



Cyber Security, Data Privacy and Information Security

UN SDGs impacted



“



SAM SUBRAMANIAM

President (Private Equity Investments and Group Strategy), Bajaj Finserv Ltd.

As a financial services company, the confluence of cybersecurity and sustainability is about having the right protocols in place for confidentiality and integrity of data. At Bajaj Finserv, we are continuously strengthening our controls to ensure our security systems are sustainable in the long run."

Building Resilient Digital Systems

At the BFS Group, digital resilience is a strategic priority. We are committed to data privacy and cybersecurity, ensuring full compliance with regulatory frameworks. Through robust policies, regular audits, and employee training, we proactively protect customer data and business continuity.



Cybersecurity Measures

- ◆ Cyber Security Operations Centre for real-time monitoring.
- ◆ Internet surveillance, including dark web monitoring.
- ◆ Proactive alerts for email and sensitive data sharing.
- ◆ Mobile Device Management (MDM) for secure use of apps, laptops, desktops, tablets.
- ◆ Virtual Private Network (VPN)/ Virtual Desktop Infrastructure (VDI) based secure access for business applications.
- ◆ Internal audits to periodically evaluate and enhance data protection.
- ◆ Oversight by the Board Risk Committee on controls, threats, and breach responses.
- ◆ No cyber security breaches were recorded in FY2025.

Cyber Security Governance and Audits

BFS conducts regular internal and external assessments to prevent and mitigate security risks:

- ◆ Internal audits, vulnerability scans, and penetration tests (network and app-level).

- ◆ Annual third-party audits.
- ◆ ISO surveillance audits and Red Team exercises on digital assets.
- ◆ All assessments inform threat detection and response enhancements.

Business Continuity and Operational Resilience

The Group has a well-established Business Continuity Management (BCM) strategy:

- ◆ Disaster Recovery (DR) procedures with defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
- ◆ Periodic DR drills with test result documentation.
- ◆ Integration of DR servers into Security Information and Event Management (SIEM) tools for real-time threat monitoring.
- ◆ Annual BCP drills and continuous improvement actions.

Governance and Oversight

- ◆ Board Risk Committees of material subsidiaries oversee cybersecurity and IT risk.

- ◆ Dedicated in-house and partner teams monitor 24x7 cyber operations.
- ◆ All subsidiaries follow ISO-aligned frameworks to implement, monitor and improve cybersecurity practices.

Advanced Security Systems

Subsidiaries deploy the following:

- ◆ Security Operations Centres (SOC) managed by third-party experts.
- ◆ Surface and Dark Web monitoring.
- ◆ Fraud detection by Risk Containment Units (RCUs).

Internal protections include:

- ◆ Continuous vulnerability management and issue closure tracking.
- ◆ Event-driven penetration testing for both network and application layers.



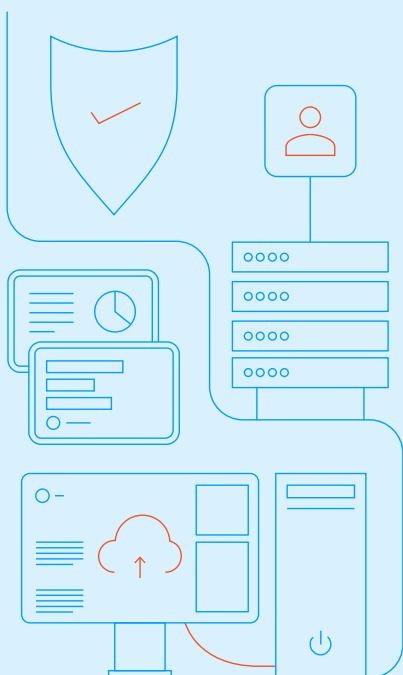
Data Privacy Framework



ASHISH PANCHAL
Managing Director and CEO, Bajaj Finserv Direct Ltd.

"Data privacy is a priority for us at Bajaj Finserv. We are building a resilient digital future for our customers by constantly strengthening cyber security systems, leveraging cloud-based solutions and proactively deploying multilayer threat detection measures."

We uphold a zero-tolerance policy for data breaches. Each group company enforces strong data privacy controls with well-defined disciplinary actions for non-compliance.



