

SOW for Audit & IT Security Compliance Management Services for Desktop/Laptop

Objective

To achieve 99% compliance in regards to SBIL IT Security policy & various standards adopted by SBIL. It helps SBI Life to comply with software & other audits conducted by internal as well as external auditors.

Responsibilities

- Adherence to SBI Life's IT & IS policy as well as Acceptable Usage Policy.
- Adherence to IT Standards accepted by SBI Life for IT security.
- Installation of windows OS version with appropriate windows security patches approved by competent authority of SBI Life.
- Installing version upgrade of existing approved software's.
- To ensure all endpoints to be part of Active Directory (AD).
- To maintain all agents like BMC remedy, Symantec Antivirus, MacAfee DLP etc. online on all the endpoints.
- To maintain local administrator password policy and make sure to do not disclose with end users.
- Group Update Provider (GUP) or any Distribution Server (DS) or Relay machines (Local Desktop) in branches are to be connected and updated with centralized servers. On site engineer to be arranged if in case it is not connected to centralized server or not resolved through remote.
- Preventive Maintenance (PM) of all desktops/laptops in branches are need to be done once in a quarter at all locations, the list of activities to be carried out during Preventive Maintenance is provided.
- Activities to be carried out in Preventive Maintenance are prepared in the form of checklist and it has to be 100% adhered. Checklist is enclosed along with RFP under section Annexure D.2.
- It is mandatory to complete PM for all assets within 90 day's cycle hence lapses for uncompleted PM will attract penalties as mentioned in RFP.
- PM schedule to be confirmed and intimated to respective SBIL branch & Belapur office.

Deliverables

- Installation, configuration, troubleshooting of following agents:
Symantec, BMC Remedy, MacAfee DLP and any other agents approved by SBIL as mandatory for desktop /laptops time to time during contract period.
- Installation of Operating Systems at least once in a year if the existing version of OS declared End of Support by OEM.
- Implementation of Secured Configuration as per SBIL's SCD guidelines.
- Monthly windows security patches to be installing in all desktops & laptops.
- Regional audit & inter audit findings about the non-compliance to be targeted as Zero findings.
- Any audit finding reported by auditor should be closed within the stipulated time given towards closure. Usually closure timing for desktop/laptop is within one week.
- Submission of checklist of PM dully filled & signed off obtained by end user on IT portal form or physical form.
- Any unauthorized software / tool found to be removed immediately & inform to SBIL Belapur Office ASAP in writing.
- Any unauthorized access / user found to be removed immediately & inform to SBIL Belapur Office ASAP in writing.
- Any noncompliance found to be corrected & reported to SBIL Belapur Office ASAP in writing.