Safex Group

Data Retention Policy

Suresh
01/04/23

Safex Group.

Data Retention Policy

1. Document Control

S. No.	Type of Information	Document Data
1.	Document Title	Data Retention Policy
2.	Document Code	ITDRP001
3.	Date of Release	01-04-2022
4.	Document Version No.	1.0
5.	Document Owner	Safex Group
6.	Document Author(s)	Suresh Yadav (AVP IT)
7.	Document Approver	Piyush Jindal (Group Director)

Document Update Summary

Version No.	Revision Date	Nature of Changes	Date Approval
1	-		
2			
3			

Suresh
01/04/23

2. Purpose

This policy sets the required retention periods for specified categories of personal data and sets out the minimum standards to be applied when destroying certain information within Safex Group, hereinafter referred as Safex Group.

3. Scope

This policy applies to all business units, processes, and systems in all countries in which Safex Group conducts business and has dealings or other business relationships with third parties.
This Policy applies to all Safex Group's officers, directors, employees, agents, affiliates, contractors, consultants, advisors or service providers that may collect, process, or have access to data (including personal data and/ or sensitive personal data). It is the responsibility of all of the above to familiarize themselves with this policy and ensure adequate compliance with it.

This policy encompasses customer data, Safex Group data, regulatory, statutory and contractual records that are critical for operations of Safex Group. The records can be in both hard and soft forms.

This policy applies to all information used at the Company. Examples of documents includes, but not limited to:

- Emails
- Hard copy documents
- Soft copy documents
- Personnel records
- Information stored on applications used by all business units of Safex Group
- Shared drive
- Cookie identifier, including cached data
- Video and audio
- Data generated by physical access control

4. Objective

To protect the data and records that are critical to Safex Group and its clients. The said data or records will be retained or safeguarded as per this policy.

5. Terms & Definitions

For the purposes of this document, the following terms and definitions apply:

Data	Data is defined as any information in both paper and electronic form created, received and maintained as evidence and information by Safex Group in pursuance of legal obligations or in the transaction of business.
Data owner	A data owner is an individual or entity that holds managerial and financial accountability for a dataset and that has legal ownership rights of a dataset, even if the dataset was collected/ administered by another party.
Archiving	Archiving is the process of moving data that is no longer actively used to a separate data storage device for long-term retention.

Shadow data	Identical copies of the data that are maintained onsite or offsite or in any computer.

6. Policy Statement

Safex Group shall recognise and understand the efficient management of its data and records which are necessary to support its core business functions, to comply with legal, statutory, and regulatory obligations, to ensure the protection of personal data and to enable the effective management of the organisation.

This Policy shall meet the standards and expectations set out by contractual and applicable legal requirements and shall develop to meet the best practices of business records management, with the direct aim of ensuring a robust and structured approach to document control and systems. Effective and adequate data management is necessary to:

- Ensure that business is conducted in a structured, efficient and accountable manner;
- Meet legislative, statutory and regulatory requirements;
- Protect the interests of the organisation and the rights of employees, clients and other stakeholders;
- Protect personal data and the rights of data subjects; &
- Avoid inaccurate or misleading data and minimise the risks to personal data.

6.1. General rules

- Safex Group shall archive, retain and dispose data either owned or managed by Safex Group.
- Data managed by Safex Group's Information Technology ('IT') division shall be archived, retained and disposed of by IT division only after a formal archival/ retention/ disposal request submitted and approved by the data owner and Group Director.
- Archived data shall be retained as per applicable legal, compliance and Safex Group policies and procedures.
- Archived Data shall include the following, but not limited to
  a) E-Mail communications
  b) Business client, agent, and supplier correspondence
  c) Customer data
  d) Employee data
  e) Accounting, finance earnings and tax data
  f) Databases
  g) Supplier and partner information
  h) Contracts
  i) Sales, invoice and billing information
  j) Documents
  k) Spreadsheets
  l) Business and financial reports
  m) Cookie identifier
  n) Other data produced and collected in fulfilling business activities.

6.2. Retention of data containing restricted & sensitive information

Safex Group uses the following guidelines and statutory procedures for data retention.

