



Technotalk



PTC MYSORE TECHNOLOGY BULLETIN

Vol I. Issue 3

Oct. 2007

Introduction

Computers have been in use in our organization for over a decade now. Initially, we deployed computers in select offices and used them to run standalone applications to support a few functions. We later networked the computers in each office (called local area network), to run applications in the client/server environment. These networks were used to run individual applications like Sanchaya Post, Meghdoot Point of Sale etc. We later added more applications, especially in Meghdoot and interconnected all these applications to transfer data of transactions generated in one application to other applications. This made it possible for the HOs to automatically generate HO summary and also cashbook, minimizing repetition of data entry. Simultaneously, we also built applications like Speednet and e-payment to transfer data across many Post offices through Internet based Wide Area Network. Sub offices have also been computerized.

This shows that there has been a steady progress in the use of computers. Today there is a need to maximize gains of computerization by networking our computerized offices and perform our tasks with more accuracy and efficiency, utilizing the capability of computers to a desired extent. The networking of offices based on NIC Net is in progress and by this year end a substantial number of HOs are expected to be connected in a wide area network.

As we expand our network of computerized offices, the matter of security of data assumes greater significance. Since our applications are operating independently in various offices, the data pertaining to each office is residing at the concerned office. When the offices are networked, it is possible to migrate to a more secure system of a central database. This is expected to take some time, we need to take necessary precautions for safeguarding the security of our local databases.

So far we have compromised on security on the plea that our supervisors are not capable of enforcing the security environment. The general opinion is that enforcement of security is a difficult task for the following reasons:

- 1 It impedes ease of use.
- 1 Users find the requirements of security too complicated and difficult to implement. Over emphasis on security issues impedes the progress of computerization.
- 1 It is difficult to run certain applications without administrative privilege

The focus of this issue of Techno Talk is to explode the above myths and to demonstrate a practicable security regime that can be implemented. Far from being an obstacle to implementation, secure practices will bolster confidence in the system in the long run.

Binding the office to a secure environment requires some tough decisions. Further all the users must be made aware of the security requirements as also the advantages of

implementing security and the fatalities associated with the open environment. Initially, the users may find it difficult to adjust and it may seem that the environment is complicated and not easy to work in, but as they get used to, the initial blues will disappear. Securing the working environment provides assurance to the users that they work in a safe place and minimizes the scope for misuse of the environment for unscrupulous purposes.

Apart from being a healthy practice, it has now become mandatory to build security in the computerized offices, as directions have been issued towards this end in Directorate's letter no Letter No 46-5/2004-Tech dated 21 July 2004 and Computer Security Guidelines – 2006 a confidential document communicated vide Directorate letter No. 51-8/2006-Tech dated 12 Feb 07. In this issue of Technotalk, we address various security related concerns and provide tips on implementing security without hassles.

FAQs on security in computerized offices

1. What are the various levels of security?

Security has to be implemented at the following levels

- 1 Physical
- 1 Operating system
- 1 Database
- 1 Application

a) Physical security - to ensure that the hardware, peripherals, consumables and offline devices are protected from theft, wrong usage and abuse.

b) Operating system security - to ensure that the resources like files, folders etc. are not accessed by unauthorized

persons, either on the local system or over the network.

c) Database security - to ensure that precious data representing transactions stored in databases are not manipulated.

d) Application level security – to ensure that the tasks expected to be performed by each user level are performed by the user concerned, thus minimizing the scope for misuse.

2. How physical security is ensured?

Physical security refers to securing the hardware environment. The following steps are suggested

1 The server should be preferably placed in a room or enclosure which can be locked;

1 The server room or enclosure should always be locked when not in use;

1 Entry to the server room should be restricted and each access should be logged (a register can be maintained for this purpose);

1 The server should never be used for operations in the normal course;

1 The hub or switch should be preferably placed inside the server room or enclosure; If these have to be placed outside, they have to be secured in cabinets which can be

locked;

1 Offline devices like external hard disks, CD writers, pen drives etc., should never be kept near the server when not in use;

