

#### **10.4 Education and Training of Users**

##### **10.4.1 Training Program**

HR Department in association with IT Department shall establish a formalized and structured training program for employees to ensure that they have adequate knowledge necessary to securely perform their duties. The training program shall focus on developing:

- a. Relevant and needed IT knowledge and skills within the workforce
- b. Training supporting competency development and helping personnel understand and learn how to perform their IT roles and responsibilities.
- c. Trainings that are tailored to the specific needs of each group of people who have been identified as having significant responsibilities for IT in the Company.

The tools and channels used by the training program may include but will not be limited to:

- a. Class-room training sessions;
- b. Computer based training;
- c. Self-paced computer based training;
- d. External training sessions.

The training channels may also be integrated with the Company's regular activities like the following:

- a. Employee induction programs;
- b. External trainings.

The Company shall also evaluate enrollment of key employees for relevant certification courses including those for IT Security like CISA, SAP, CISSP, CEH, ITIL, ISO 27001 and the like.

#### **10.5 Management of the Configuration**

Company shall establish and maintain an accurate and complete configuration repository of all hardware and software configurations. Company shall ensure that all configuration information is stored in the repository, baselines are established and the repository is updated as and when required.

#### **10.6 Management of Problems**

Company shall establish problem management processes to identify, classify, analyze and resolve problems. The problem management process shall include identification of recommendations for improvement, maintenance of problem records and review of the status of corrective actions.

#### **10.7 Management of Records and Data**

Company shall establish procedures to manage the media library, backup and recovery of data, and proper disposal of media.

Company shall implement an electronic and physical records retention schedule, to ensure that Company adheres to existing recordkeeping regulations and requirements and does so consistently. Company shall formulate a process of systematically determining which records need to be captured and how long they need to be retained in the Company.

#### **10.8 Management of the Physical Environment**

Company shall ensure regular monitoring of physical environmental factors and management of physical access to computer processing facilities in order to reduce business interruptions from damage to computer equipment and personnel.

## **Petronet Record Retention and Destruction Policy**

### **1. Purpose**

The purpose of Petronet Record Retention and Destruction Policy is to ensure that Petronet LNG Limited (Hereinafter referred as PLL) retains its official records in accordance with the requirements of all applicable laws and to ensure that official records no longer needed by PLL are discarded at the proper time. This Policy provides guidelines concerning the timelines for retention of official records under ordinary business circumstances, as well as in the event of any pending or imminent government investigation, audit or proceeding, or any civil or criminal lawsuit.

This Policy also includes guidelines for;

- a) Ensuring protection and maintenance of documents in the event of, elimination by accidental or unintentional destruction.
- b) Retention and maintenance of documents necessary to facilitate operations by promoting efficiency within PLL as well as to comply with applicable legal requirements
- c) Destruction of documents which no longer need to be retained; and
- d) Responsibilities of all the stakeholders viz, Directors, employees, suppliers, vendors etc. concerning document retention and destruction.

### **2. Scope**

This Policy shall be applicable to all the business or non-business Units/sub-units of the company which is under direct jurisdiction of Petronet LNG Management.

### **3. Administration**

#### **3.1 Responsibilities of the Administrator.**

MD & CEO shall be the administrator (hereinafter referred to Administrator) in charge of the administration of this Policy. The Administrator shall also be authorized to :

- a) Any modification to the Document Retention Schedule from time to time.
- b) Periodic review of this Policy
- c) Authorizing Functional Heads viz Directors/Head HR for finalizing scope for creation, retention and destruction of documents pertaining to concerned areas of operation.

- d) Authorizing, Functional Heads viz Directors/Head HR to determine how privacy (confidentiality) will be applicable to PLL's documents pertaining to concerned areas of operation.
- e) Any other act he may deemed necessary to give effect/improvise the policy.

#### **4. Classifications of documents**

##### **4.1 Categories of information based upon intended use and expected impact if disclosed.**

**i. Public:** Information intended for public use that, when used as intended, would have little to no adverse effect on the operations, assets, or reputation of PLL or the PLL's obligations concerning information privacy.

**ii. Internal:** Information not intended for parties outside PLL that, if disclosed, could have adverse effect on the operations, assets, or reputation of PLL, or the PLL's obligations concerning information privacy.