Archiving: Organizational data, including sensitive information, which are not being used for active organization business, may be archived until retention requirements have been met.

a) Safex Group divisions shall determine the criteria for inactive data status in their areas, based on need for the data and available storage space and other legal requirements.
b) Request for data archiving, shall be approved by the relevant Group Director and then submitted to the IT division for archival.
c) Storage areas for inactive data shall be physically secure and environmentally controlled, to protect the data from unauthorized access and damage or loss from temperature fluctuations, fire, water damage, pests, and other hazards.
d) When appropriate, only primary data shall be archived. The contents of true "Shadow" data shall be destroyed after it has been determined that they contain only duplicates of data maintained elsewhere, and do not contain any original materials.
e) Off-site storage facilities or locations for sensitive data shall be approved by the IT Steering Committee.

6.3. Data Retention Principle

In the event, for any category of records not specifically defined in this Policy and unless otherwise mandated differently by applicable law, the required retention period for such a document shall be deemed to be ten (10) years from the date of creation of the same.

6.4. Legal & statutory records

The legal and regulatory records of Safex Group shall be retained with appropriate protection as per the requirements of the law.

6.5. Customer data & records

- Customer data and records shall be retained as per customer's requirement outlined in the signed contract (Master Service Agreements 'MSA' and/ or Scope of Work 'SOW') or as per any specific requests from the customer. In case of requests from the customer data shall be retained till such time the customer receives them and acknowledges the receipt of the same.
- In case of absence of instruction from customers with respect to data retention period, data must be kept in a form that permits identification for no longer than necessary for the purposes for which the data are collected or processed and should not be kept 'just in case' the business has a need for it in the future.

6.7. Safex Group data

Safex Group data shall be retained and protected as long as they are needed for collection of evidence or statutory and regulatory requirements and functioning of businesses. Such data shall be treated for disposal or retention under approval from the process owner and top management of Safex Group.

6.8. Retention period

- The "Retention Period" begins at the end of the year when the data was sent, published or received and ends at the end of the year of the relevant required Retention Period.

- Any changes to the retention period should be enforced post the approval of the following personnel:
  a) Data owner
  b) Legal & Compliance Team
  c) A.V.P (IT)
  d) Group Director

- In the event, for any category of documents not specifically defined elsewhere in this policy (and in particular within the Data Retention Schedule) and unless otherwise mandated differently by applicable law.
- A schedule describing the data and the official retention period shall be mentioned in the archival/ retention/ disposal request submitted to the IT division.
- The retention period for the data should be reviewed on an annual basis by the data owner.
- All functions shall periodically review their data retention schedule to determine any special circumstances that necessitate changes in the retention period.
- As an exemption, retention periods within Data Retention Schedule can be prolonged in cases such as:
  a) Ongoing investigations from member states authorities, if there is a chance that records of personal data are needed by the Company to prove compliance with any legal requirements.
  b) When exercising legal rights in cases of lawsuits or similar court proceedings recognized under local law.

6.9. Data Retention Schedule

Record category	**Person responsible for storage**	**Access to records restricted to**	**Retention period**	**Approver**
Supplier related records: - Contracts & related correspondences, etc	Legal & Finance Head	Legal, Finance & Project Managers	As per Company Requirement.	**Group Director**
HR records: - Employment contracts; - Attendance records; - Performance evaluation etc.	Human Resource Team	HR team members as per role / responsibility assigned	As per Company Requirement	**Group Director**
Customer related records: - Contracts & related correspondences, etc.	Legal & Finance Head	Legal, Finance and Project Managers	As per Company Requirement	**Group Director**
Financial records: - Annual reports; - Budgets & Plans; - Financial records, etc	Finance Department	Finance Team members as per role / responsibility assigned	As per Company Requirement	**Group Director**
Tax related records: - Tax returns; - Receipts, correspondence, etc.	Finance Department	Finance Team members as per role /	As per Company Requirement	**Group Director**

