Preventive Maintenance (PM) Activity Guidelines V7.0

Contents

Preventive Maintenance Guidelines

Below is the guideline which needs to be followed by all PM Engineers while doing the PM activity in SBI Life Insurance Premises.

Need to notify below points to all branch users.

It has been made mandatory by ISC (Information Security Committee) and RMC (Risk Management Committee-E) that:

- All users connect their company provided Laptops to office LAN and log on to SBIL domain using their NT/Windows ID.
- Location-in- charge/Department Heads needs to ensure that all PCs located at their location/department are connected office LAN and log on to SBIL domain using their NT/Windows ID at least once in 15 days.
- In case any user found to be not connecting their company allocated PCs/Laptops to office LAN then their IT Services like email, NT/Windows Login, Pro-Center, Attendance System, EMS etc. will be disabled.
- New single session login policy is being implemented, with one NT id users can login only in one system and incase of multiple login will prompted a self-explanatory error and login to the system will be rejected.
- As per SBI-LIFE procurement team HP S3000 S2 & Below are not covered in any support and against the same HP S3000 S3 & Above and S5000 S3 Scanners are provided,

❖ Step-1: user standardization

➢ **Check Default Administrator (sbilsuadm) in all assets**

If the Default administrator is (**sbilsuadm**) then no action is required

Incase sbilsuadm is missing from systems need to follow below instructions.

- ✓ Rename default administrator account to **sbilsuadm. (Ensure exact format of user id it should in small case)**
- ✓ Set the password given by CST Team. **(Do not Share the admin password to any end user and this should be strictly followed).**

➢ **Checking unique user-id in all systems**

User shall access PC/Laptop using the unique user-id/password provided to them only. Password should have necessary complexity, changed frequently and be treated as confidential.

- ✓ **Unique user-id (NT ID):** Ensure that all branch users are login with their **NT ID**.
- ✓ If the user login with **Local user** or any local user available then follow below instructions.
  - o Disable the **Local user** and inform user to login with the their NT login ID.
  - o Incase **NT login ID** is unavailable with user then inform them to log a ticket at CST and get the new user requisition form filled, obtained the required approvals and forward to CST to create the NT ID.

CST Helpdesk Contact details: - : 022-61720900 || cst@sbilife.co.in ||

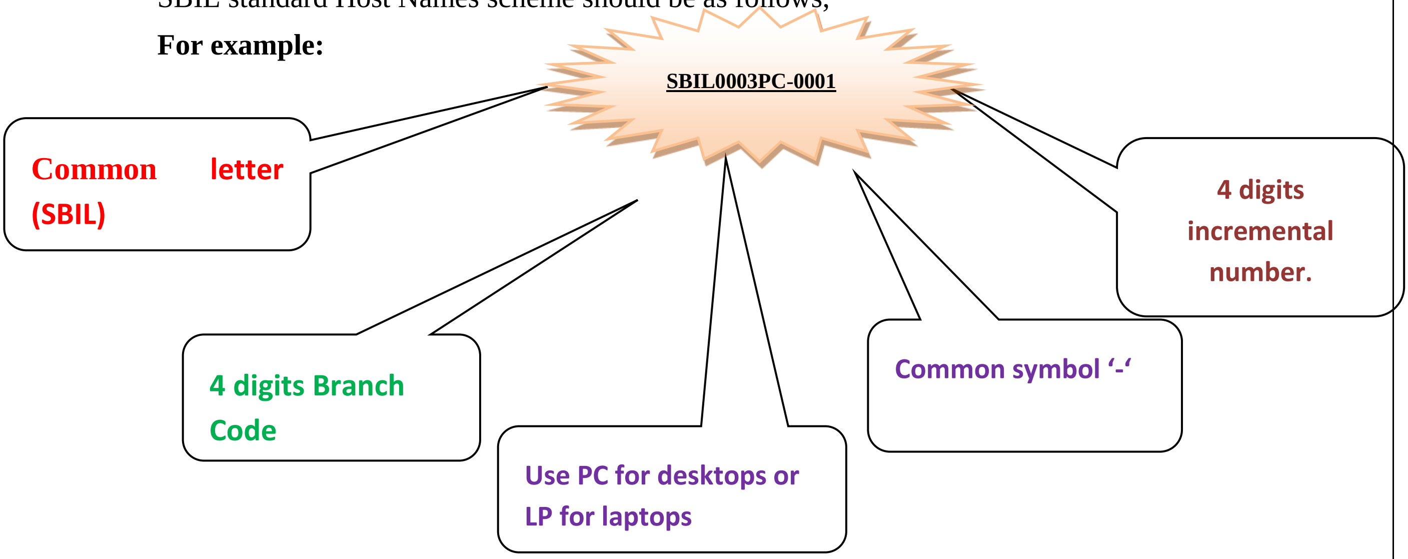
Local accounts except “sbilsuadm” and “Netadmin” need to be deleted from system and disable Sbilguest User ID.