**iii. Confidential/ Sensitive:** Sensitive/ confidential information is defined as information that is protected against unwarranted disclosure and the information intended for limited use within PLL that, if disclosed, could be expected to have a serious affect on the operations, assets, or reputation of PLL, or the PLL's obligations concerning information privacy. Such confidential information can be in any form including on printed media (e.g., forms, reports, memoranda, correspondence, microfilm, microfiche, books), computers, networks, magnetic or optical storage media (e.g., hard drive, zip drive, flash drive, memory card, diskette, tape, CD, DVD), physical storage environments (e.g., offices, filing cabinets, drawers), or in a person's memory.

##### **4.2 Confidential/Sensitive Documents.**

Workplace information can generally be broken down into three categories:

- a) Employee information - personal identifying information
- b) Management information - includes corporate strategy, strategy, financial results, employee related issues, investment plans, etc.
- c) Business information - refer to confidential business information as "proprietary information" or "trade secrets." This refers to information that's not generally known to the public and would not ordinarily be available to competitors except via illegal or improper means.

##### **4.3 General Principles to deal with Confidential documents**

- a) All confidential information gathered and maintained by Directors and other employees in the course of their duties and responsibilities for PLL is considered PLL information and, as such, must be used, maintained and handled by them in a manner that appropriately safeguards and secures such confidential information.

- b) All confidential/sensitive information in digital format must be handled in accordance with relevant provisions of IT Policy of the company.
- c) All confidential/sensitive information in physical format must be stored in file cabinets that are secured and locked.
- d) Employees who are authorized to access and use such confidential information shall take all necessary precautions to assure that proper administrative, technical, and physical safeguards are established and followed in order to protect the confidentiality of such confidential/sensitive information.
- e) Employees shall only make copies of confidential/ sensitive data or document assets and move the same outside the premises of PLL with prior approval.

#### **5. Document Creation and Generation.**

The authorized Functional Heads viz Directors/Head HR shall discuss with all concerned stakeholders regarding creation of documents with respect to concerned function/s. All such documents shall be grouped & classified based on an approved common nomenclature and to be followed across all locations. This will help to segregate all the documents effectively from each others, so that, when it comes time to destroy (or retain) those documents, they can be easily culled from the others for disposition.

#### **6. Suspension of Document Destruction; Compliance.**

PLL becomes subject to a duty to preserve (or halt the destruction of) documents once litigation, an audit or a government investigation is reasonably anticipated. Further, government law imposes criminal liability (with fines and/or imprisonment) upon whomever —knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department in relation to or contemplation of any such matter or case. Therefore, if the Administrator or authorized Functional Heads, becomes aware that litigation, an audit or an investigation has been instituted, or is reasonably anticipated or contemplated, document destruction under this Policy shall be immediately stopped, communicating the order to all affected constituencies in writing. The Administrator or authorized Functional Heads ,may thereafter amend or rescind the order only after conferring with legal department. If any board member or staff member becomes aware that litigation, an audit or an investigation has been instituted, or is reasonably anticipated or contemplated, with respect to the organization, and they are not sure whether the Administrator or authorized Functional Heads is aware of it, they shall make the Administrator or authorized Functional Heads aware of it. Failure to comply with this Policy, including, particularly, disobeying any destruction halt order, could result in possible disciplinary action, civil or criminal sanctions. In addition, it could lead to disciplinary action including possible termination.

## 7. Record Retention

The following table indicates the minimum requirement period for which the designated document need to be preserved .

