Munjal Kiriu Industries Private Limited

Data Retention Policy

Confidentiality Agreement

Mr. K. Saravanan (MD)	Ravee Kant Sharma		Controlled copy STAMP	Revision detail	
Approved by	Checked by	Prepared by		REV.NO. 01	REV.DATE 02/07/2025

Document Control

DOCUMENT REVISION HISTORY				
Ver	**Date**	**Editor**	**Nature of Revision**	**Previous Correspondence**
1.0	**02/07/2025**	**Ravee Kant Sharma**	**First Release**	**NA**

Document Reviewers

Reviewed by	**Approved by**	**Final Comments**
Vijay Pal Singh	**Mr. K. Saravanan (MD)**	**Initial Document**

Table of Contents

1. Background

Record management refers to the entire 'lifecycle' of records, from the point of creation, to their use, and until eventual disposal. MUNJAL KIRIU also creates and maintains various records (customer as well as business records) as a part of its regular business operations in various forms (soft or hard copies).

Records tend to grow over time in line with the growth of the MUNJAL KIRIU ’s business, and in the absence of a record retention framework, the cost incurred by the MUNJAL KIRIU to maintain and store the same is significant. It is important that all records are retained as long as such records are required for the MUNJAL KIRIU to meet its business, legal, or applicable regulatory requirements, and also allow it to fulfil obligations towards its customers. Hence, it is important to put in place a record retention policy that would govern the period for which records must be retained, how such records are retained, and finally, disposed of at the end of their retention period.

2. Purpose

The MUNJAL KIRIU shall put in place a well-defined framework for the management of records to ensure that:

- Records are at minimum retained for the period required by applicable legal, regulatory, and business requirements;
- Records are stored appropriately, giving due importance to their sensitivity and confidentiality;
- Records no longer necessary for legal or business reasons are destroyed in an orderly way to prevent any unauthorized disclosure;
- Records that may be relevant to ongoing litigation and/or regulatory investigation are immediately identified and safeguarded from routine record disposal requirements.

3. Scope

The record retention policy shall apply to MUNJAL KIRIU ’s business records and does not apply to personal or non-business records. All business records, wherever they may be stored, whether maintained in an individual’s workplace, computer applications, or vendor premises, or off-site locations, irrespective of their format, are subject to the requirements of this policy.

4. Policy statement

The MUNJAL KIRIU shall establish a framework towards identifying business records, defining the period for which the same needs to be retained in line with business requirements as well as applicable legal and regulatory requirements, provide and implement relevant archival and retention solutions, and provide for safe disposal of such records post retention period.

5. Policy Requirements

The policy mandates all functions to formulate retention schedules for their set of records, storage, and eventual destruction of their business records post the retention period. Mentioned below are the policy requirements segregated as per the areas of identification, storage, and destruction. All records, including Customer Records, shall be complete and accurate.

6. Identification of business records:

Functions shall identify all business records that are created/ generated within their function. Business records shall typically include Customer Records and reports, especially those that are placed before any forum and/or regulator, policies and procedures, intra and inter departmental MIS, actuarial models, contracts, etc.

Further concerning all outsourcing arrangements undertaken, functions shall ensure that requisite documentation created/ generated under complying with the stipulated requirements is identified & maintained

Records can thus be divided into three broad categories:

- Records legally required to be retained for prescribed periods as specified by applicable legislation, e.g., Customer records, legal data, audit reports, etc.
- Records required for business operations, e.g., policies, procedures & actuarial or financial models
- Records generated in the course of business

7. Record retention schedule

All functions shall develop a retention schedule for the identified business records within their function, which shall have the following areas of information:

7.1 General records information

The record retention schedule shall capture necessary details pertaining to the records, i.e., record name, description, category, type, location, and Information asset rating.

7.2 Record retention information

Record retention trigger/event shall be identified and retention period defined for all business records in the retention schedule, giving necessary reference to applicable legal and regulatory or business requirements. Customer Records will also be maintained in electronic form, irrespective of maintenance in any other form.