If user is Login with the Sbilife or any other local ID then Inform to CST Team. User should login to the desktop/laptop using unique user-id (NT ID) only.

- ❖ **Step-2: Hostnames**

SBIL standard Host Names scheme should be as follows,

For example:



Above systems is in branch having code 0003 and it’s a desktop.0001

Laptop’s first incremental number should be start from 0001 (not from where desktop’s incremental numbers ends).

- ❖ **Step-3: Symantec Antivirus**

Latest Version / signatures of Symantec End point protections

Of antivirus is required in all desktops and laptops in branches.

The Setup is already available in the branch with latest software in GUP system With IP address xx.xx.xx.06

Below are some antivirus related guidelines...

- ➢ **Symantec EP:** Ensure that Symantec Endpoint Protection clients are install in all systems.
- ➢ As installer is updater, required to execute the setup with Admin privilege. The setup will automatically remove the old version & update to new one (Provided old antivirus is Symantec endpoint protection 14.x)
- ➢ In every branch GUP server is configured and Branch user has to ensure that GUP server is updated with the latest Definition and online.
- ➢ GUP (Group update policy) machine should be label and highlight the importance to branch user. Inform user to make sure about the GUP Machine should be power ON in production hrs.

- **IP Address assigned to GUP & ITAM Relay should be 10.X.X.6 (Secondary ITAM rely should be configured 10.X.X.7)**
- Ensure that all systems Symantec Endpoint are updated with latest virus definition and online**.**
- Keep update the host name and IP address of GUP machine to SBI Life - PM activity team in Mumbai.
- Kindly confirm with CAST team if the desktops/laptops are located in proper OU in SEPM else required to replace the sylink file with the help of CAST.

❖ Step-4: Printer Installation

As per IT Compliance Printer installation is Mandatory in branches

- Printer should be installed on Network only
- Printer IP address should be Static and IP assigned to Printer is 10.x.x.12
- If in branch printer count is more assign second IP address as 10.x.x.13

❖ Step-5: Domain

- In all type of Network connectivity branches systems (MPLS\ UTM Devices) needs to join in Domain with proper Hostname.
- All desktop / laptops should be a part of the SBI Life domain and all local users should be disable/deleted.
- If any workgroup is present then required to remove the same.
- Ensure that all laptop or desktop to be part of SBIL domain.

❖ Step-6: Windows security patches / Anti-virus installation.

Latest window patches along with latest version of Anti-virus EP need to install in all the systems.

Selected vendor should ensure before visiting the branch that the Setup files are already available in the branch with latest software in GUP system With IP address xx.xx.xx.06 if not available connect with CST and get it available

Any media created by selected vendor for distribution to their team members for PM activity has to be free of virus / malware etc.

- ✓ Windows OS (as per SBI Life policy) Security Patch 64 Bit.
- ✓ Anti-virus EP (Latest Version) needs to reinstall and update with latest definition.
- ✓ Kindly ensure that the patches mentioned for 64 bits required to be installed in appropriate systems.