| <u>Document Type</u>   | <u>Retention Period</u>            |
|--|------------------------------------|
| <b>Corporate</b>   |                                    |
| a) Memorandum and Articles of Association and its Amendments   | Permanent                          |
| b) Bylaws and Amendments   | Permanent                          |
| c) Board and committee meeting agendas and minutes   | Permanent                          |
| d) Annual Reports  | Permanent                          |
| e) Corporate Filings   | Permanent                          |
| f) Correspondence with MCA, Stock Exchange, R&A or any other Regulatory/Statutory Authority                            | Permanent                          |
| g) Exemption Application   | Permanent                          |
| h) Exemption Determination Letter  | Permanent                          |
| i) Permanent Licenses and Permits  | Permanent                          |
| j) Copyrights & Trademark Registration   | Permanent                          |
| k) Intellectual Property Documentation   | Permanent                          |
| l) Conflict-of-interest disclosure forms   | 8 years                            |
| m) Legal Correspondence & Documents  | Permanent                          |
| n) Investor Relationship   | 8 years                            |
| <b>Management</b>  |                                    |
| a) Business Model and Strategic business Plan  | 10 years after Plan period         |
| b) Minutes of Meeting of Executive Committee   | 10 years                           |
| c) Business plans and budgets  | 10 years                           |
| d) Risks/opportunities assessment documents  | 10 years                           |
| e) Project feasibility & business plans  | 10 years                           |
| f) Standard contracts  | 10 years after all obligations end |
| g) Non-standard contracts and Agreements (government, projects, long term, high value)                                 | Permanent                          |
| h) Standard Contracts and agreements (routine)   | 10 years after all obligations end |
| i) Statutory Compliance  | 10 years                           |
| j) Notices/ MOU / agreements / supplementary agreements  | 10 years after all obligations end |
| k) Documents related to selection, acquisition, development, installation, of infrastructure and assets of the company | Permanent                          |
| l) CSR Records   | 10 years                           |

## Projects and Operations

### General

- |  |   |
|--|---|
| a) Business critical analysis and business performance   | 10 years  |
| b) Project and Operational plans   | 10 years  |
| c) Mandatory policies and SOPs governing all aspects of Technical, Projects, Shipping and Operations, HSSE and asset integrity | Current version with revision history of 10 years |
| d) Original drawings, manuals, contracts and other documents   | Permanent   |
| e) Minutes of health, safety, security and environment and asset integrity standards meeting                                   | 5 years   |
| f) Capex and Opex expenditure  | 10 years  |
| g) Compliance documents of audits and statutory requirements   | 5 years   |

### Projects

- |  |           |
|--|-----------|
| a) Due diligence report of projects  | 10 years  |
| b) Proposals, RFQ and EPC contract documents   | 10 years  |
| c) Feed, detailed engineering, construction and commissioning  | Permanent |
| d) Vendor contract/ assignment   | Permanent |
| e) Performance Security, Progress/Performance  | 10 years  |
| f) Project Quality Assurance/Quality Control   | 10 years  |
| g) Approval of amendments on drawing   | 10 years  |
| h) Construction Documents  | Permanent |
| i) Testing and Commissioning   | Permanent |
| j) As-built Drawings and Operations and Maintenance Manuals  | Permanent |
| k) Conflict resolution on Contract agreements and obligations, Contract documents, register, depository, Technical variation, and contract matters | 10 years  |
| l) Project management, project engineering, discipline engineering and construction  | 10 years  |
| m) Final Project Certificate and Final Report  | Permanent |
| n) MIS of Projects   | 5 years   |

### Plants General

- |  |           |
|--|-----------|
| a) Annual Plan   | 5 years   |
| b) Statutory approvals, licenses, compliances, documentation, returns  | Permanent |
| c) Statutory payment, Custom duty, ILH, Port Dues, Water Front Loyalty | 10 years  |
| d) Terminals performance   | 10 years  |
| e) Safety & ISO Audits   | 10 years  |
| f) Compliance report of safety, security, fire and statutory audits    | 10 years  |
| g) Custody Transfer  | 5 years   |
| h) Approval of Management of Change                                    | 5 years   |

- |                                       |           |
|---------------------------------------|-----------|
| i) Terminal Assets and equipment Plan | Permanent |
| j) MIS of Plant Efficiency            | 3 years   |

**Operations**

- |   |           |
|---|-----------|
| a) LNG received – quantity and quality  | 3 years   |
| b) Daily send out actual vs Targets   | 3 years   |
| c) Internal Consumption of LNG  | 3 years   |
| d) Permits and Fluid- Lock out sheet  | 3 years   |
| e) Check sheet of measurement System (DCS)  | 3 years   |
| f) Water quality, Nitrogen Level reports  | 3 years   |
| g) Plant Performance Metrics -Operating cost/send out ratio of consumables , Diesel and power utilisation | 5 years   |
| h) Availability of equipment/system   | 3 years   |
| i) Asset register   | Permanent |

