IT and Data Protection Policy

Sujagriti Samaj Sevi Sanstha
Morena, Madhya Pradesh

1. Purpose
The IT and Data Protection Policy outlines Sujagriti Samaj Sevi Sanstha's approach to managing and protecting data and sensitive information. It also defines the use of IT systems and data management practices to ensure compliance with applicable laws.

2. Scope
This policy applies to all employees, contractors, consultants, volunteers, fellows, and interns who access or use Sujagriti's IT systems and handle personal data or confidential organisational information.

3. Definitions
- Personal Data: Information related to an identified or identifiable individual, such as name, contact details, or IP address.
- Sensitive Data: Information revealing race, ethnicity, political opinions, religious beliefs, health data, etc.
- Data Subject: The individual to whom the personal data relates.
- Data Controller: The entity determining the purpose and means of processing personal data.
- Data Processor: The entity processing data on behalf of the Data Controller.

4. IT Systems Usage
All employees must:
- Use organization-provided devices only for work-related activities.
- Avoid unauthorized installation of software or alteration of hardware.
- Refrain from sharing login credentials.

5. Data Protection Principles
Sujagriti adheres to the following principles:
- Lawfulness, Fairness, and Transparency
- Data Minimization
- Accuracy
- Storage Limitation
- Confidentiality and Integrity
- Accountability

6. Data Subject Rights
Data Subjects have the right to:
- Access their personal data.
- Request correction of inaccurate or incomplete data.
- Request deletion of their data under certain conditions.
- Restrict data processing.

- Port data for their own use across services.
- Object to data processing in certain scenarios.

7. Data Breach Reporting
In case of a data breach, Sujagriti will:
- Inform affected individuals if their data is at risk.
- Document the breach and remediation actions.

8. IT Security Measures
Sujagriti implements the following IT security controls:
- Access Control
- Firewalls and Antivirus Software
- Secure Data Backups
- Network Security Monitoring

9. Employee Responsibilities
Employees must:
- Follow IT and data protection guidelines.
- Report any suspected breaches to the reporting officer or the Policy Steering and Compliance Committee.
- Keep systems up-to-date by applying official patches and updates.

10. Training and Awareness
All employees will undergo orientation and receive training to understand their responsibilities under this policy.

11. Third-Party Access and Data Sharing
Third parties accessing Sujagriti's systems or data must:
- Comply with this policy.
- Sign data processing agreements.
- Ensure adequate security is in place.

12. Data Retention and Disposal
Data will be retained only as long as necessary for its intended purpose or as required by law. Secure disposal will be ensured once data is no longer needed.

13. Monitoring and Review
This policy will be reviewed regularly by the Policy Steering and Compliance Committee and the Director. Any updates will be communicated to all staff and stakeholders.

Approved by:
Zakir Hussain, President

Name,...........................
Head of the Organization
President
Sujagrati Samaj Sevi Sanst
Morena (M.P.)