SB Order No. 06 / 2021

File No. FS-76/1/2021-FS-DOP
Government of India
Ministry of Communications
Department of Posts
(FS Divison)
Dak Bhawan, New Delhi – 110001
23.03.2021

To

All Head of Circles / Regions

Subject: Preservation of Backup of Sanchay Post Databases and reporting of errors in respect of Sanchay Post Application – Reg.

Madam / Sir,

A kind reference is invited to the SB Order No. 7 / 2010 dated 11.03.2010 issued in connection with the **Security of Sanchay Post Database and issues relating to common problems, database back-up, storage and preservation** and a revised procedure on maintenance of Database, Signature Scanning, Security of database, Frequency of data backup, Storage location of data backup, Preservation of audit trail and accountability of these activities was circulated. The same is reiterated in the **Annexure-I**.

2. It is observed that in some non-CBS offices, copies of backup of Sanchay Post databases are not being preserved as per the security guidelines issued by Directorate. Since Sanchay Post data is decentralized, preservation of backup of databases at periodical intervals (daily, weekly and monthly) as per security guidelines issued by Directorate, is essential for the purpose of investigation, prevention of frauds / misappropriation, backup restoration in case of system failures and for smooth day to day functioning of those offices.

3. Whenever error is displayed in Sanchay Post application in respect of non-CBS offices working in Sanchay Post, the offices should report the error immediately along with the complete details (such as name of the non-CBS office, Division email id and details of the error along with error screenshot) from official email id to CEPT SBLAN Help Desk (sblan.chennai@indiapost.gov.in).

4. In case of any database consistency errors, the errors may be forwarded to CEPT SBLAN Help Desk along with authentication of Divisional Heads (scanned copy of letter signed by Divisional Heads). Divisional Heads shall provide authentication only after ascertaining the correctness of the complete details provided by the office including the details of error reported in transactions of previous days, any action attempted for rectification of the error, along with date of availability of recent backup of the database of the office, which is in good condition without any database consistency errors.

...2..

5. Hence the Circles / Regions are requested to ensure that backup of databases in respect of non-CBS offices are preserved without fail as per the security guidelines issued by Directorate and errors are reported as detailed above.

6. This is issued with the approval of the Competent Authority.

Encl: Annexure – I

23/3/2021

(T C VIJAYAN)
Asst. Director (SB-I)

Copy to:-

1. Sr. PPS to Secretary (Posts)
2. PS to Director General Postal Services.
3. PPS/ PS to Addl. DG (Co-ordination)/Member (Banking)/Member (O)/Member (P)/ Member (Planning & HRD)/Member (PLI)/Member (Tech)/AS & FA
4. Addl. Director General, APS, New Delhi
5. Chief General Manager, BD Directorate / Parcel Directorate / PLI Directorate
6. Sr. Deputy Director General (Vig) & CVO) / Sr. Deputy Director General (PAF)
7. Director, RAKNPA / CGM, CEPT / Directors of all PTCs
8. Director General P & T (Audit), Civil Lines, New Delhi
9. Secretary, Postal Services Board/ All Deputy Directors General
10. All General Managers (Finance) / Directors Postal Accounts / DDAP
11. Chief Engineer (Civil), Postal Directorate
12. All recognized Federations / Unions / Associations
13. GM, CEPT, Mysuru - for uploading the order on the India Post website
14. The Dy. Director (OL), Postal Directorate for kind information and for translation of the order in Hindi Language accordingly.
15. Guard File

23/3/2021

(T C VIJAYAN)
Asst. Director (SB-I)

Maintenance of Database

1. The System Administrator should run consistency checks for all SB databases every month. The query is given below:-

- Run SQL Query Analyzer
- Select the SB databases one by one
- Run the command "DBCC CHECKDB"
- The above query does not require SA rights and if any consistency/allocation errors are received, Regional/Circle Office should be contacted.

