Data Retention and Disposal Policy

FitZone Health & Wellness Pvt. Ltd.

1. Purpose/Objective

The purpose of this Data Retention and Disposal Policy is to establish guidelines for the retention, storage, and secure disposal of business records, member personal data, and information assets throughout their lifecycle. This policy aims to:

- Ensure FitZone retains data only as long as necessary for legitimate business, legal, or regulatory purposes
- Comply with Digital Personal Data Protection Act (DPDP Act) 2023 data minimization and storage limitation principles
- Meet legal and regulatory retention requirements while minimizing unnecessary data exposure
- Establish consistent procedures for secure deletion and destruction of data across all systems and media
- Reduce organizational risk by eliminating outdated, redundant, or obsolete data
- Support business operations by ensuring critical records are preserved and accessible
- Protect member privacy by preventing indefinite retention of personal and health information

2. Scope

This policy applies to:

- **Data Types:**
    - Member personal data (name, contact information, date of birth, identification documents)

    - Member health information (medical history, fitness assessments, body metrics, health goals)
    - Payment and financial data (transaction records, payment card tokens, billing information)
    - Employee records (personal information, employment contracts, salary, performance reviews)
    - Business records (contracts, agreements, financial statements, audit reports, correspondence)
    - IT system data (logs, backups, configurations, security incident records)
    - Marketing data (consent records, communication preferences, campaign data)
    - Video surveillance footage (CCTV recordings)
- **Storage Media:**
    - Electronic data: Databases, file servers, cloud storage, email systems, backup media
    - Physical records: Paper documents, printed reports, contracts, medical forms
    - Portable media: USB drives, external hard drives, CDs/DVDs, mobile devices
    - Archived data: Offsite backups, archival storage systems
- **Personnel:** All employees, contractors, and third parties handling FitZone data
- **Locations:** All FitZone facilities across Mumbai, Pune, and Bangalore

---

3. Policy Statement

3.1 Data Retention Principles

3.1.1 Storage Limitation

- Personal data shall be retained only for as long as necessary to fulfill the purposes for which it was collected
- Data shall not be stored indefinitely without documented business or legal justification

- Retention periods shall be clearly defined and documented for each data category

3.1.2 Data Minimization

- Only necessary data shall be collected and retained
- Excessive or redundant copies of data shall be avoided
- Data shall be reviewed periodically and purged when no longer needed

3.1.3 Lawful Basis for Retention

- Data retention shall comply with:
  - Legal and regulatory requirements (DPDP Act 2023, Income Tax Act, Companies Act)
  - Contractual obligations (member agreements, vendor contracts)
  - Legitimate business interests (dispute resolution, financial audits)
  - Member consent (where applicable)

3.1.4 Accountability

- Each business unit is responsible for managing retention and disposal of data under its control
- Data owners shall ensure compliance with retention schedules
- IT Department shall implement technical controls supporting retention policies

---

4. Data Classification and Retention Schedules

4.1 Member Data

Data Category	Description	Retention Period	Legal/Business Justification	Disposal Method
Member Registration Data	Name, contact information, date of birth, address, emergency contact	**Active membership + 3 years**	Contract management, legal claims limitation period (3 years per Limitation Act)	Secure deletion from database; physical forms shredded
Member Health Information	Medical history, fitness	**Active membership +**	Medical-legal requirement;	Secure deletion with audit trail;

Data Category	Description	Retention Period	Legal/Business Justification	Disposal Method
	assessments, body metrics, health goals, injury records	**7 years**	potential liability claims (longer limitation for medical matters)	encrypted backup deletion
Payment & Billing Records	Transaction history, invoices, payment methods (tokenized), subscription records	**7 years from last transaction**	Income Tax Act 1961 (retain for 6 years after relevant assessment year); PCI-DSS compliance	Secure deletion; paper records shredded
Membership Agreements	Signed contracts, terms acceptance, liability waivers	**7 years after membership ends**	Contract law; statute of limitations for breach of contract claims	Physical contracts shredded; electronic copies securely deleted
Identification Documents	PAN card, Aadhaar photocopies (if collected)	**Delete immediately after verification** OR **Active membership + 1 year** (if business need documented)	DPDP Act data minimization principle; should not retain longer than necessary	Secure shredding of physical copies; secure deletion of digital copies
Member Communication History	Emails, SMS, WhatsApp communication, complaint records	**Active membership + 2 years**	Customer service, dispute resolution	Email purge; message logs deleted
Member Consent Records	Marketing consent, data processing consent, communication preferences	**5 years after consent withdrawn or membership ends**	DPDP Act requirement to demonstrate lawful processing	Secure deletion with audit log
Video Surveillance	CCTV footage of gym floors,	**30 days** (unless related to	Security monitoring;	Automatic overwrite after

Data Category	Description	Retention Period	Legal/Business Justification	Disposal Method
(Member Areas)	common areas	incident)	privacy considerations	30 days; incident-related footage retained per incident retention policy

