"DATA PROTECTION & RETENTION POLICY"

JAN VIKAS SAMITI

Murdaha, Christnagar PO | Varanasi – 221003 | Uttar Pradesh, India.

TABLE OF CONTENTS

1: THE ORGANIZATION 3

2: INTRODUCTION & BACKGROUND 3

2.1. Introduction 3

2.2. Aims & Objectives 3

3: TYPES AND SOURCES OF DATA 4

3.1. Data related to beneficiaries: 4

3.2. Data related to Operational/Administrative/Financial &HR 4

4: STORING DATA SECURELY 4

5: DATA PROTECTION BREACH 5

6: STAFF ROLE & RESPONSIBILITIES; 5

7: DATA RETENTION POLICIES AND TIME FRAME 5

8: AMENDMENT TO POLICY 7

1: THE ORGANIZATION

Jan Vikas Samiti (JVS) is a charitable society registered in 1997 under Societies Registration Act, 1860 From its inception it has been rendering services for the empowerment of the marginalized groups of the society including women, children, scheduled caste and persons with disabilities.

Vision
To build an inclusive humane society based on the values of Equality, Justice, Freedom.

Mission
Empowerment of the marginalized people of the society, including women, children, scheduled caste and persons with disabilities through a process of awareness, organization for collective actions and advocacy for raising Socio- Political, Educational, Economic, Health Status and Promotion of Environment.

2: INTRODUCTION & BACKGROUND

2.1. Introduction

Jan Vikas Samiti (hereafter referred to as "JVS") is committed to protecting the rights and freedom of our data subjects, and safely and securely processing their data in accordance with all of our legal obligations, including compliance with applicable Data Protection rules and regulations. We process both personal and sensitive data about our employees, beneficiaries, and other data related to the operation, administration and financial affairs of the organization.

JVS works with women, children and persons with disabilities through various developmental projects and programs. While implementing and coordinating these programs JVS do collect personal data of these target groups for the execution of activities, training and other managerial purpose.

This policy sets out how we seek to protect these data and ensure that our employees understand the rules governing their use of the personal data to which they have access during the course of their work on behalf of JVS. The policy also will describe the data storage and retention policies for various types of organizational data.

2.2. Aims & Objectives

This policy is a security policy that aims to design, implement, guide, monitor and manage security over JVS's data. It primarily aims at securing and protecting logical data stored, consumed, and managed by the organization. It also aims to store and retain these data for the future access, references and also compliances. JVS will develop various methods, timeline for storing these kinds of data for future access depending on ones requirement.

3: TYPES AND SOURCES OF DATA

3.1. Data related to beneficiaries:

JVS as a developmental organization collects and records various data and information regarding the area of operation, target groups, targeted beneficiaries, communities etc. for the program planning, development and execution and reporting purposes. All these data related to the project and program purpose collected by JVS will be maintained at the head office of JVS. These documents will be in the custody of the respective program heads until such respective project/program come to an end. All the data related to the closed projects will be stored in the data store room which is under lock and key. These documents will be at the custody of the Executive Director of the Organization or any other delegated person. Access to these documents will be done only with the permission from the Executive Director. These documents will only be used for reporting purposes, filing compliances to the donor agencies and government authorities in need. The Executive Director or the delegated person will make sure that these data are not used for any personal benefit and advantages.

3.2. Data related to Operational/Administrative/Financial &HR

As part of day to day operation and managerial purpose JVS would maintain and execute various data related to its operations, financials, administrative and Human Resource for better functioning, transparency and accountability. These documents will be handled by the departmental heads and other persons delegated by the Executive Director. The departmental head will make sure that the related documents are protected and not misused by self or by any other departmental staff.

4: STORING DATA SECURELY

- In cases when data is stored on printed paper, it would be kept in a secure place where unauthorized personnel cannot access it
- Printed data will be shredded when it is no longer needed
- Data stored on a computer will be protected by strong passwords that are changed regularly.
- Data stored on hard disks or memory sticks will be locked away securely when they are not being used
- The Executive Director must approve any cloud service used to store data.
- Financial and other administrative Data will be regularly backed up and be stored in external storage disk/devises and such devise will be kept under lock and key I the custody of the respective authority.
- Data should never be saved directly to mobile devices such as personal laptops, personal tablets or smartphones.

5: DATA PROTECTION BREACH

A protection data breach is described as a breach of data security by any staff members leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to data transmitted, stored or otherwise processed. In the event of such data breach occurring by any staff, the management will take appropriate disciplinary action as per the policies and procedures of HR & Data protection policy of JVS.

6: STAFF ROLE & RESPONSIBILITIES;

- The only people able to access data covered by this policy are those who need it for their work.
- Data will not be shared informally.
- When access to confidential information is required, employees can request from their line managers/HODs.
- Employees will keep all data secure, by taking sensible precautions.
- For Financial data in particular, strong passwords will be used and they should not be shared to un-authorized persons.
- Personal data of beneficiaries will not be disclosed to unauthorized people, either within the organization or externally.
- Data will be regularly reviewed and updated if it is found to be out of date, or no longer required, it will be deleted and disposed of.
- Employees should request help from their line manager or the authorized person for data protection if they are unsure about any aspect of data protection.
- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Employees should not save copies of personal data to their own computers/smartphone/or any other external storage devices.

7: DATA RETENTION POLICIES AND TIME FRAME

JVS will not retain personal data related to the beneficiaries for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but will be determined in a manner consistent with the use of such data. Other important data and documents related to all other affairs of the organization will be retained by following the below policies and time frame.

Document/data Retention policies and time frame.

Documents	Time Frame
Books of accounts; payable & Receivable ledgers, cash book, bank book and schedules	Permanently
Bills/Vouchers	12 years
Audit reports of accountants	Permanently

Bank statements	12 years
Checks (canceled, with exception below)	5 years
Checks (canceled, for important payments, i.e., taxes, purchase of property, special contracts, etc. [checks should be filed with the papers pertaining to the underlying transaction])	Permanently
Contracts and leases (expired)	10 years
Contracts and leases still in effect	Permanently
Correspondence, general	2 years
Correspondence (legal and important matters)	Permanently
Depreciation schedules	Permanently
Duplicate deposit slips	3 years
Employee personnel records including appointment and contracts (after termination)	7 years
Project/Program Financial statements (end-of-projects), after completion.	7 Years
All Insurance policies (expired)	2 years
Insurance records, current accident reports, Medi-claims, policies, etc.	Permanently
Program/Project Progress Reports	7 years
Bills/Invoices of fixed assets	Permanently
Receipts books	Permanently
Minute books of Board of Directors, including bylaws and Articles of Association	Permanently
Payroll records, salary register, performance appraisal etc.	10 years
Purchase orders	10 years
Income Tax Returns of the organization	Permanently
TDS and other tax Returns	Permanently
Foreign Contribution related returns, intimations, approvals,	Permanently
PF & ESI paid Records	Permanently
Research Documents	Permanently
Survey and mapping documents	3 Years

Individual information of beneficiaries of projects/ programs	10 years
Papers of Land, Building, and other immovable properties	Permanently
Digital version of accounts and financial information	Permanently
Case studies, researches, documentaries etc.	Permanently
Third party agreements and contracts (other than lease)	Permanently

8: AMENDMENT TO POLICY

This policy may be amended from time to time as per the need and demand by the programs and managerial affairs of the organization.

JAN VIKAS SAMITI
CHRISTNAGAR, VARANASI