1 Maintenance work should be performed by authorized personnel in the presence of a responsible official of the office; Any component that is being taken out by the maintenance staff for repairs should be logged;

1 CD, floppy or any other device should be removed from the drives immediately after use and should not be left in the drives;

1 PCs should not normally be moved around unnecessarily; If movement becomes necessary, such events should be logged;

1 Wherever possible, PCs should be placed in lockable cabinets and should be securely locked when not in use;

1 PCs, printers and scanners should be covered with synthetic covers when not in use and these covers should be completely removed during usage;

1 Power supply for computers and peripherals should always be through UPS.

3. How to implement Operating system level security?

As already discussed, operating system level security ensures that computers are not misused. The following steps are suggested:

1 The first and the most important step in implementing Operating system level security is to secure the built-in administrator's account. This account which is created at the time of installing the operating system has unlimited rights and must be used most diligently for the following reasons -

i. This account gives the users the capability to even remotely administer the server without having the need to locally login to the server

ii. Viruses require administrative privilege to attack the system and casual use of administrator's account can leave the system open for attack

1 The password of the administrator on each of the client/standalone system(s) or domain must be with the authorized person

1 Every other user must have a user account created with limited rights

1 Creation of common user accounts should strictly be avoided as this leaves the system open for misuse

1 There is no need to logon to the server daily after switching it on. Everyday, after the server is switched on, the clients can use the resources on the server over the network and no local login is required at the server. One needs to logon to the server only to perform administrative tasks. Hence logging on to the server should not be a routine habit. It is normally seen that the administrators logon to the server and leave the login as it is even without securing the same

1 Password security should be implemented to ensure the following

i. Passwords are changed by users periodically

ii. Whenever passwords are changed, users enter a new password and do not repeat the old password

1 Indiscrete sharing of resources on the server should be avoided

4. How to ensure application level security?

Applications like Meghdoot or Sanchay Post are designed to perform PO tasks with the help

of computers. Since office transactions are performed using these applications, it is necessary to exhibit utmost care in using applications as lapses in security are likely to create a security void which can be misused. The following suggestions may be kept in view

1 All day-to-day transactions will have to be invariably performed using the relevant applications, adopting the work flow as expected

1 While troubleshooting any problems faced, tools provided by the applications alone should be used and short cut methods like correcting the databases should never be attempted

1 Each user for whom a user account is created in the application should immediately login and change the password. The password should be such that it cannot be easily guessed.

1 Once a password is changed by the user, even the administrator would not be able to gauge it except that such passwords can be changed. So, on any day, when a user tries to login with a password which was used on the previous occasion and the attempt is not successful, the supervisor and the head of the office should be alerted

1 The passwords should be of the length prescribed and should be changed periodically as per the directions

1 Users should perform tasks on their own and should not allow others to login with their user accounts to perform

the tasks assigned; Supervisors should specially note this

5. How to ensure user level security on a standalone PC in use in the office?

This security can be implemented only if the operating system in use is Windows 2000 Professional or later versions. We can implement user level security in this environment when many users are using a standalone PC for various purposes. The administrator should login, use the computer management tool under Administrative tools, expand the **Local users and Groups folder**, right click the Users folder, select the menu **New User** and proceed to create the new user for each user. The user should immediately login and change his/her password. Action to be taken to permit users to use various applications is explained separately.

6. Is it necessary for the administrator to be available whenever a new user has to be created to use a standalone PC?

This is not required. The administrator can delegate this right of creation of user to a responsible person. The administrator can create a user account for such person as explained above and add this user to the **Power Users** group which will enable this user to create user accounts for other users. Such delegation will not create any security risk as this user has very limited rights like creating users and installing applications

7. What is a domain?

With Microsoft client/server network, we build a domain. A domain, simply put means a logical group of computers that share trusted information. The domain is not created by default when the Windows server operating system is installed. It has to be created with an appropriate name on the server. Once the domain is created on the server, client systems connect to the domain.

Hub and switch - a comparison

Hub is a network device which is at the centre of the network. A cable from each system is connected to the hub. The data reaches the hub through the cable. The hub just amplifies the signal and broadcasts it to all systems connected in the network. Only that system to which the signal is addressed receives and the other systems ignore the signal.

