

Overview:

The services, processes and solutions designed and deployed for SBI Life shall follow a standard configuration/customization process and shall meet the functional, security, performance, legal, regulatory and statutory requirements of SBI Life. The participant shall comply with SBI Life Policy on Information Security Requirements, for on prem deployment / Participant/ service provider (terms used interchangeably) location, in key concern areas as under:

- Responsibilities for data and application privacy and confidentiality
- Responsibilities on system and software access control and administration
- Custodial responsibilities for data, software, hardware and other assets of SBI Life being managed by or assigned to the Participant
- Physical Security of the facilities
- Incident response and reporting procedures
- Password Policy of SBI Life
- Data Encryption/Protection requirement of SBI Life
- Server hardening, security policies and Secure Configuration Documents
- Sharing of Background Verification of its personnel, working on SBI Life project

The Participant having access to IT infrastructure of SBI Life shall be managed as per Third-Party Access Standard & Procedure of SBI Life. If required, SBI Life Policy on Information security requirement for third-party document will be shared with the successful Participant / Bidder. SBI Life shall reserve the right to carry out Gray Box, White Box and Black Box Testing, VA/PT and Security Assessment of the application and underlying infrastructure components through their empaneled information security service providers. In case of any observations or vulnerabilities reported during these testing, the successful Participant/Bidder shall close the observation and mitigate the risk within agreed timelines, before production go live without any additional commercial levied to SBI Life. The contracts relating to outsourced services with the selected Participant shall detail security requirements in compliance with SBI Life Security Policies and supporting Standards & Procedures and the selected Participant shall demonstrate compliance with such requirements.

Detailed:

1. The Participants shall adhere to, Information Technology Act 2000, Digital Personal Data Protection Bill 2023, its amendments and rules published by Government of India and applicable sections of IRDAI Guidelines on Information Security for Insurers. The Participants shall ensure that they have Information Security organization in place to implement the provisions of SBI Life's information security requirements and protection of intellectual property.
2. The participant shall have documented policies & procedure to discharge the security requirements detailed within the RFP.
3. Information security requirements such as controls for maintaining confidentiality, integrity and availability of the SBI Life's data shall be considered at all stages throughout third party/vendors having access/handling the organizational system/data.

4. All arrangements with external party/vendors shall have a well-defined service level agreement (SLA) that shall specify information security requirements and controls, service levels and liability of suppliers in case of SLA violations, non-mitigation of information security (IS) vulnerabilities, IS incidents etc.
5. The Participants shall provide right to SBIL or its empaneled vendors or Cert-In/Cert-Fin/any other law enforcement agencies to audit / conduct security review of the center/processing facility where the services will be carried out from while designing the required deliverable/output.
6. The Participants shall be subject to a relationship assessment (sometimes referred to as due diligence review) which shall cover:
 - Dealing with the said party (e.g. details of provider history, previous and current business arrangement and dispute information)
 - Demonstrable level of maturity in relation to information security and their degree of commitment to information security. This is via a self-assessment checklist covering controls related to information security. This self-assessment checklist shall also be validated by a Cert-In empanelled vendor through selected participant at their own cost.
7. Prior to finalization of order, the Participants shall allow SBI Life Security Team or its empaneled Participants to inspect and check the designated framework/services proposed for SBI Life and undertakes necessary corrective actions as may be suggested by SBI Life prior to or during the implementation.
8. The Participants shall have a process to sign Confidentiality agreement with its employees for SBIL related services. The Participants shall provide a letter of undertaking to SBI Life as adherence to secure usage and handling of information by its employees.
9. The Participants shall have process of background check on its employees prior to their induction into SBIL project. Level of background checks should meet the sensitivity of information associated with the project. The Participants shall also provide Information Security awareness training for their resources which will be engaging with SBIL to provide services from time to time.
10. The contract requirements with service provider's Participants, if any shall include non-disclosure agreements, roles and responsibilities, and termination clauses by Organization, Law enforcement agencies and regulating agencies including IRDAI.
11. The data shall be shared with the ONLY on "Need to know" basis, if any.
12. In case of renewal, the security considerations in line with the Prior to engagement scenario shall be considered.
13. SBI Life's Internal Audit shall conduct audit for Participants(s) handling critical data/providing critical services to measure the effectiveness of the security controls implemented.
14. Network and infrastructure service level agreements (in-house or outsourced) shall clearly document security controls, capacity and service levels, and

business or customer's requirements including data flow diagram, network architecture diagram etc. for the project.