7.3 Record retention trigger

The retention trigger is the event that starts the retention period.

8. Responsibilities

- **Employees**: Responsible for adhering to this policy and managing documents in their care.
- **Department Heads:** Ensure compliance with the retention periods and secure disposal of documents.

- **IT Department:** Provide secure storage solutions and oversee the secure disposal of electronic records.
- **HR Department:** Manage the retention and disposal of employee-related documents.
- **GA Department:** Manage the retention and disposal of general administrative documents.
- **CISO:** Review the record retention schedules at least once a year and update as necessary

9. Appropriate storage of retained information

Records which have been archived should be stored using an appropriate archival solution at an appropriate location, giving due importance to their retention period as specified in the retention schedule and the frequency with which access will be required to the record. Business records that are no longer required in the live/ production environment are kept in a compressed format in storage devices, such as a disk or magnetic tape, till the end of their retention period.

Also, MUNJAL KIRIU 's critical data /information will also be available at the Disaster Recovery site in line with MUNJAL KIRIU 's Business Continuity policy-related requirements.

Records shall be organized in a manner as required for business use and facilitate retrieval to support policyholder servicing and ensure compliance with applicable laws as applicable from time to time.

About the maintenance of records in electronic form, the following requirements shall be adhered to:

- **Processing and electronic maintenance of records:** All records about policies issued and claims made shall be held in data centers located and maintained in India only.
- **Privacy and security of Client data:** Information & Cyber Security considerations, including the degree of security required for file storage & archival, shall depend on the sensitivity and nature of records as prescribed by MUNJAL KIRIU ’s Information & Cyber Security framework.
- **Handling Virus, vulnerability issues:** The MUNJAL KIRIU 's Information & Cyber Security framework shall govern the deployment of a suitable anti-virus solution towards handling of viruses and controls towards mitigating security vulnerabilities noted.
- **Security of hardware and software:** Security of hardware and software shall be subject to requirements emanating from the Information & Cyber Security Policy of the MUNJAL KIRIU.
- **Backups, Disaster Recovery, and Business Continuity, and Data Archival:** The MUNJAL KIRIU 's Information & Cyber Security policy shall govern the backup requirements, whereas the Business Continuity Management policy shall govern the Business Continuity/Disaster Recovery requirements.

10. Retention Periods

10.1 Information Technology (IT)

- **System Logs**: Retain for 1 year, or for a period equivalent to comply with cybersecurity monitoring requirements and internal audits.
- **Backup Tapes**: Retain for 6 months, or for a period equivalent to ensure data recovery capabilities while balancing storage costs.
- **Software Licenses**: Retain for the duration of the license period plus 1 year, or for a period equivalent to comply with software agreements and for audit purposes.
- **Incident Reports**: Retain for 3 years, or for a period equivalent to analyze incident trends and comply with regulatory requirements.
- **System Development Documents**: Retain for the life of the system plus 2 years, or for a period equivalent to support system maintenance and upgrades.
- **Access Control Records**: Retain for 1 year, or for a period equivalent to comply with security audit requirements and incident investigations.
- **Audit Logs**: All audit logs shall be stored for at least a period of 6 months, and critical logs as per the compliance requirement.

10.2 Human Resources (HR)

- **Employee Records**: Retain for the duration of employment plus 6 years, or for a period equivalent to comply with Income Tax Act and labour laws, and for reference in future employment disputes.
- **Payroll Records**: Retain for 7 years, or for a period equivalent to comply with tax and labour laws.
- **Recruitment Records**: Retain for 1 year for unsuccessful candidates; duration of employment plus 6 years for successful candidates, or for a period equivalent to comply with legal requirements and for reference in potential employment disputes.
- **Training Records**: Retain for 3 years, or for a period equivalent to track employee development and for compliance with training regulations.
- **Performance Reviews**: Retain for 3 years, or for a period equivalent to support employee development and for reference in employment decisions.