**Ports**

- |  |          |
|--|----------|
| a) Fuel Consumption of Tugs, Time Chartered Vessels, and Port Operator Charges | 5 years  |
| b) Vessel berthing and un-berthing schedule/actual                             | 3 years  |
| c) Protest letter from ships   | 5 years  |
| d) Availability of Port and Marine Asset                                       |          |
| e) Service delivery as per Port Operator Service Agreement                     | 5 years  |
| f) Port asset Register Current version with history of                         | 10 years |
| g) Port Equipment Maintenance  | 5 years  |
| h) Painting of Port  | 5 years  |

**Maintenance**

- |   |          |
|---|----------|
| a) Result and Targets - Preventive Maintenance, Breakdown Maintenance, Calibration, Material Resource | 3 years  |
| b) Statutory Compliance for Electrical, Mechanical, Instrumentation and Material                      | 3 years  |
| c) Material Requirement Schedule  | 3 years  |
| d) OEM Manual and SOP Current version with revision history of  | 10 years |
| e) Time sheet for breakdowns maintenance / critical situations  | 5 years  |
| f) Calibration sheet of critical meters / gauges & detectors  | 3 years  |

**Material management**

- |                         |          |
|-------------------------|----------|
| a) Material plan        | 3 years  |
| b) Materials Accounting | 10 years |
| c) Vendor Development   | 3 years  |
| d) Contracts            | 10 years |
| i. AMCs                 |          |

- ii. Hiring of services
- iii. Equipments
- e) Purchase Orders and Challans 10 years
- f) Material Requisition 3 years
- g) Spares / consumables consumed 10 years
- h) Material Department Efficiency Analysis 3 years

### Security

- a) Checklist of ISPS/NSPC/Coast Guard/Port Facility Security 3 years
- b) Contracts for maintenance of Security Equipment 10 years
- c) Security Risk Assessment 3 years
- d) Security and Surveillance check sheet 5 years
- e) Systems check sheet 10 years
  - i. Physical and Electronic Security Systems
  - ii. surveillance and vigilance Systems
  - iii. Investigations, Search, Law
  - iv. Protection and Security Automation
- f) Service delivery as per Security Service Agreement 10 years

### Fire

- a) Checklist of Fire drill 1 year
- b) Fire Risk Assessment 3 years
- c) Check sheet for test all the fire prevention, detection and protection asset / equipment 10 years
- d) Availability sheet of Fire Prevention and Fire Fighting equipment and appliances 10 years
- e) Checklist of emergency preparedness 1 year

### Safety

- a) Checklist of Safety and Environment Protection Practices (Safety Awareness training, knowledge sharing, defining unsafe Acts and Safety Promotion Activities) 10 years
- b) Checklist of Housekeeping practices and unsafe Condition 3 years
- c) Safety systems
- d) Job safety analysis
  - i. Hazard within the job
  - ii. Safety precaution for carrying out the job 10 years
- e) Minutes of Safety Committee Meeting 10 years
- f) Rectification of unsafe conditions and unsafe act 10 years
- g) Safety Awards Permanent
- h) Statutory Compliance Permanent



## IT & Systems

|   |          |
|---|----------|
| a) Availability of system servers and allied equipment            | 5 years  |
| b) Service of Infrastructure                                      | 2 years  |
| i. Asset management   |          |
| ii. Service level management                                      |          |
| iii. Issues management  |          |
| iv. Configuration management                                      |          |
| v. Application change management                                  |          |
| vi. Communications management                                     |          |
| c) Training to business process owners                            | 1 years  |
| d) Data backup  | 8 Years  |
| e) Check sheet of uptime of lease line/internet facility and vsat | 2 years  |
| f) Check sheet of Network infrastructure and network security     | 5 years  |
| g) Consumables consumed   | 10 years |