- **Step-7: Unauthorized software**

All software used in SBI Life must have proper approval from authorization. Below are some applications guidelines. Approved software list to be obtained from CST

- **Browsers:** Currently "Edge" "Google Chrome" & "Mozilla Firefox" are only authorized browser in SBI Life (uninstall other browsers), or any other web Browser defined by SBI Life.
- **PDF software:** Latest "Adobe Reader" & PDF Creator (uninstall any other PDF related software. E.g. PDF Writer, Pdf Creator etc.).
- **Other Software:** Remove the PDF to Word, Word to PDF, and other convertor Software (Except File Format Convertor), iTunes, Mobile Software (Nokia, Samsung etc.). Remove Win Zip and Win Rar, install 7 Zip which is authorized Software in the SBILIFE. Apple Software, iTunes.
- Refer the approved s/w list and any other s/w found should be removed from the end point
- Need to copy all the PM signed copy in branch GUP server for audit purpose.
- **Media Players:** except "Windows Media Player" all other music /video players need to be removed.
- **Tool Bars:** Currently no add-on toolbars are allowed in user systems (uninstall all toolbars in all Browsers or in system tray area, especially Google toolbars).

Note: -

In case of any requirement to installed the software follow the software inclusion process by raising the ticket in Centralized IT help desk application or connect with Software license manager

- **Step-8: Unauthorized Data**

Unauthorized or personnel data is not allowed in user systems. Below are some data related guidelines.

- **Pictures:** personal photos, pictures, images are not allowed in systems (delete it and ask user to adhere the data policy).
- If the Official Photo (Office meeting, Get-together, Price Distribution) is available kept only in one system and then remove from all systems.
- **Videos:** No videos are allowed in systems except Training material (user need to take Regional Risk Manager approval to keep training videos in system).
- **Music:** Delete songs (in any format), meditation sound clips, etc..

- **Games:** Remove all games from systems including built in games in windows. Also remove all flash games, excel games, small exe-based games, etc.

- **Objectionable contents:** Any objection contents found in system should be highlighted to Branch head, BSM, Regional Risk Manager, Regional Auditor and CST team in Mumbai with snapshot as a evidence and remove it immediately.

- **Unauthorized User:** Need to check Local User and unauthorized users in branch systems delete the local User permanently if any found except, Standard local Administrator (sbilsuadm), Netadmin and sbilguest should be there in disable mode only.

- **Folder Sharing:** Remove unauthorized folder sharing from local computers, remove local Drive sharing unauthorized drive mapping. Remove everyone Rights from local sharing properties.

❖ Step-9: Clean temporary files

Clean temporary files \ Cookies \ Temp internet files.

❖ Step-10: Install the Update Java (Jre)Approved Version to Image flow using systems.

- Check the Java Version in Branches system which is using Image flow software.
- If the User is using Image flow in the system, Kindly Update with Java latest approved version.

❖ Step-11: Installation of ITAM agent

It’s mandatory to Install ITAM Agent in the all systems during the PM.

- Check Blue icon at the right corner of taskbar
- Check Process **“BCM AGENT”** is running or not in services.
- **Each branch is having the relay machine which is distribution server of branch and should be power ON during the production hrs.**
- **Please highlight the importance of RELAY SERVER and label the same**.
- If there is any change update the host name and IP address to SBI Life - PM activity team in Mumbai.

❖ Step-12: Installation of DLP Agent.

- Check Red icon at the right corner of taskbar ELSE.
- Check Process “McAfee DLP Endpoint Service”, Dct zscaler coscto any connect is running or not.

- **Step-13: Branch IT Infrastructure Check**

“Floor Plan diagram” should be available in server/network room. If not available then draw one diagram and share with Central Team.

All IT assets should be connected through UPS Power system.

- Modem / Router / Switch / Desktop / Laptop / Printer / Scanner / Audio video equipment etc.

Highlight the importance and functioning of UPS to branch.