Key Data Privacy Practices

- ◆ Data is collected lawfully and transparently with user consent.
- ◆ Clear disclosure on how user data is used, shared, and retained.
- ◆ Defined Standard Operating Procedures (SOPs) for limited-purpose data processing.
- ◆ Mandatory breach reporting and stakeholder notification protocols.
- ◆ Group-wide privacy policy governed by designated teams and integrated with compliance systems.
- ◆ No customer data breaches were recorded in FY2025.

Preparing for the DPDP Act 2023

We are actively preparing for the Digital Personal Data Protection Act (DPDP Act), 2023 through:

- ◆ Formation of cross-functional teams across IT, Legal, and Compliance of all Companies.
- ◆ SOP and process map development for data discovery, access, and privacy governance.
- ◆ Material subsidiaries have made Board-approved privacy policies accessible on their websites.

Customer Data Retention and Access

To ensure trust and compliance, we have implemented:

- 1 Clear guidelines for data retention timelines.
- 2 Regular audits to assess compliance.
- 3 Restricted, role based access protocols for sensitive information.
- 4 Industry-leading practices across Group companies for secure storage, retrieval and disposal of customer data.

We follow the below principles:



Customer Rights

Allows customers to access and rectify their personal information via digital platforms (App and Web) or through our contact centres with thorough authentication.



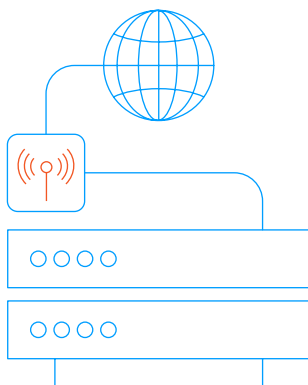
Data Usage

Data Privacy policy, available at [Bajaj Finance Investor Relations - Policies and Codes](#), outlines that customer data is used for legitimate purposes and is not sold or shared with third parties, except for completing transactions/ services.



Retention Policies

Data retention policies and durations are clearly defined in Board-approved policy, accessible on the public domain.



Our Commitment to Consumer Financial Protection

At Bajaj Finserv Group, we are committed to Consumer Financial Protection by delivering prompt, efficient, and personalised services with strict adherence to compliance and transparency.

To uphold this, over 76,000 employees—73% of our workforce—were trained in FY2025 on data privacy, cybersecurity, and consumer protection.

Information Security and Policies

The BFS Group follows a robust IT governance framework to secure customer data and ensure operational continuity. All material subsidiaries are aligned with regulatory requirements and certified under:

- ✦ ISO 27001 – Information Security Management System.
- ✦ ISO 22301 – Business Continuity Management System.
- ✦ Payment Card Industry Data Security Standard (PCIDSS) v4.0.1 – For Wallet Environments.

Additional frameworks followed (as applicable) include:

- ✦ RBI's IT Framework for NBFCs and Payment Systems.
- ✦ NHB IT guidelines for HFCs.

- ✦ IRDAI's cybersecurity guidelines and ISNP framework.
- ✦ SEBI's Cybersecurity and Resilience Framework.

Remote Work and Data Security Controls

To safeguard remote operations, advanced protective technologies have been implemented:

- ✦ Endpoint, Network and Email Data Loss Prevention (DLP).
- ✦ Endpoint Detection and Response (EDR) for malware protection.
- ✦ Conditional access for Office 365 and corporate assets.
- ✦ Defined Cybersecurity, IT and Data Privacy policies in all subsidiaries.

Data Privacy and Personal Information Protection

The Group enforces a **zero-tolerance policy on data breaches** and has implemented structured processes to ensure compliance:

- ✦ Lawful, consent-based collection and limited processing of user data.
- ✦ Transparent privacy policies and user notifications.
- ✦ Privacy concerns addressed via cyber cell units.
- ✦ Restricted and encrypted access to Personally Identifiable Information (PII).
- ✦ Continuous employee training and customer education.
- ✦ Zero data breaches reported in FY2025.