## Accounting and Finance

|   |                                    |
|---|------------------------------------|
| a) Business plan, performance objectives and projections        | 10 years after Plan period         |
| b) Investment appraisal and proposal evaluation reports         | 10 years                           |
| c) Financial modeling   | 10 years                           |
| d) Bank guarantees, performance bonds                           | 15 years after all obligations end |
| e) Tax payments and Returns compliances                         | Permanent                          |
| f) Annual Financial Statements and Audit Reports                | Permanent                          |
| g) Internal Audit Reports                                       | 5 years                            |
| h) Bank Statements, Reconciliations & Deposit Slips             | 10 years                           |
| i) Accounts Payable   | 10 years                           |
| j) Accounts Receivable  | 10 years                           |
| k) Cheque register and checks                                   | 10 years                           |
| l) Canceled Cheques – routine                                   | 10 years                           |
| m) Canceled Cheques – special, such as loan repayment           | Permanent                          |
| n) Receipts   | 3 years                            |
| o) Employee/Business Expense Reports/Documents                  | 10 years                           |
| p) General ledgers and journals (includes bank reconciliations) | Permanent                          |
| q) Interim Financial Statements                                 | 10 years                           |
| r) Pricing strategies, risk matrix                              | 10 years                           |
| s) Contract Records   | Permanent                          |
| t) Documents Evidencing Terms of Contract                       | Permanent                          |
| u) Auditor management letters                                   | 10 years                           |
| v) Payroll records  | 10 years                           |
| w) Bank deposits and statements                                 | 10 years                           |
| x) Chart of accounts  | 10 years                           |

- y) Investment performance reports 10 years
- z) Equipment files and maintenance records 10 years after disposition
- aa) Mortgages & Note Agreements 15 years after all obligations end
- bb) Correspondence — general 3 years
- cc) Asset Register Permanent

#### **Tax**

- a) Tax exemption documents & correspondence Permanent
- b) Rulings Permanent
- c) Annual and other returns Permanent
- d) Tax returns Permanent

#### **Insurance**

- a) Business interruption, asset valuation, General Liability Insurance Policies Permanent
- b) Insurance Claims Records Permanent
- c) Policies — occurrence type Permanent
- d) Policies — claims-made type Permanent
- e) Accident reports 10 years
- f) Safety reports 10 years
- g) Claims (after settlement) 10 years

#### **Legal and Contracts**

- a) Contracts, related correspondence and other supporting documentation 10 yrs after termination
- b) Legal correspondence Permanent

#### **Miscellaneous**

- a) Disaster Recovery Plan 10 years after replacement
- b) Policies and Procedures Manual Current version with revision history
- c) Technical and Intellectual Up gradation Current version with revision history of 10 years

#### **Property – Real, Personal and Intellectual**

- a) Property deeds and purchase/sale agreements Permanent
- b) Property Tax Permanent Real Property Leases Permanent
- c) Personal Property Leases 10 years after all obligations end
- d) Trademarks, Copyrights and Patents Permanent
- e) Mortgages, security agreements 10 years after all obligations end

#### **HR, Administration and PR**

- a) HR, Admin and PR policies Current version with revision history of 10 years

|   |                              |
|---|------------------------------|
| b) Talent Management Documents                        | 10 years                     |
| c) Recruitment Advertisements                         | 3 years                      |
| d) Selection documents                                | 3 years                      |
| e) Performance Contracts<br>(PMS documents)           | 5 years                      |
| f) Training Documents                                 | 5 years                      |
| g) Succession Planning                                | 10 years                     |
| h) Employees related Surveys                          | 5 years                      |
| i) Statutory and regulatory compliances               | Permanent                    |
| j) Capex and Opex                                     | 10 years                     |
| k) Personnel Records                                  | 10 yrs after employment ends |
| l) Employee contracts                                 | 10 yrs after termination     |
| m) Retirement and pension records                     | Permanent                    |
| n) Employee Expense Reports                           | 10 years                     |
| o) Employee Payroll Records                           | 10 years                     |
| p) Timesheets and daily time reports                  | 3 years                      |
| q) Administrative contract                            | 10 years                     |
| r) Publication of statutory compliance of information | 10 years                     |
| s) CSR activities/reports etc.                        | 10 years                     |

