IT Security Policy
Siyaram Silk Mills Ltd.
Data Security & Cryptography Policy

Version:	1st Reviewed Version
Approving Authority:	ESG Committee
Approval date:	30/03/2023
Effective date:	N.A.
Review Period:	On 6 Months interval or in case of any change in IT System
Review Date:	30/03/2023
Consultation via:	Dr CBS Cyber Security Services LLP, Jaipur
References:	ISO 27001:2013, Schedule II- IT Security Guidelines IT Act 2000

Data Security Policy

1. **Introduction:**
   The data protection policy ensures that the organization complies with data protection law and follows good practice, protects the rights of staff, customers and partners and protects itself from the risks of a data breach.
2. **Purpose:**
   The purpose of this policy to ensure that organization data must:

   2.1 Be processed fairly and lawfully

   2.2 Be obtained only for specific, lawful purposes

   2.3 Be adequate, relevant and not excessive
   2.4. Be accurate and kept up to date
   2.5. Not be held for any longer than necessary
   2.6. Processed in accordance with the rights of data subjects
   2.7. Be protected in appropriate ways
   2.8. Not be transferred outside company premises unless IT Team, Management or any other authorized person ensures an adequate level of protection

3. **Scope:**

   This policy applies to all employees who are accessing organization data and information.

4. **Policy:**

SIYARAM SILK MILLS LIMITED MUMBAI

4.1 The IT manager is responsible for:

4.1.1 Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

4.1.2 Performing regular checks and scans to ensure data stored on various computer resources.

4.1.3 Regularly update the existing IT Security System to ensure confidentiality, integrity and availability of organization data and information.

4.1.4 License management of various software used in organization.

4.1.5 Evaluating data security issues in data stored at third-party services (Cloud services, data centers, servers etc.).

4.1.6 Check and monitor logs on various network devices like firewall, servers, Intrusion detection system (IDS), Intrusion Prevention System (IPS), Routers, CCTV etc.

4.1.7 Evaluating the possible data leakage points through internal audits in existing IT infrastructure on regular interval.

4.1.8 Performing third party IT Security Audit to ensure about reasonable security practices and procedures on regular interval.

4.2 **The Business Development Team is responsible for:**

4.2.1 Approving any data protection statements/ disclaimer attached to communications such as emails and letters.

4.2.2 Where necessary, working with other IT team and other staff members to ensure marketing initiatives abide by data protection principles.

4.2.3 Social media guidelines as per social media policy to employees for promotion of organization with data security principles.

4.3 The Account Department responsible for:

4.3.1 To follow Best Security practices for e-banking.

4.3.2 Reasonable security practices and procedures to handle personal sensitive data of employees like financial information such as bank account or credit card or debit card or other payment instrument details.

4.4 The HR Department responsible for:

4.4.1 To add data security measures in HR policy and employee guidelines for Manuals.

4.4.2 Reasonable security practices and procedures to handle personal sensitive data of employees like: Financial Information such as Bank Account or credit card or debit card or other payment instrument details; Physical, physiological and mental health condition; Sexual Orientation; Medical records and history; Biometric Information; Any other details for processing, stored or processed under lawful contract or otherwise.

4.5 The Admin Department responsible for:

4.5.1 To handle and prepare for any disaster/ emergency like fire

SIYARAM SILK MILLS LIMITED * MUMBAI

4.5.2 Assure physical security measure like locks, biometric/ RFID based entry, CCTV Surveillance, Alarm systems, uninterrupted power supply system, Air conditioning system, etc.

4.5.3 Periodic testing, inspection and maintenance of physical security equipments.

4.5.4 Training of employees to make them aware about physical security aspects.

4.6 General staff guidelines

4.6.1 The data accessibility must be made only to the employees concerned and must be restricted otherwise.

4.6.2 Data should not be shared informally. When access to confidential information is required, employees should request the same to their assigned head.

4.6.3 Organization will provide training to all employees to help them understand their responsibilities when handling data.

4.6.4 Employees should keep all data secure, by taking sensible precautions and following the guidelines below:

- In particular, strong passwords must be used and they should never be shared as per password policy.
- Personal data should not be disclosed to unauthorized people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

4.6.5 Employees should not violate any data security practice implemented by the IT team. For e.g.

(a) Trying to bypass controls implemented on operating system
(b) USB Blocking/ Unblocking
(c) Installation of unknown or pirated software
(d) Uninstall any organization specified software
(e) Forget to log off the password screen (Win+L)
(f) Sharing the passwords
(g) Store the passwords in browser

4.7 Data storage

- When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it.
- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorized people could see them, like on a printer/ photo copy desk.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts.

SIYARAM SILK MILLS LIMITED
MUMBAI

- Backup Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly.
- Data should never be saved on personal laptops/ mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a well configured firewall.

4.8 Personal Data Use

- Employees are suggested to not store their personal data (e-banking information, ID proofs like aadhar, personal photos/ videos etc.) on computer resources of the organization. Organization is not responsible to secure the personal data of employees.
- If working with personal data, employees should ensure adequate security of it.
- Personal data should not be shared informally. It should never be sent by official email, as this form of communication is not secure.

4.9 Additional Cryptography Controls

4.9.1 The entire storage medium containing sensitive data shall be stored in encrypted form with strong disk encryption tools.

4.9.2 Hypertext protocol secure (HTTPS) may be implemented in all web applications to reduce the risk of man in the middle attack.

4.9.3 Backup of important local end point computers like account department, HR department, Engineering & Design and other critical data should be in encrypted form.

4.9.4 IT team will ensure the type of encryption required for data and information.

5. Policy Compliance:

Compliance Monitoring

The management will verify compliance to this policy through various methods.

5.2 Exceptions:

Any exception or change to the policy must be approved by the management in advance.

5.4 Non-Compliance:

SIYARAM SILK MILLS LIMITED
MUMBAI
★

An employee found to have violated this policy may be subject to strict disciplinary action.

6. Reference & Requirements:

S. No.	Reference Standard	Requirement
1	**ISO 27001:2013 – Clause.5.2**	Policy should be documented, communicated and available to all employees and interested parties.
2	**ISO 27001:2013- A.11.2.3: Cabling security**	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.
3	**ISO 27001:2013- A.11.2.7: Secure disposal or reuse of equipment**	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
4	**ISO 27001:2013- A.14.3.1: Protection of test data**	Test data shall be selected carefully, protected and controlled.
5	**ISO 27001:2013- A.10.1.1: Policy on the use of cryptographic controls**	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
6	**IT Act 2000, Security Guidelines- Sch. II: 2. Implementation of an Information Security Program**	(a) Adoption of IT Security Policy
7	**IT Act 2000, Security Guidelines- Sch. II: 3. Sensitive Systems Protection**	(3) For sensitive data, encryption of data in storage shall be considered to protect its confidentiality and integrity.

SIYARAM SILK MILLS LIMITED MUMBAI