

PRINCIPLE 9: Businesses should engage with and provide value to their consumers in a responsible manner

Essential Indicators

1. Describe the mechanisms in place to receive and respond to consumer complaints and feedback.

Customer advocacy is central to our Aspirations 2030, and we aim to be a trusted and preferred business partner by fostering strong, responsive relationships. We have a structured complaint resolution system in place, accessible through the "Contact Us" section of our website, ensuring timely redressal.

Our marketing and customer relationship management team regularly engage with customers through discussion, surveys, and meetings to gather insights. We also float periodic satisfaction surveys for our customer. Their response helps us in improving our offerings reflecting our dedication to customer-centricity.

2. Turnover of products and/services as a percentage of turnover from all products/service that carry information about:

	As a percentage to total turnover
Environmental and social parameters relevant to the product	100%
Safe and responsible usage	100%
Recycling and/or safe disposal	Not Applicable

3. Number of consumer complaints in respect of the following:

	FY 2024-25			FY 2023-24		
	Received during the year	Pending resolution at end of year	Remarks	Received during the year	Pending resolution at end of year	Remarks
Data privacy	0	0	None	0	0	None
Advertising	0	0	None	0	0	None
Cyber-security	0	0	None	0	0	None
Delivery of essential services	0	0	None	0	0	None
Restrictive Trade practices	0	0	None	0	0	None
Unfair Trade Practices	0	0	None	0	0	None
Others	555	13	None	520	5	None

4. Details of instances of product recalls on account of safety issues:

	Number	Reasons for recall
Voluntary recalls	0	Not applicable
Forced recalls	0	Not applicable

5. Does the entity have a framework/policy on cyber security and risks related to data privacy? (Yes/No) If available, provide a web-link of the policy.

Safeguarding the security and confidentiality of the Company's information and data is essential for maintaining smooth operations and stakeholder trust. At SRF, we have established a comprehensive cybersecurity policy and implementation framework to uphold these standards. The policy can be found here <https://www.srf.com/wp-content/uploads/2024/03/Cyber-Security-Policy.pdf>

Some of our key strategies to mitigate Cybersecurity risks are mentioned below:

- Strengthening network boundaries with technologies like dual firewalls, content filtering for internet and email, and secure VPNs.
- Securing data centers and implementing robust identity and access control, including multi-factor authentication.
- Managing and monitoring privileged IT user access through PIM/PAM systems.
- Conducting regular cybersecurity awareness training for employees.
- Managing mobile devices to mitigate data leak risks for specific users.
- Protecting intellectual property through classification and encryption using IRM solutions to prevent data exfiltration.
- Maintaining and upgrading infrastructure (servers, network, IT-OT) with proper segregation and micro-segmentation.
- Utilizing additional security hardware and software for enhanced data protection.
- Operating a 24/7 Security Operations Centre (SOC) for security event management and monitoring.
- Deploying advanced anti-malware and Endpoint Detection and Response (EDR) on all endpoints and servers.
- Performing routine automated vulnerability scans and applying necessary patches.
- Maintaining segregated backups to ensure data recovery after a security incident.

6. Provide details of any corrective actions taken or underway on issues relating to advertising, and delivery of essential services; cyber security and data privacy of customers; re-occurrence of instances of product recalls; penalty / action taken by regulatory authorities on safety of products / services.

Not Applicable

7. Provide the following information relating to data breaches:

a. Number of instances of data breaches along-with impact

None

b. Percentage of data breaches involving personally identifiable information of customers

None

c. Impact, if any, of the data breaches

None

Note: Reasonable assurance has been carried out by BDO India LLP on above indicator