Cyber Security and Data Privacy Policy

# of Baazar Style Retail Limited

Control Summery

Version	Approving Authority	Date of Approval
1	Board of Directors	August 1,2025

1 Purpose

Baazar Style Retail Limited (hereinafter referred to as "the Company") acknowledges the critical importance of safeguarding information in all its forms. In the era of increased digital integration, the Company recognises the necessity of robust systems to protect its information technology resources and the privacy of its stakeholders.

This policy aims to:

- Ensure the confidentiality, integrity, and availability of the Company's information assets.
- Protect sensitive personal data and uphold the privacy rights of all individuals, in alignment with the Rights of Persons with Disabilities Act, 2016.
- Mitigate risks associated with cybersecurity breaches and data privacy violations.

2 Scope and Applicability

This policy applies to all individuals accessing the Company's information technology resources, including:

- Employees, contractors, vendors, and suppliers.
- Devices owned, leased, or controlled by the Company, including hardware, software, networks, and databases.
- Remote access to Company systems and resources.
- Data collected, processed, or stored by the Company, including sensitive personal data.

The responsibility for policy dissemination and adherence lies with the IT Head and Site IT Heads at respective locations.

3 Definitions

- **Information Technology Resources:** Includes all IT infrastructure, hardware, software, and data owned, licensed, or managed by the Company.
- **Sensitive Personal Data:** As defined under the Indian Information Technology Rules, 2011, includes passwords, financial data, health information, biometric data, and other similar details.

- **User:** Any individual accessing the Company's IT resources, including employees, contractors, and third parties.

4 Cybersecurity Policy

4.1 Device Security

- Users must secure devices by setting strong passwords, employing up-to-date antivirus software, and installing security patches.
- Personal devices accessing Company systems must meet security standards and avoid connecting to public networks.

4.2 Email Safety

- Employees must exercise caution when opening email attachments or clicking links.
- Suspicious emails should be reported to the IT team for verification.

4.3 Password Management

- Strong, unique passwords must be used and updated every two months.
- Credentials must not be shared unless necessary and must be communicated securely.

4.4 Secure Data Transfer

- Sensitive data transfers should use Company-authorised tools and networks.
- Data access should be restricted to authorised individuals with adequate security policies in place.

4.5 Incident Reporting

- Security breaches, suspected phishing attempts, and device losses must be reported immediately to the IT team.

5. Data Privacy Policy

5.1 Information Collection

The Company collects data for legitimate business purposes, including:

- Information from the Company's website, subscriptions, and correspondence.
- Vendor, supplier, and customer data required for transactions.

5.2 Data Usage and Storage

- Data is used for marketing, administration, customer relationship management, and analytics.
- Collected data is securely stored and encrypted to prevent unauthorised access.

5.3 Data Sharing

- Data may be shared with authorised entities under the following circumstances:
- With consent from the data subject.
- To comply with legal requirements or protect the Company's rights.

5.4 Website Usage

- The Company's website collects data to enhance user experience and may utilise cookies to personalise services.
- Visitors' consent is obtained for collecting and using personal information.

6. Responsibilities

6.1 IT Team Responsibilities

- Implement firewalls, anti-malware software, and authentication systems.
- Conduct regular cybersecurity training and communicate updates on potential threats.
- Investigate breaches and enforce remedial actions promptly.

6.2 User Responsibilities

- Adhere to the guidelines for device security, email safety, and password management.
- Report potential vulnerabilities or security concerns immediately.

7. Disciplinary Actions

- Violations of this policy may result in disciplinary measures, ranging from warnings to termination of employment, depending on the severity of the infraction.
- Legal actions may be initiated in cases of severe violations.

8. Cybersecurity and Data Privacy Governance

The governance structure includes the IT Head, Store Maangers, and System Administrators, who are responsible for implementing and maintaining cybersecurity and data privacy measures.

9. Raise Your Concern

Stakeholders are encouraged to report any policy violations or concerns to the IT Head or Compliance team. Reports can be submitted via email at it.admin@stylebaazar.in

The Company ensures confidentiality and prohibits retaliation against individuals reporting concerns in good faith. Investigations will be conducted to address reported issues and enforce necessary actions.

10. Review and Amendments

This policy will be reviewed annually to incorporate advancements in cybersecurity and data privacy practices and ensure alignment with regulatory changes.
