedence over this Policy. In cases if the Employee is unsure whether specific legal and/or contractual obligations apply, they should consult with their Line Manager and/or Legal department.

Retention schedule covers key types of records that we use, but not always every record can be clearly attributed to a specific type. In this case, responsible Employee should apply common sense and judgment to allocate specific record to the most relevant type and use respective retention period. In case a record can be attributed to several types, it should be retained for the longest applicable period. If you find yourself in doubt regarding which type of record and respective retention period to use, please consult with your Line Manager.

During the retention period, key principles of confidentiality, security, integrity, and availability of information management system, as well as applicable guidelines of the Information Security Management System Policy Manual should be closely followed.

Several exceptions, outlined in the chapter "Exceptions" above, apply to the retention periods, most notably to records containing personal data.

### 5.1 Retention schedule: Governance and management records

Record type	Retention period
Corporate Governance documents, including Articles of Association, other document on forming and dissolving of legal entities, intercompany agreements	Permanent
Delegation of Authority Matrix (DOA)	Permanent
Compliance registers	Permanent
Resolutions of the Shareholders, Board and Board Committees, reports and/or presentations to and by Board Committee and Shareholders, meeting agendas and minutes	10 years
Partnership agreements, buy-sell agreements	10 years after expiration
Power of Attorney	10 years after expiration
Litigation with Third Parties	10 years
Non-financial audit reports (internal and external)	10 years
Policy, procedure and process documents	10 years after revision
Company strategy and business plans, managerial financial reports	7 years after expiration

## 5.2 Retention schedule: Finance, accounting, and taxation records

Record type	Retention period
Accounting records	10 years
Accounting transactions supporting documents	10 years
General ledger, including subsidiary ledgers (suppliers, customers, inventory records, etc.) for holding entities	10 years
Fixed Asset Register	10 years
Financial Delegation of Authority (i.e., banking signatories)	10 years after expiration
Bank statements	10 years
Financial statements and Auditor's reports	10 years
Management letter received from Auditor(s)	10 years
Management representation letters issued to the Auditor(s)	10 years
Periodic financial reports	10 years
Tax records and filings	10 years
Subsidy financial records	10 years
Payroll records	10 years
Investment and divestment records	10 years after completion
Financing (loan) records	10 years after expiration
Write-off / write-back approvals	10 years
Invoicing supporting documents	10 years
Annual plans and budgets	7 years

### 5.3 Retention schedule: Commercial, Business development and Procurement records

Record type	Retention period
Permits, licenses, certifications	Permanent
Contracts, agreements, and other arrangements	10 years after expiration
Commercial or business letters received and sent	10 years
Business development records, including due diligence reports	10 years
Successful tender documents	10 years
Unsuccessful tender documents	6 years
Published tariff	10 years after expiration
Discount/rebate/waiver approval documents	10 years after expiration/completion

### 5.4 Retention schedule: Operational and technical data

Record type	Retention period
Construction blueprints and other design and construction documentation	Permanent
Port/terminal/superstructure/infrastructure design, blueprints, layouts, and specification documents	10 years after end of operation of terminal/infrastructure
Equipment documentation, including but not limited to equipment maintenance record, equipment certification documents, etc.	10 years after end of operation of equipment
Supplier's guarantee and warranty documents	10 years after end of operation
Commercial records and reports to management	6 years
Operational records and reports to management, including asset productivity/efficiency records, operational productivity/efficiency records, vessel operational records, etc.	6 years

Record type	Retention period
Operational workforce deployment records, including shifts schedule (Roster Record), overtime allocation records, etc.	6 years
Consumable stores and spares inventory records	6 years
Terminal/port cargo inventory records	6 years
Cargo release supporting documents, including customs declarations, etc.	6 years

#### 5.5 Retention schedule: HR records

Record type	Retention period
Employment contracts	6 years after end of employment
Personnel files, including job history (e.g., records, assessment, etc.) and payroll-related records (e.g., pension scheme, bonuses, etc)	6 years after end of employment
Payroll register and salary payment records	6 years after end of employment
Recruitment information	6 months


#### 5.6 Retention schedule: HSE/HSSE records

Record type	Retention period
Accident book	Permanent
HSE/HSSE records, reports to management, audit reports, related studies (e.g., impact assessments), compliance records, visitors' books	6 years
Quality certificates	6 years after expiration

## 6. DISPOSAL

When retention period of a record expires and it is not subject to exceptions, responsible person/entity should review the document to ensure that it can be disposed without harm to the Company. Confidentiality





and classification procedures should be followed during disposal. Physical records with publicly available information can be recycled but sensitive and confidential data must be shredded to ensure that it becomes unreadable. Electronic records should be fully erased and not simply deleted. Regardless of the form, all copies should be disposed at the same time.

## **7. RESPONSIBILITIES**

All Employees are responsible for adhering to this Policy. We expect them to read, understand, acknowledge, and adhere to all aspects of this Policy and any supplementary procedures issued by QTerminals. All Employees are encouraged to contact Line Manager and, if required, HR or Compliance Officer/Representative to clarify questions, request information or express concerns relating to this topic.

All Line Managers, along with the relevant guidance of Compliance or HR departments, shall ensure that any concerns related to data retention of those Employees reporting to them are resolved.

Management of QTerminals is responsible for ensuring that legal requirements and provisions of this Policy are followed. Each managing senior executive of QTerminals at port or terminal level must ensure that the business unit they are responsible for is and will remain fully compliant with this Policy, promoting awareness and understanding of this Policy and ensuring allocation of adequate resources to effectively implement this Policy. Specifically, the Compliance team has to ensure that required processes are in place that enable adherence to this Policy.

## **8. SPEAK UP**

QTerminals promotes an environment of integrity and transparency under which its Employees are encouraged to report any violation or suspected violation of this Policy within QTerminals or at any of the Third Parties, either by informing their Line Manager, their HR department, their Compliance Officer/Representative or alternatively through the QTerminals Ethics Line, which is available on QTerminals intranet, QTerminals website and as a dedicated phone line.

Additionally, any retaliation against anyone who notices and reports a known or suspected violation of the Policy is strictly prohibited. Anyone proven to have retaliated against a person who has reported a breach in good faith is to be subjected to disciplinary action. However, any false or malicious allegations may lead to appropriate disciplinary and legal action, up to and including termination of employment.

For more information on the whistleblowing process, please refer to [QTerminals Whistleblower and Anti-fraud Procedures](#).

## **9. DISCIPLINARY ACTION**

At QTerminals, all Employees are expected to abide by this Policy. Any violation thereof may result in disciplinary action, termination of employment or legal proceedings.

In case the complaints for wrongdoings warrant an investigation, there will be investigations whose results and proposed corrective actions will be reviewed by the Ethics Review Panel (ERP). The corrective actions will be determined based on the facts and circumstances of the breach of conduct and results of the investigation.

For more information on the process of investigation of alleged misconduct and violations of the Code of Conduct or this Policy, please refer to [QTerminals Whistleblower and Anti-fraud Procedures](#).

## 10. REVIEW PROCESS

Compliance team is responsible for monitoring risks relating to data retention and regularly reviewing, evaluating and improving this Policy. Risks and overall effectiveness of the Policy should be reported to executive management.

**Approved By:**



---

**Group CEO**  
**Neville Bissett**