Switch is also a network device which is an improvement over the hub. A switch remembers the addresses of machines connected to its ports and channelises the signal only to the system to which it is addressed.

The point for comparison here is that while the hub transmits the signal to all the ports irrespective of the system to which it is addressed, the switch transmits it to only that

address to which the signal is destined. This results in dramatic reduction of network traffic and increases the potential bandwidth.

It is therefore suggested that the existing sites where hubs are already installed can definitely change over to switch. The change over is very easy and the comparative cost of switch over hub is meager compared to the advantage.

The advantage of having a domain is that, in the client/server network, we can create user accounts, set security policies and define how the shared resources can be used on the server which is called the domain controller. When the users connect to the domain and attempt to use the resources of the network, security policies set already are applied. This is an effective way of building security in the network.

8. How to create a domain user account with ordinary rights?

The domain users connect to the server from the client systems. These users cannot login locally at the server and use shared resources on the server from client systems. These users cannot also perform any administrative tasks on the local system from where they login, unless specific permissions are assigned. To create the domain user, the administrator should use the menu **Start – Programs – Active Directory Users and Computers** on the domain controller

9. Can any other user apart from Administrator create a domain user account?

Yes. The administrator can delegate this right to any other user like a Supervisor or head of the office, by adding such user to the **Account Operators** group using the **Active Directory users and Computers** tool in the Domain controller. This user can create and administer the users created by him/her alone, but cannot perform any other critical administrative tasks.

10. How to ensure that floppies and CDs are not indiscriminately used in the office?

a) This can be ensured in one of the two ways. One method is to physically disconnect these drives. The other method is to disable these drives using the **Device Manager (Start – Settings – Control Panel – System –**

Hardware – Device Manager or Right Click on ‘My Computer’ – Properties – Hardware – Device Manager).

b) Administrator can disable these drives. Other users will not be able to enable such drives unless they have the administrative privileges.

c) Floppy & CD drive may be enabled only in one system. Such system should be under the physical control of either the administrator or a supervisor. This system must have an anti virus software installed and updated. Any offline device that needs to be used (like pen drive) must be scanned for virus and cured before the files contained therein are copied to the system.

11. How the users can be prevented from connecting to the domain beyond the authorized working hours

The administrator can set the working hours during which the users can login to the domain based on each user's requirement. Proceed in the following steps to implement this security

1 Login as Administrator in the Domain controller

1 Select **Start – Programs – Administrative tools – Active Directory users and Computers**

1 Expand the users folder and double click on the user concerned in the right pane; The user properties dialog box appears

1 Click the **Account** tab and next on the **Logon Hours** button

1 In the **Logon hours** dialog box, You may observe that by default, the user has unrestricted access all through the day and night; select time for which access is not required and select the option **Access denied**; Now click the OK button in the Logon hours dialog box and the user properties dialog box to complete the task

1 From now on, the user will not be able to connect to the domain beyond the hours prescribed

1 This may however, not

prevent a user who has already logged in, during the permitted hours from accessing the server beyond the authorized hours; For this, the security policy of Autologoff should be enabled (use the menu **Programs – Administrative tools – Domain Security Policy – Local Policies – Security options** and enable the Policy **Automatically Logoff users when Logon time expires**

12. Is it possible for the domain users to change their passwords, working in the client systems?

Yes. After the user logs in, if the Ctrl, Alt and Delete keys are pressed together in the given sequence, the Windows security dialog box comes up. One of the options available is **Change Password** that can be used to change the password by the logged in user

13. How to set the password policy of requiring users to compulsorily change password after a certain number of days?

a) This policy for the entire network can be set on the domain controller (server). Under **Administrative Tools** use the menu **Domain Security Policy - Account Policies - Password Policy**. Select the policy **Maximum Password Age** and set the number of days after which user will have to change the password. Once this policy is set, the users will have to change the password after the prescribed number of days, else login will not be allowed.

