BHARTI AXA LIFE INSURANCE INFORMATION SECURITY

Data Protection Policy

Version: 4.10

Contents

1 Purpose

This policy makes sure that all data used or stored on Bharti AXA Life Insurance's systems is kept safe, private, and used properly. It protects the data from being changed, destroyed, or shared without permission—whether by mistake or on purpose. The policy also explains how we safeguard personal and sensitive information, follow the law, and build trust with our employees, customers, and partners.

2 Scope and Applicability

This policy applies to anyone who works with Bharti AXA Life Insurance data—whether you are an employee, a contractor, or a third-party partner—no matter where you are located. It covers every kind of information, not just what's stored on computers. That means digital files, printed papers, audio recordings, and visual materials are all included. The data can range from personal details like names, addresses, phone numbers, and ID proofs to sensitive business information such as financial records, customer data, and internal reports. In simple terms, if you handle Bharti AXA Life Insurance information in any format, this policy guides how you must protect and use it responsibly Sensitive business information is defined as any information which is uniquely assigned to an individual or can provide traceability to the unique person.

3 Responsibility

All function heads at Bharti AXA Life Insurance Company Limited are responsible for making sure this policy is followed. They must ensure that data is handled carefully, any suspicious activity or security incident is reported right away, employees avoid clicking on unknown links or downloading unverified files, and all function heads of Bharti AXA Life Insurance Company Limited will be responsible for ensuring adherence with this policy.

4 Key Principles

- **Confidentiality**: Only the right people should be able to see the data.
- **Integrity**: Data should stay correct and not be changed unless it's properly updated.
- **Availability**: Data should be easy to get when it's needed for real work.
- **Transparency**: People should know how their data is collected, used, and stored.
- **Accountability**: Anyone who handles data must follow the rules and take responsibility.

5 Policy

Anyone who uses Bharti AXA Life Insurance's computer systems or networks must take care to protect the company's data—whether digital, paper, or any other form—from being changed, destroyed, or shared without permission. Everyone with access to these IT resources is expected to follow the key security rules outlined in the policy.

6 Data Handling & Do' & Don'ts

- **Collection**: Only gather the data you really need for work.
- **Storage**: Keep data safe with passwords, encryption, and security controls.
- **Access**: Allow only authorized people to use the data.
- **Sharing**: Share data outside the company or on personal email ids only if approved by the Function Head and CISO/CRO, with proper agreements and business justification.
- **Retention**: Keep data only as long as required by law or business needs.
- **Disposal**: Securely delete or destroy data when no longer needed.
- Business Communications: Share only legitimate work documents and information to approved email IDs (external IDs must be whitelisted and approved).
- **Approved Channels**: Use company-authorized platforms (e.g., corporate email, secure portals, SFTP for external transfers) with prior approvals.
- **Password Protection**: Always protect files with passwords when transmitting externally.
- **Verify Recipients**: Double-check email addresses and distribution lists before sending sensitive data. Do not copy your personal email id for record keeping
- **Exception Approvals**: For sharing over personal/external email, obtain prior approval from the Channel Head and InfoSec with valid justification.
- **Incident Reporting**: Immediately notify InfoSec if you suspect accidental data leakage or unauthorized sharing.
- **External Data Restriction**s: Do not send customer, vendor, employee, or Bharti AXA Life–specific data externally without approval of business head and Infosec with valid justification.
- **Personal Accounts**: Never use personal email, cloud storage, or messaging apps for business information unless explicitly approved by InfoSec.
- **Encryption**: Do not share sensitive files without encryption or security controls.
- **Confidentiality**: Do not forward any company specific internal reports, PII or sensitive data, audit findings, or investment details to unauthorized recipients either through email or any other social media/ chat app what's app
- **DLP Alerts**: Do not bypass or ignore system warnings without InfoSec clearance.
- **External Storage**: Avoid saving/uploading corporate files on personal devices, USB drives, or third-party platforms.
- **Policy Compliance**: Do not violate Bharti AXA Life Insurance's policies or data privacy laws.
- **Authorized Access**: Access confidential/company data only if it is part of your assigned job duties.

- **Data Integrity**: Do not add, change, or delete data unless officially authorized.
- Licensed Software: Use only properly licensed software; do not install pirated or single-user licenses on multiple devices.
- **System Access**: Do not attempt to log into someone else's computer or files without permission (unless part of your job).
- **Network Security**: Do not attempt to break into or tamper with Bharti AXA LI's network or connected devices.
- **Secure Disposal**: Dispose of confidential company information safely, following company rules.
- **Customer Data**: Handle customer personal information carefully and in line with privacy rules.
- **Removable Devices**: Employees cannot save/copy files onto USB drives or removable devices unless approved by an LT member and CISO/CRO.
- **Technology Controls**: The Technology team must deploy user- and role-based access controls for information.

7 Dispute Resolution

All inquiries or concerns regarding the handling of personal information should be addressed to information security team on infosecsupport@bhartiaxa.com.

8 Compliance

Compliance with these guidelines is mandatory for all staff and partners. Any violation may result in disciplinary measures and legal consequences as per company policy. For Bharti Axa Life, data refers to any information concerning policyholders, prospects, leads, employees, or vendors, including personally identifiable or sensitive information.

***** End of Document*****