10.3 General Administration (GA)

- **Contracts and Agreements**: Retain for the duration of the contract plus 6 years, or for a period equivalent to comply with legal and business requirements, and for potential dispute resolution.
- **Financial Records**: Retain for 8 years, or for a period equivalent to comply with the Companies Act, Income Tax Act, and for financial audits.
- **Policies and Procedures**: Retain for the duration they are in effect plus 2 years, or for a period equivalent to ensure compliance with current standards and for historical reference.

10.4 Confidentiality Categories

10.4.1 Confidentiality A: Highly Confidential

Retention Period: Retain for the duration of relevance plus 10 years. To protect the most critical and sensitive information that has a long-term impact on corporate management.

10.4.2 Confidentiality B: Confidential

Retention Period: Retain for the duration of relevance plus 5 years. To protect significant business operations information and ensure compliance with business partner agreements.

10.4.3 Confidentiality C: Company Use

Retention Period: Retain for the duration of relevance plus 3 years. To support internal operations while ensuring the timely disposal of outdated information.

11. Appropriate storage of retained information

Records which have been archived should be stored using an appropriate archival solution at an appropriate location, giving due importance to their retention period as specified in the retention schedule and the frequency with which access will be required to the record. Business records that are no longer required in the live/ production environment are kept in a compressed format in storage devices, such as a disk or magnetic tape, till the end of their retention period.

Also, MUNJAL KIRIU 's critical data /information will also be available at the Disaster Recovery site in line with MUNJAL KIRIU 's Business Continuity policy-related requirements.

Records shall be organized in a manner as required for business use and facilitate retrieval to support policyholder servicing and ensure compliance with applicable laws as applicable from time to time.

With regard to the maintenance of records in electronic form, the following requirements shall be adhered to:

- **Processing and electronic maintenance of records:** All records pertaining to policies issued and claims made shall be held in data centers located and maintained in India only.
- **Privacy and security of Client data:** Information & Cyber Security considerations, including the degree of security required for file storage & archival, shall depend on the sensitivity and nature of records as prescribed by MUNJAL KIRIU ’s Information & Cyber Security framework.
- **Handling Virus, vulnerability issues:** The MUNJAL KIRIU 's Information & Cyber Security framework shall govern the deployment of a suitable anti-virus solution towards handling of viruses and controls towards mitigating security vulnerabilities noted.

- **Security of hardware and software:** Security of hardware and software shall be subject to requirements emanating from the Information & Cyber Security Policy of the MUNJAL KIRIU.
- **Backups, Disaster Recovery, Business Continuity, and Data Archival:** The MUNJAL KIRIU 's Information & Cyber Security policy shall govern the backup requirements, whereas the Business Continuity Management policy shall govern the Business Continuity/Disaster Recovery requirements.

12. Appropriate destruction after retention periods

Records that have completed their retention period shall be securely disposed of, taking into consideration the sensitivity of the information as prescribed by the MUNJAL KIRIU ’s Information & Cyber Security Policy.

12.1 Access to records

The MUNJAL KIRIU shall provide access to records as defined above to the Authority for both onsite and offsite inspections.

12.2 Plan to review the implementation of the requirements pertaining to the maintenance and storage of records

The MUNJAL KIRIU shall ensure that the requirements mandated as a part of this policy are implemented, and the same is reviewed at least annually to ensure adequacy and ongoing effectiveness

13. Exception

Functions shall continue to retain records in excess of their retention schedule only in case of being notified by such requirement from any one of the functions, viz., complaints redressal unit (CRU), Legal & Compliance, Finance, etc., owing to any prevailing legal matters or applicable regulatory requirements.

Wherever, for technical or business reasons, it is not possible to comply with this policy, a time-bound waiver might be requested. The waiver needs to be approved by the functional head, the Chief Risk Officer & Chief Compliance Officer.

14. Non-Compliance

Any violation of this policy must be reported immediately to the corresponding department head & Security & Fraud Risk function.

15. Disposal Method

Records that have completed their retention period shall be securely disposed of to prevent unauthorized disclosure. Secure disposal methods include shredding, incineration, and secure digital deletion.