b) While setting this policy, additionally the administrator will also have to use the tool **Domain Controller security Policy** and **Local security Policy** to set similar policy so that this can be applied on the domain controller as well as on all the systems connected to the server respectively.

c) A similar policy can also be set on a standalone system using the menu **Administrative tools – Local Security Policy** which will apply to all users on that system. But once such

system is connected to the domain, the domain level policy set as above will override the local policy

14. How to ensure that users enter a new password whenever they change the password?

Using the same menu as in the above question, the administrator can set the policy **Enforce password History** to 1, which will ensure that whenever any user attempts to change the password, the previous password is not given. There is however an option to set this policy up to 24 which is not desirable, since the user will be able to use any of the previous 24 passwords. This is certainly fraught with risk. It is ideal to set this policy to 1.

15. How to ensure that users type a minimum number of characters as password?

The administrator can use the tool **Minimum password length** to set the number of characters that users must type as password. The minimum length prescribed by the department is 8.

If this policy is to be implemented in an existing environment, it should be noted that this will not apply to passwords already set and will be invoked only when the user attempts to change the password the next time

16. What precaution should be taken when a user leaves the system temporarily for any reason during the working hours?

While working on a system, it may sometimes become necessary for a user to leave the system temporarily to attend to some other work or for any other reason. In such situations, it would be difficult to expect the user to shut down the system for security reasons as the process of shut down and start up will result in loss of precious time. In these circumstances, the user is advised to adopt any of the following methods to secure the logins

1 The user can exit from

all the applications and logoff Windows;

1 The user can set a screen saver with password protection; This can be set by selecting the Display properties – Screensaver, setting an idle time interval(say, 10 minutes) and clicking the check box **On resume, password protect**; This will ensure that when the system is not used for the specified time, a screen saver will be applied and to use the system again, the logged in user will have to enter the password; This utility protects your system when you leave it without protecting it

1 Access the Windows security dialog box by pressing **Ctrl+Alt+Del** keys and select the option **Lock Computer** from the options available; This ensures security to your login by Locking Computer as no other user can login; When you have to use the system again, you can press **Ctrl+Alt+Del** keys again and enter your password to unlock computer; However, the administrator can unlock the computer in which case your user account will be logged off

17. What precautions should be taken while handling the passwords?

While setting passwords remember the following guidelines

1 Use a mixture of alphabetic and number keys and also special characters for the passwords

1 Do not relate the passwords to your name, that of your relative or any other associations which can be imagined by others

1 Change the passwords every 15 days

1 Do not reveal the password to any one else, even in case of emergency

1 Do not attempt to logon other user accounts

1 The Supervisors should never part with their passwords for the sake of convenience as this has dangerous consequences

1 When you are not able to logon with the password that

you are regularly using, there may be a security breach; Please inform the Supervisor and seek a fresh password from the administrator. Change the password immediately.

1 In case you have a problem of remembering the password, it is suggested to keep the password in sealed cover, in safe custody.

18. What resources should be shared? What precautions are required?

The normal habit is to share the hard drives straightaway. Such indiscrete sharing should be avoided and only required resources should be shared based on the need. The following list shows the various resources to be shared

In the Meghdoot environment

1 For Point of sale – The PointofSaleServer folder in the server in the installation path

1 For Subaccounts – The Server component in the server – either C:\Subaccounts or any other path where the server component is installed

1 For treasury module – The server component in the server – either C:\Treasury or any other path where the server component is installed

While sharing it should be ensured that the default permission **Everyone – Full control** in Windows 2000 Server and **Everyone – Read** permission should be removed and appropriate permission as below should be given to ensure security to the contents

1 The administrator should be granted **Full control** permission

1 Each of the other users who will be using the applications concerned should be granted the appropriate permissions(Read and change)

Speednet

The server component of Speednet – **Speednetserver** folder in the server should be shared with appropriate permissions

The **EMSCClient** folder in the system where the Speednet

communication module is installed with appropriate permissions

There is no need to share any other folder on the server where the above two modules are running.