		responsibility assigned		

6.10. Retention of Personal Data / Information:

- This Section sets out the data retention policies and procedure of the Safex Group, which are designed to help ensure compliance with legal obligations in relation to the retention and deletion of personal information;
- Personal information that is processed by the Company for any purpose shall not be kept for longer than is necessary for that purpose.
- The Company will retain data/records including electronic (documents, email, Multimedia etc.) and physical storage (paper data, documents etc.) containing personal data:
  a) to the extent that the Company is required to do so by law;
  b) if the Company believes that the documents may be relevant to any ongoing or prospective legal proceedings;
  c) to establish, exercise or defend the Company's legal rights; and
  d) if explicit consent is given by the data subject.
- Safex Group understands that the retention of personal data is subject to the data subject's withdrawal of consent & exercise of right to have his / her personal data removed under GDPR.

6.11. Safeguarding of Personal Data during Retention period:

Safex Group recognises the need to protect the personal data at all times, including during the retention period and in this relation Safex Group has adopted various technical and organisational data security measures to protect the security of personal data.

Technical measures in place for security of personal data include:

- All emails containing personal data shall be treated with utmost confidentiality.
- The personal data from emails shall be stored in a secure location (Folder) which is access controlled with respect to need to know principle and password protected.
- Personal data shall only be transmitted over secure networks;
- Personal data contained in the body of an email, whether sent or received, shall be copied from the body of that email and stored securely. The email itself and associated temporary files shall be deleted;
- Where personal data is to be transferred in hardcopy form, it shall be passed directly to the recipient or sent marked as "confidential";
- All hardcopies of personal data, along with any electronic copies stored on physical media shall be stored securely;
- No software may be installed on any Safex Group -owned computer or device without approval of the IT head and Computers used to view personal data shall always be locked before being left unattended.

Organisational measures in place for security of personal data include:

- All employees and other parties working on behalf of Safex Group shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR while handling personal data;

- Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company;
- All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised; and
- The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.

6.12. Data disposal

- The proper destruction of data is essential to creating a credible data management program. Data containing restricted/ sensitive information shall only be destroyed in the ordinary course of business; no data that are currently involved in, or have open investigations, audits, or litigation pending shall be destroyed or otherwise discarded.
- No primary data of any type belonging to Safex Group may be destroyed until they have met retention requirements established by Safex Group policies and procedures.
- When retention requirements have been met, data shall be either immediately destroyed or placed in secure locations in a controlled manner.
- The authorized methods of destruction for non-electronic data are burning where authorized or shredding.
- Using the certified data destruction software, secure data destruction process shall be used for safe destruction of data. Data destruction software does erase the data and each data destruction program utilizes one or more data sanitization methods that can permanently overwrite the information on the drive.

7. Responsibilities

- The A.V.P (I.T) is responsible to review and approve the policy and to ensure that it reflects the current requirements of Safex Group.
- The H.R is responsible for development, implementation, maintenance and enforcement of the policy.
- The Internal Audit Team is responsible for conducting regular audits to ensure compliance to this policy.
- Employees and non-employees of Safex Group are responsible and/or accountable to ensure adherence to the terms of this policy in the course of their job duties.
- Asst. Managers should be informed with immediate effect for any changes in the retention policy by the company as well as should be closely involved in the process of data destruction and disposal.

8. Enforcement

8.1. Policy violations

- Violation of the policy will result in corrective action from the management. Disciplinary action will be consistent with the severity of the incident, as determined by the investigation, and may include, but not limited to:
  a) Loss of access privileges to information assets
  b) Termination of employment or contract
  c) Other actions deemed appropriate by management, Human Resource team, Legal team and their relevant policies.
  d) Violation or deviation of the policy shall be reported to the A.V.P (I.T) and a security incident record has to be created for the further investigation of the incident.

8.2. Policy exceptions

- Any exceptions to this policy have to be formally approved by the Director. All the exceptions shall be tracked by Safex Group's IT team in IT exceptions request tracker. The exception request shall follow the below mentioned approval matrix.

First level	Asst. Manager (I.T)
Second level	Sr. Manager/A.V.P (I.T)
Third level	Group Director

9. Document References

Document/ Form No.	Title

01/04/23