15. The Participants shall be ISO Certified for the designated line of business e.g. ISO 27001, ISO 22301 preferably etc. If the Participants is not certified, then they should adhere to the requirement of these aforesaid standards and undertaking in this regard shall be submitted to SBI Life.
16. The information security responsibilities of all Participant's employees working for customer shall be defined by Participants. Participants shall ensure that all information security requirements in the Agreement are communicated, including in writing, to all its employees in relation to their role.
17. In case of the Participants uses its own laptop/ systems for providing services to SBIL then, the operating systems, web servers, database etc. used for processing SBIL information shall be hardened in line with SBIL hardening document along with deployment of SBIL security technologies like AV, EDR/XDR, DLP etc. and VA & configuration review of these systems shall be performed at least yearly by a CERT-In empaneled vendor by the Participants at their own cost.
18. Independent security assessments (Gray Box, White Box/Secure Code Review, Secure Config review and VAPT) shall be performed for any application(s)/websites and related infrastructure components collectively referred to as Information Processing Facility, supplied to/used by SBI Life through a Cert-In empaneled Information Security service provider by the Participants at planned intervals, at least on annual basis at their own cost.
19. Participants shall submit periodic (at least annually) integrity & compliance statements of application(s)/websites, providing for reasonable level of assurance that the setup is free of malware & viruses, free of any obvious bugs, free of any covert channels in the code, free of any known vulnerabilities and free of misconfiguration.
20. SBI Life shall have the rights to conduct Independent security assessments (Gray Box, White Box/Secure Code Review, Secure Config review and VAPT) for any application(s)/websites and related infrastructure components collectively referred to as Information Processing Facility, supplied to/used by SBI Life through it's empaneled Information Security service provider. In case any vulnerability identified in these assessments then the selected participant has to close it, without adding any additional cost to SBI life, before moving to production. In case any vulnerability is identified in SBIL owned infrastructure, which is hosting the Bidder provided solution, then the selected participant shall provide all required support to SBIL team to close the vulnerabilities without any additional cost levied to SBIL.
21. i.) Foreign OEM
 - a.) The selected bidder / participant shall provide the SBIL IT Application Owner (IT AO) a certificate of assurance as per SBIL's self-certification format from Foreign OEM where source code is not available with SBIL for review.
 - b)It should be ensured by the selected bidder / participant that application is updated with latest security patch / update released by the Foreign OEM as per compatibility with existing IT systems. A self-certification from the SI (System

Integrator) partner should be enclosed with the application induction/ go-live/change management approval form.

ii. Indian OEM

- a.) The selected bidder / participant shall submit to SBIL IT AO a source code / secure code review report, submitted by a CERT-IN empaneled vendor, where source code is not available with SBIL for review.
- b.) A self-certification from the OEM or SI (System Integrator) partner should be enclosed with the application induction/ go-live/change management approval form that the application / solution is updated with latest security patch / update released by the Indian OEM
- c.) In case of the Participants is providing its services from their premises and/or the participant is accessing SBI Life network/IT systems then, as a part of pre-engagement due diligence, and as a part of yearly activity, the selected Participant needs to undergo 'Third Party Security Control Checklist' of SBIL Life. This checklist shall be validated through a CERT-In empaneled information security service provider appointed by the selected participant for each time and the report of same needs to be submitted to SBIL without any additional commercials levied to SBI Life. SBIL shall reserve the right to verify this validation report and ask for additional evidences, if any, or visit the site to verify the controls.
- d.) In case of any VPN connectivity or Leased Line connectivity with SBIL by the selected participant/Participants, hardening of desktops/Laptops (of selected participant) as per SBI Life provided hardening/SCD document to be carried out along with deployment of SBIL Antivirus, EDR, DLP solutions, regular security patches to be deployed on the desktops/Laptops. The VA/SCD/Hardening review to be carried out through a CERT-In empaneled information security service provider and the report to be submitted by the selected participant to SBI Life. The SBIL shall reserve the right to verify this validation report and ask for additional evidences, if any.
- e.) The Participants should ensure that appropriate technology measures are in place to protect the storage and exchange of information. These measures may include the following, but not limited to:
 - i. The Participants shall maintain integrity of the software in use, including patch upgrades, operating systems and applications.
 - ii. Mail attachments should be encrypted before sending as the traffic could be sniffed in transit, leading to unauthorized disclosure and modification of information.
- f.) The Participant shall comply with data retention and purging requirements of SBI Life, in case any data (SBI Life production data for testing) is shared with Participant. Compliance certificate for data retention and purging shall be sent to SBI Life as per stipulated time agreed with SBI Life
- g.) In case of any changes to the application and related ICT infrastructure components, irrespective of the magnitude of the change, mandatory security testing including gray box, black box & white box / secure code review shall be

conducted by the Selected Participant through a CERT-In empaneled information security service provider (ISSP) without any additional cost levied to SBI Life. The Production move / change management shall be done by adhering to an appropriate change management procedure after ensuring that the application and related ICT infrastructure components are free of vulnerability.