In case of Sanchay Post, there is no need to share any folder

19. How to prevent clandestine access to resources on the server by users from clients

It will not be possible for users to access the resources on the server from clients that are not shared if the administrator's password is secured

20. What installation issues are to be taken care of in SQL Server?

In a network environment, the personal edition of SQL Server 2000 should never be installed in the client systems. Also, while installing the Standard editions, the administrative tools should never be selected for installation. In case of SQL server 2005, the administrative tools should be deselected while installing in the client systems

21. How to prevent casual access by users to SQL Server?

The administrative tools of SQL Server like Enterprise manager and Query Analyzer pose a security hazard if not protected. Two users – the built in administrator of Windows and SQL Server administrator (SA) can administer the SQL server. We normally come across two security lapses here. First, the administrator's account is known to all the users. The other lapse is that usually a default password is set for SA in almost all offices which gets easily known to all the users. These lapses provide unobstructed access to critical components of SQL server which can be misused to the extent of committing frauds. The following steps are suggested to prevent such misuse

1 The administrator's password should be secured and all the users must have domain

user accounts without additional privileges. To re-iterate, there is no need to have administrative privileges to run the applications and ordinary user accounts can suffice this purpose

1 A unique password has to be set for the SA which should not be known to ordinary users

22. According to recent instructions, the password of SA of SQL server has to be with the divisional head. How to implement this security while ensuring that day-to-day operations are not hampered?

a) The first step in implementing this security is to set a unique password for SA, if possible by divisional head himself or herself and to secure the same. If there are a large number of offices and it is not practicable for the divisional head to do this, it is suggested that this task be delegated to system administrator of the divisional office.

b) The next step is to deny access to SQL server for the built in Windows administrator account. It is now necessary to ensure that day-to-day operations are not affected by such a move as no administrative tasks can now be performed. Great care should be taken in performing this task. If denial to Windows administrator is applied without properly securing the SQL Server SA password or if the password is forgotten, there is no option but to reinstall SQL Server.

c) The only day to day requirement now is to perform backup. This can be attended to by either automating the backup or creating a SQL server user who can attend to this task.

(i) In the first case, when the backup is scheduled, it is necessary that the SQL Server Agent service should be running at the scheduled time. If access to built-in administrator is denied, SQL Server Agent will not start and so logon should be changed to that of SQL Server SA.

(ii) In the second case, a separate SQL server user can be

created using the Security – Login tool in the Enterprise manager, making the user a member of Processadmin group with the database role being backupoperator with access to all the user databases. This user can perform backup but cannot access the components of databases.

d) The other occasion when the SA password is required at the site is when upgrades are applied. On such occasions, it is inevitable that database upgrades are applied at each site personally by the divisional head or the designated system administrator using the SQL Server login. Though this is a painfully long process, it cannot be neglected at the cost of the much required security.

23. How to ensure that users in a network do not change their desktop environments?

This can be done by editing default domain policy using the Active Directory users and computers tool on the Server. The steps are listed below. Before proceeding with this, ensure that in all the clients the customizations of the desktops and screen savers are removed and only default settings are available

- 1 Login as Administrator in the Domain Controller

- 1 Run the **Active Directory Users and Computers** tool

- 1 In the next window, right click on the domain and click **Properties**

- 1 In the domain properties dialog box, click the tab **Group Policy**

- 1 With the default domain properties selected, click the **Edit** button

- 1 In the Group Policy window, expand the folder **Administrative templates** under **user configuration**

- 1 Now expand the **Control Panel** and select **Display**

- 1 In the right pane double click the policy **Disable Display in Control Panel**

- 1 In the Properties dialog

box that followed select the option **Enabled** and click OK button; Close the Group Policy window

- 1 In the domain Properties dialog box, click the OK button

- 1 Now, no domain user will be able to change the desktop properties

- 1 The administrator can at any time disable this setting which will facilitate users to change their desktops. So, administrative rights should never be given to ordinary users

24. When a user other than administrator logs in from a client system in the domain, Point of Sale does not run. How to solve this?