#### **Correspondence and Internal Memoranda**

- |  |                              |
|--|------------------------------|
| a) Hard copy correspondence and internal memoranda relating to a particular document otherwise addressed in this Schedule should be retained for the same period as the document to which they relate. |                              |
| b) Hard copy correspondence and internal memoranda relating to routine matters with no lasting significance  | Two years                    |
| c) Correspondence and internal memoranda important to the organization or having lasting significance  | Permanent, subject to review |

#### **Electronic Mail (E-mail) to or from the organization**

- |  |                              |
|--|------------------------------|
| a) Electronic mail (e-mails) relating to a particular document otherwise addressed in this Schedule should be retained for the same period as the document to which they relate, but may be retained in hard copy form with the document to which they relate. |                              |
| b) E-mails considered important to the organization or of lasting significance should be printed and stored in a central repository .  | Permanent, subject to review |
| c) E-mails not included in either of the above categories  | 12 months                    |
| d) Electronically Stored Documents Electronically stored Documents (e.g., in pdf, text or other electronic format) comprising or relating to a particular document otherwise addressed in this Schedule should be retained for the same period as the          |                              |

document which they comprise or to which they relate, but may be retained in hard copy form (unless the electronic aspect is of significance).

- e) Electronically stored documents considered important to the organization or of lasting significance should be printed and stored in a central repository (unless the electronic aspect is of significance). Permanent, subject to review
- f) Electronically stored documents not included in either of the above categories Two years

## **12. Digitization of records/data:**

All such data or records, where the retention period has been defined as Permanent, such records/documents needs to be digitized and stored on IT server of the company in accordance with IT Policy of the company.

## **13. Retention and Disposal Process**

Records disposal is the process by which PLL Records are either destroyed or retained as PLL Archives. Disposal is a range of processes associated with implementing the records retention, destruction or transfer decisions documented PLL's Records Retention and Disposal Policy. These include:

- a) Immediate destruction
- b) Retention by the work unit for a specified number of years prior to destruction
- c) Transfer to intermediate storage for a specified number of years prior to destruction
- d) Transfer to records services for permanent retention
- e) Transfer by Records Services to PLL's Archives for permanent retention

## **14. Destruction of Documents (Physical Form and Digital Form)**

The Document Destruction Policy identifies the record retention responsibilities of employees, members of the board of directors, and outsiders for maintaining and documenting the storage and destruction of the organization's documents and records.

The organization's Directors, employees and outsiders (independent contractors via agreements with them) are required to honor the following rules:

- a) Paper or electronic documents indicated under the terms for retention in the Clause (7) will be transferred and maintained by concerned department;
- b) All other paper documents and electronic documents will be destroyed or deleted from all individual computers, data bases, networks, and back-up storage after three year;

- c) No paper or electronic documents will be destroyed or deleted if pertinent to any ongoing or anticipated investigation or proceeding or litigation ; and
- d) No paper or electronic documents will be destroyed or deleted as required to comply with auditing standards
- e) PLL records should be destroyed in accordance with Data Retention Policy or departmental retention schedules.
  - a. Authorized personnel shall only have access to files and storage closets
  - b. The destruction date should be clearly marked on all records that are in storage. All file boxes should contain complete lists of their contents in a visible spot on the outside of the box so it is easily identifiable.
  - c. All documents shall be destroyed under the supervision of employees , rank not less than a Manager and confidential/ sensitive documents shall be destroyed under a supervision of a Chief Manager .
  - d. All documents in Digital Form shall be destroyed in accordance with IT Policy of PLL.

#### **15. Loss of information**

**Users must notify the asset owner and the IT Service Desk immediately if 'internal', 'confidential/sensitive' or 'restricted' information:**

- a) Is lost or disclosed to unauthorized parties
- b) Is suspected of being lost or disclosed to unauthorized parties.

#### **16. Enforcement**

Whoever knowingly/ corruptly alters, copies, destroys, mutilates, conceals a record, document, or other object, or attempts to do so, with the intent to impair the object's integrity or availability for use in an official process; falsifies or makes a false entry in any record, document, or tangible object through negligence, willfulness or gross negligence with the intent to take advantage, impede, obstruct, or influence the process shall be liable for serious disciplinary action, including suspension or termination of employment. It may also result in civil and/or criminal prosecution and penalties.

\*\*\*\*\*