2. The following basic database maintenance tasks should also be carried out using DB Analyzer software:

- Check for database corruption using "DB Analyzer >> DB Utilities >> Check database consistency" option. This should be done for all the databases. If the result displayed is not (0 consistency errors and 0 allocation errors found) contact SDC Chennai through email for rectification. (To be done at least once in a fortnight)
- Clear the log files of all databases using "DB Analyzer >> DB Utilities >> Clear Log File" option. (To be done at least once in a week)
- Errors listed in DB Analyzer should be rectified. Steps to be taken are indicated in the discrepancy list.

3. Upgradation manual should be read before commencement of upgradation and interest posting. For this, instructions are available in SDC Chennai website and in Sanchay Post upgradation CD.

Signature Scanning

- Only one signature in SB3 card is to be scanned.
- In version 6.5, the size of signature file should not exceed 25K.
- Procedure for scanning is available in the upgradation manual and on the SDC Chennai website.

Security of database (Virus problem)

Anti-Virus software should be installed in the server and all the clients and should be updated regularly. A number of offices running Sanchay Post software are complaining of an error received when they try to logon to the Sanchay Post Module viz. "Fatal disk error". This problem could be due to a virus named "Sality". Symptoms of "Sality" virus infection are:-

...2...

- An error 'Fatal disk error' is shown when Sanchay Post is started.
- Post5.exe size is above 50kb.
- If reinstalled, Sanchay Post runs only once but fails with 'Fatal disk error' from the next time onwards.

To solve this problem, take backup of all databases and then scan/clean the system with updated antivirus software. To prevent this problem, ensure that antivirus software is updated regularly.

Datbase Backup and its frequency

- Backup should be taken daily by the System Administrators / Official identified for the purpose at HOs and SOs.
- Backups are to be taken for all the databases i.e. BPRO, BPLOG, POST, SOSB, SIGN and all the SO databases in HOs and SOs.
- In case of scheduled backups using 'Database Maintenance wizard' it should be ensured that the backup has taken place and completed without errors.
- A full database backup can be scheduled at the end of transaction hours and differential backup if needed at regular intervals depending on the number of transactions handled at that office.

Location / Storage of Backups

- Backup files ideally should be saved on a node or should be transferred to a node after completion.
- Backups are to be written to an external media such as CD / DVD every week and sent to the designated identified office for safe custody.
- The CD / DVD should be neatly labeled with the date of backup, Office name, person performing the backup and verification.
- The CD / DVD up should be checked on another system for readability, before being sent to safe custody.
- SO / MDG should send the CD / DVD to the respective HOs.
- HOs should send one copy of the CD / DVD to the Divisional Office and other to Regional Office/Circle Office.
- **It must be ensured by the Postmasters that at least one copy of the backup, every week should be kept in a building away from the office (offsite)** to provide protection against location-specific catastrophes.

...3...

Accountability

1. A register is to be maintained by the head of the office to record the periodical backup process.

2. In case of server breakdown / change of server / upgradation, if databases are to be restored from backups, it must be ensured that all the databases are restored inclusive of BPLOG and BPRO. The date and time of restoration should also be recorded in the register.

3. The date of performing the additional maintenance tasks should also be recorded in the register.

4. The register should contain the following details:
   - Date and time of backup / restoration / maintenance
   - Name of Person performing the task
   - Backup file Location – Node / CD / DVD
   - Date of sending CD to safe custody
   - Countersign of Head of the Office.

Removal of Audit Trails

- After confirming the reliability of the backup received at the Regional/Circle office with the help of the Regional/Circle System Administrator, the Divisional Office can be authorized to remove the audit trails of specified period.
- Removing the data may be carried out by the Divisional System Administrator in the presence of an inspecting authority i.e SSP/SP/ASP or IP and duly documented for records. This operation should be performed every year in HOs and heavy transaction offices and once in two years in smaller offices.
- The period of retention of audit trail data should be 10 years or until agreement is completed, whichever is later.
- For investigations and whenever necessary, the older backup can be obtained from Divisional/Regional/Circle office.