To troubleshoot this problem, the following tasks will have to be completed

- 1 The administrator should login to the system from where login should be provided to the user concerned. Upon such login, the administrator should permit the domain user account created for the user to the local Change System time policy using the tool **Administrative Tools – Local Security Policy – Local Policies – User right assignment**

- 1 If the C drive of the system from where access to Point of Sale for the domain user to be permitted is in NTFS, appropriate write permission to be assigned to the domain user

- 1 In the server, appropriate share permission (write) should be assigned to the PointofSaleServer folder to the domain user

25. How to permit a domain user to run the Accounts module from a client system in the network?

The administrator should login and install the Accounts module. Thereafter the registry entry concerned should be exported and applied to the registry of the user concerned. This process is explained in the following steps which should be attempted to carefully as playing with registry can be harmful to

the OS

- 1 The administrator should access the Run command and type **regedit**

- 1 In the **Registry Editor** window, expand HKEY_CURRENT_USER, expand software and select **VB and VBA Program settings**

- 1 Now select the menu **Registry – Export registry file**

- 1 In the dialog box that follows, save the file with a filename in a drive or folder which can be accessed by all users

- 1 Now login as the user who should use the accounts module

- 1 Use the regedit

- 1 Select the menu **Registry – Import registry file**

- 1 In the dialog box that follows, select the exported file and click OK button which will apply the registry entries to the logged in user's registry

- 1 The user can now run the accounts module; However, if the Accounts module is installed in a NTFS drive, appropriate permissions should be granted to the user concerned

26. How to ensure that backups are available to recover from a failure, in case of Meghdoot applications?

Apart from the database backups, backup of mdb files of Point of Sale, Subaccounts and Treasury should be available to apply restoration successfully

27. What backup strategy should be adopted to ensure that latest data is recovered through restoration in the event of failure?

SQL server offers three types of backup – Complete, Differential and Transaction log. A combination of these three can be employed to take backup without disturbing the routine work while ensuring availability of latest backup for recovery in the event of failure. The following strategy is suggested. This is apart from any backup that is being taken as per the directions existing

Database backups – Complete

Complete backup backs up everything regardless of when the previous backup was taken.

Complete backup has to be taken at the end of each day on completion of office work. This can be either scheduled or done manually but preferably performed manually. To perform this backup, access the Enterprise Manager, open the SQL Server, expand the Databases folder, right click on the database whose backup should be taken, select the menu **All Tasks – Backup database** from the context menu. In the backup database dialog box that comes up, select the backup option as **Database – Complete**, select the destination as either tape or disk, if it is tape ensure that the cartridge is placed in the DAT drive, if it is disk, click the **Add** button, specify the path, enter a backup filename and click OK. If it is proposed to schedule the backup click the check box **Schedule**, click the period button and in the **Edit schedule** dialog box that follows, select the option **Recurring**, click the **Change** button and in the next dialog box, select the option as **Daily** and enter the time at which the backup should be taken in the **Daily frequency** frame and click OK, click OK on Edit schedule dialog box and OK in backup dialog box.

Alternatively, you can use Database maintenance plan to perform complete backup of multiple databases and this can be scheduled to be performed at recurring intervals.

Database backups – Differential

Differential backup backs up changes made to the database since last complete backup regardless of when the previous differential backup was taken. It is applied between two complete backups.

There is no option to use the Database maintenance plan to perform this backup in SQL Server 2000 but available in SQL Server 2005 version.

This can be applied and

scheduled to be performed between 1300 to 1400 hours. Follow the same method as in complete backup except that the backup type may be chosen as **Differential**

Database backups – Transaction log

Transaction log backup backs up changes made to the database since last complete, differential or transaction log backup whichever is the latest. It is applied after a complete or differential backup, depending on the strategy adopted.

It may be observed that for some of the databases, this option is not available in the backup databases dialog box. To resolve this, right click the database concerned, select Properties, click the tab **Options** in the database properties dialog box, set the **Recovery model** to full and click OK button.

This backup can be scheduled to be performed every 15 minutes or 30 minutes depending on the database. All counter databases can be scheduled for 15 minutes and others, once in 30 minutes. Such backups should be arranged in sequence and labeled properly for easy restoration.