Awareness, Training and Culture Building

Recognising the human element in cybersecurity, BFS fosters awareness through:



Employee and vendor training on key systems and risks



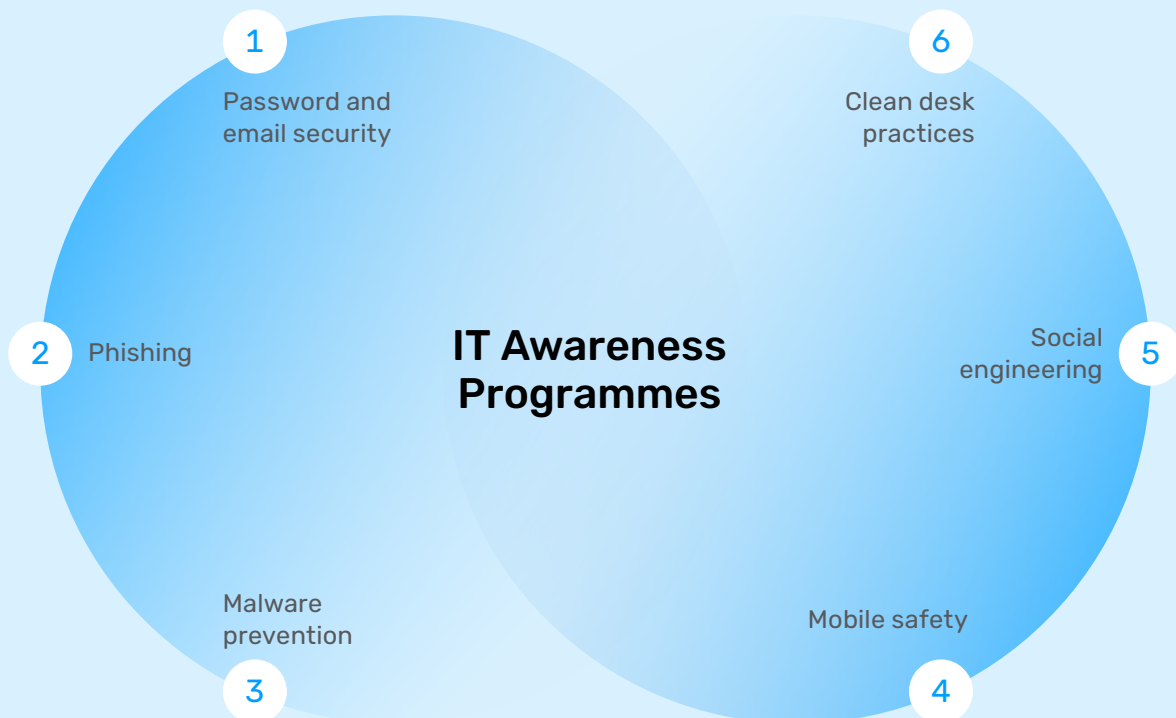
Customer campaigns on digital hygiene and fraud prevention



Law enforcement sessions on fraud patterns (e.g. insurance frauds)



Our specialised IT awareness programmes cover essential topics such as:



Cyber Security Awareness Campaigns

A series of digital campaigns run by BFL helped demystify common risks and promote secure behaviour:



'Loan Ka the End'

Importance of No Dues Certificates

'Just Ask for A Receipt'

Preventing cash misappropriation

'No Mukti Only Muskaan'

Countering fraudulent 'loan waiver' groups

'Charges For What'

Explaining financial charges to borrowers

'Wait Nahi, Update Karo'

Importance of updating contact details

'Har Koi Bajaj Nahi'

Guarding against impersonation fraud

'Settle Karna Hai Loan, Pehle Pucho Aap Kaun'

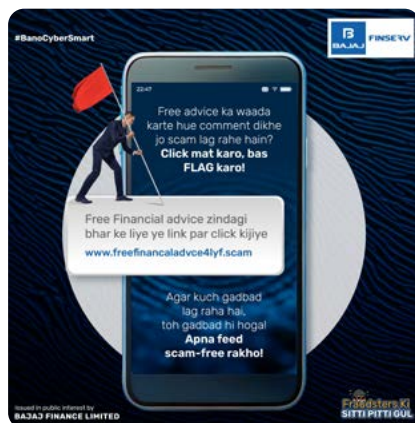
Caution against fake settlement agents

'Doori Hai Zaroori From Loan Settlement'

Clarifying foreclosure vs. settlement

'Har Time EMI On Time'

Encouraging timely repayments



9

Number of campaigns

14,06,817

Video views

492

Number of posts

29,582

Engagement

17,82,619

Impressions