4.2 Employee Data

Data Category	Description	Retention Period	Legal/Business Justification	Disposal Method
Employment Applications	Resumes, interview notes (not hired)	**1 year after recruitment process**	Anti-discrimination compliance; potential legal claims	Shredded or securely deleted
Employee Personal Information	Name, address, contact, identification, family details	**7 years after employment ends**	Labor laws, tax requirements, potential employment disputes	Secure deletion; physical files shredded
Employment Contracts & Agreements	Offer letters, contracts, NDAs, non-compete agreements	**7 years after employment ends**	Contract law, litigation defense	Physical documents shredded; digital copies deleted
Salary & Payroll Records	Salary slips, tax deductions, PF contributions, bank details	**Permanent (minimum 10 years)**	Income Tax Act, EPF Act, labor laws, audit requirements	Archived securely; not deleted without legal review
Performance Reviews	Appraisals, disciplinary records, warnings	**7 years after employment ends**	Employment litigation defense, performance documentation	Secure deletion; paper records shredded
Training Records	Security awareness training, certifications, skill development	**Duration of employment + 3 years**	ISO 27001 competence requirements; audit trail	Archived then deleted

Data Category	Description	Retention Period	Legal/Business Justification	Disposal Method
Time & Attendance Records	Login/logout times, leave records, overtime	**7 years**	Labor law compliance, wage disputes	Secure deletion after retention period
Termination Records	Resignation letters, exit interviews, final settlement	**7 years after termination**	Employment disputes, severance litigation	Secure deletion; physical records shredded

4.3 Business & Financial Records

Data Category	Description	Retention Period	Legal/Business Justification	Disposal Method
Financial Statements	Annual accounts, balance sheets, P&L statements	**Permanent (minimum 8 years)**	Companies Act 2013, Income Tax Act, audit requirements	Archived securely; permanent retention recommended
Tax Records	Income tax returns, GST returns, TDS records, tax assessments	**8 years after relevant assessment year**	Income Tax Act 1961 (Section 34, 153)	Secure deletion; physical copies shredded
Invoices & Purchase Orders	Vendor invoices, customer invoices, purchase orders	**7 years**	GST Act, Income Tax Act, audit trail	Archived then securely deleted
Bank Statements & Reconciliations	Bank statements, payment reconciliations	**7 years**	Financial audit, tax compliance	Archived then securely deleted
Vendor Contracts & Agreements	Service agreements, vendor contracts, DPAs	**7 years after contract expires**	Contract law, dispute resolution, audit requirements	Physical contracts shredded; electronic deleted
Audit Reports	Internal audit reports,	**10 years**	Corporate governance,	Archived securely

Data Category	Description	Retention Period	Legal/Business Justification	Disposal Method
	external audit reports, compliance assessments		regulatory inspections, litigation defense	
Board Minutes & Resolutions	Board meeting minutes, shareholder resolutions, governance records	**Permanent**	Companies Act 2013, corporate governance	Permanent archival; never disposed
Insurance Policies & Claims	Insurance policies, claim records, liability coverage	**10 years after policy expires**	Legal claims, liability defense	Archived then deleted
Correspondence	General business emails, letters, memos	**2 years** (unless part of contract/dispute)	Operational needs; purge to reduce data volume	Email purge; archived important correspondence

4.4 IT & Security Records

Data Category	Description	Retention Period	Legal/Business Justification	Disposal Method
Access Logs & Audit Trails	System access logs, authentication logs, database audit logs	**1 year (standard); 3 years (sensitive systems)**	ISO 27001 monitoring requirements, incident investigation	Automated log rotation and deletion
Security Incident Records	Incident reports, investigation findings, remediation actions	**7 years**	Legal evidence, regulatory reporting, lessons learned	Archived securely; deleted after retention period
Vulnerability Scan Reports	Vulnerability assessments, penetration test reports	**3 years**	Compliance audit trail, risk management	Archived then deleted
System Backups (Operational)	Daily/weekly incremental backups	**90 days**	Business continuity,	Automatic rotation and overwrite

Data Category	Description	Retention Period	Legal/Business Justification	Disposal Method
			operational recovery	
System Backups (Archival)	Monthly/quarterly full backups	**7 years**	Data recovery, legal hold requirements	Encrypted archival; deleted after retention
CCTV Footage (Incident-Related)	Surveillance footage related to security incidents, theft, accidents	**3 years**	Legal evidence, insurance claims, criminal investigations	Archived securely; deleted after investigation concludes
Network Configuration	Network diagrams, device configurations, change logs	**Current version + 3 years of historical changes**	Operational continuity, audit trail, compliance	Old configs deleted; current configs retained
Software Licenses	License agreements, proof of purchase, activation keys	**Duration of software use + 3 years**	Audit compliance, vendor audits	Deleted after software decommissioned and retention period expires

4.5