Though an option is available to take transaction log backups through the Database maintenance plan, since there are different schedules for different databases, it is preferable to set the backup on individual databases. Since a differential backup is being taken in the middle of the day, one schedule can be created to run from the morning up to prior to the time set for differential backup and the other schedule from the 15th or 30th minute, as the case may be, from the differential backup time and can run at intervals to conclude just before the time when complete backup is due.

28. What are the databases that need to be selected for backup?

As far as Meghdoot is concerned, there are several databases related to various

modules whose list is given below. Apart from this, the relevant mdb files also need to be copied. Please refer to this list below

Databases in SQL Server

1 C O U N T E R ,
ECOUNTER and IPO databases for Point of Sale

1 POSTMAN database for Postman module

1 BOSUBACCOUNTS,
BOSUPPLYSUBACCOUNTS,
S U B A C C O U N T S ,
S U B T R E A S U R Y ,
SUPPLYSUBACCOUNTS and
TREASURY databases for
Subaccounts and Treasury
modules

1 MOCOMPILATION
database for MO compilation

1 A C C O U N T S ,
CASHBOOK, INCOMETAX
and NPC databases for Accounts

1 SCHEDULE database
for Accounts PBS

Access database files

1 Counter.mdb in
PointofSaleserver folder

1 Subaccounts.mdb in
Subaccounts server folder

1 Treasury.mdb in
Treasury server folder

1 Access database
files(mdb files) – Twice
physically every day using
Windows backup in Point of
Sale, sub accounts and treasury
modules

□ First when Shift/day
begin is done

□ Next when Shift/day
end is done

In respect of Sanchay Post,
the following databases in SQL
Server should be selected for
backup

1 BPLOG, BPRO, POST,
SIGN and SOSB

1 In HOs, if SO databases
are also created, backup of all the
SO databases

A log book should be
maintained to note down the
strategy, the backup file names
on completion, the schedule and
the media where they are
available for reference during
restoration

29. What should be the

restoration policy for the backup strategy?

The restoration procedure for the backup strategy suggested is listed below which can help in smooth recovery.

This plan is suggested presuming that in case of server or other failures, the office brings up a new server which should be brought up using the backups available. The new server may preferably be given the same name as the old one with the same IP address and a domain configured. All the prerequisites are to be installed before proceeding further. The recovery process for Meghdoot is explained in the following steps

1 All applications to be installed on the server (both server and client components)

1 Complete backup of all databases to be restored with 'no recovery' option first

1 Latest differential backup after last complete backup to be restored with 'no recovery' option

1 All transaction log backups after the latest differential backup to be restored in sequence, one after the other, except the latest log backup with 'no recovery' option

1 Latest log backup to be restored with recovery option

1 Latest Access database file(mdb) of Point of sale, Sub accounts and treasury to be copied to the respective server components overwriting the existing ones

1 The **PTClogins.exe** available in the Meghdoot 6.4 CD should be executed, entering the SQL Server name and sa password

1 If the Server name is different from the one that crashed, the SA should open Treasury database, select tables, open the table Server data and enter the new server name in the rows against the column **Linkedservername** wherever the old server name is seen (against Pointofsale and Postman Branchname) and close the table and database opened

and exit the enterprise manager

1 Treasury Supervisor has to login and confirm whether the login is successful

1 After this, the Point of Sale Supervisor has to login and select the new server name as the treasury server name

1 The Postman Supervisor has login and enter the server name for Counter, Ecounter and Treasury databases replacing the existing names

1 MO compilation supervisor has to login and enter the new server name for counter, Postman and Subaccounts databases

1 Accounts Supervisor should login to general module and enter the name of new server for all databases using the menu

Tools – Network links

The recovery process for Sanchay Post, in the similar situation is as below

1 Install the Sanchay Post and run DB creation to create dummy databases

1 Drop the databases – BPLOG, BPRO, POST, SIGN & SOSB

1 Restore the databases in the sequence as explained for Meghdoot

1 Download the latest **DBAnalyzer.exe** from the Sanchay Post support site (SDC, Chennai) and use SQL 2000 or SQL 2005 option to update the DCL login of the new installation to all the databases restored