Highlight the voltage requirement to the IT assets (E.g.- 230V AC to IT assets, Earthing Voltage should be below 2V).

Server room and Network cabling should be as per SBI-LIFE standard IT policy.

- Server room should have sufficient cooling & ventilation.
- All the data/voice cables in server room should be label. If labeling is not available then ask branch to get it done through regional admin and utility team.
- Highlight the importance of router, switches, Modems, light indications and important ports and their cables.
- If server rack is found messed-up then highlight to branch head or BSM and CST team in Mumbai with snapshot as evidence and inform to get it clear through regional admin and utility team.
- Serial number, make, model of switches/routers/UTM’s/printers/scanners to be captured and update to SBI Life – PM Team in Mumbai.

- **Step-14: IT Asset Possession Certificate**

Ones all above mentioned PM activities are completed fill up below online certificate

“IT Asset Possession Certificate” Form online for all systems.

“IT Asset Possession Certificate” URL and guidelines would be shared in the Separate file.

IT Asset Possession Certificate Link: http://itasset.sbilife.co.in:95

- Once open the link fill up your all detail for the login and click on Submit.
- One option is showing **“Do you want to complete the Incomplete Details”** Click NO.
- In the Employee mode Select the “Own” Option.
- Required the user all details. (Telephone number, Check the Mobile number, Branch Code and Type, Asset Tag).

- Kindly make sure about the information captured on IT possession cert is correct Before submitting the details.

Note: PM engineer need to inform BSM or branch head two days in advance before visiting branch to ensure maximum IT assets are available in branch.

IF any system is removing from the desk or found disconnected then engineer needs to connect the system and do PM activity and highlight to PM team.

If any system found in not working condition then mention the details in the form along with user details and logs the call with the CST.

Note: - Incase asset is not allocated to any user then mention Branch Manager Name with designation.

All Common IT Asset other than Laptop/ Desktop should also be mention against Branch manager name

In the "**IT Asset Possession Certificate"** online form you can add more than one system in the one file.

Once file is saved then further it will not be editable.

Note: - It's mandatory to fill up Online IT Asset Possession Certificate" for each system and incase if it's not done then PM will be considered as incomplete.

When the Form is completely fill then click on the Submit, after that click it generate PDF report.

Required the PM PDF file name is "**ITPC-Branch Code-Employee code"**

1. Kindly note: Required all report in the PDF format only and proper file name format.

2. Do not send the scan copy in the JPG or other format. We will not accept this report.

3. Engineer once visited at branch provide all IT assets (Desktop \ Laptop \ Printer Scanner etc..) which is not working or not available in the branch at Time of PM.
4. Provide the engineer visit details one day in advance on daily basis.
5. CST will log the call on mail for the PM. Provide us the Vendor/Service desk call ID.
6. If any system is dead, or not working due to hardware inform to PM Team log the call on Field. Make the call report for this system and mention the user name, System serial number and Call log ID and send us the scan copy in the PDF with the sign and stamp of the user. Any Laptop user not available Mail the User name \ Email \Contact numbers to PM Team.
7. If the Windows not booting or not working then repair or reinstall the OS with the Sbilife PD Only and install the all approved Basic software's and Domain configuration.
8. Ensure that the IP address and Host name is not changed and in case of any confusion take help from PM Team.
9. If warranty systems having the hardware issue then log the call with respective vendor and take the Case ID and the Service provider details.

   Mail the Case ID and Service Provider details to PM Team and make the call report.

Important Note: -

After Completing the PM needs to take confirmation from PM Central team about system reflecting in Active Directory, ITAM Agent, Symantec EP, NAC Agent and DLP Agent. Asset register

Branch stamp and Signature of respective user should be available in each and every IT possession certificate.

Hard copy of IT possession certificate with stamp and Signature of respective user should be provided to Branch Manager / SPOC and keep the copy in local GUP sever.

PM Completed system verify with CAST, DLP, DCT, ITAM Team.

---------: End Document: --------