1 On completion of this step, the server may preferably be restarted

In the client systems

1 The IP addresses need to be changed, if required

1 Clients to join the new domain created with the server

1 Configuration files in each client for all the applications to be modified to point to the server component in the new server

With this the restoration is complete and the environment is ready to proceed with subsequent transactions

Overview of Work Flow in SpeedNet

In the first issue of 'Techno Talk' FAQs on SpeedNet 3.0 were discussed. Feedback on the issue indicated that there is a need for a more preliminary exposure on the work flow in SpeedNet. This document explains the work flow in Speednet module. The objective is to acclimatize the user to the working environment and to provide quick tips on using various tools to perform day-to-day operations.

1. Role of Supervisor (routine)

The Supervisor of each set performs shift begin (**Tools – Shift Begin**) and allocates work (**Tools – Today's Job Allocation**) at the beginning of the set and performs Shift end (**Tools – Shift End**) on completion of the set. Before performing shift end, if there are any users who did not perform shift end, the supervisor has the option to forcibly end the shift of such user (**Tools – Forcible shift end**). On completion of the tasks in the set, the Supervisor generates the Set report and Discrepancy Report using the Reports menu.

There are other specific roles which will be explained under each transaction item separately

2. Collection and despatch of articles

a) Data updation of speed post articles booked in Point of Sale

Speed post articles can be booked in the counter of the office using Point of Sale or at any of the linked offices. The data from such booking points need to be uploaded (this may be either full data or minimum data). The menu **Receipts – Data updation** is used for this purpose. Physical collection of articles should follow

b) Collection of articles

Booked articles are collected for further handling in Speednet. Articles should be scanned individually using the following tools under various circumstances

1 The tool **Receipts – collect booked articles - My office** is used to collect articles booked in the counter of the office

1 The tool **Receipts – Collect booked articles - other office** is used to collect articles booked in linked office

1 In both the above cases, instead of individual scanning of articles collected, **virtual scanning** can be enabled. This helps to collect all the articles without scanning. This method can be adopted only if the virtual scanning is enabled by the Supervisor using the menu **Tools – Virtual scanning**.

1 Ins The tool **Receipts – Collect booked articles with booking details** is used to collect articles booked manually entering all the details of the articles

1 Articles from BNPL customers are collected using the menu **BNPL – Collect BNPL articles**

1 Option is available to collect articles from bulk customers either at SPC or at BPC using the bulk customer module along with collection of data in any format presented by the customer; option is also available to collect bulk articles without address details in the same module.

1 Articles from Agents using Collection Agent package can be collected using the menu **Collection Agent – Collect Articles from Agents**

Once articles are collected they need to be sorted and scanned to the various bags according to the despatch schedule

c) Despatch of articles

Use the menu **Issues – Scan articles** to scan the sorted articles in respective bags periodically. Once scanned, the articles are identified in the respective bags and are ready to be closed. This option can be used to scan the articles as they arrive.

Use the menu **Issues –**

Closing of bags to include all the articles which are not scanned already (normally the late arrivals) and finally close the bag. When the bag is closed finally, bar code for bag has to be scanned. Once the bag is closed operator will not be able to make any modifications to bag entry but the supervisor can attend to this

On closing the bag, manifest can be printed either from the **close bag** window itself or using the menu **Reports – Speed Post manifest**

d) Supervisor's role

The Supervisor can add an article in a bag using the menu **Modification – Article sent data**. If the bag that is closed should be summarily canceled, the supervisor can use the menu **Modification – Cancel Bags sent**. However this option can be used only as long as the bag is not dispatched

TBs prescribed, if any, can be closed using the menu **Issues – Closing of TBs**. Mail list can be generated using the menu **Issues – Despatch of bags**. Thereafter, bags to be included in various routes can be added and mail list is printed from the same menu or using the menu **Reports – Speed Post mail list and Speed Post TB list**. In case some bags are left out of the mail list erroneously, the same can be added by the operator using the same menu or by supervisor using the menu **Modification – Bag sent data**

3. Role of operator handling of articles for delivery

a) Receipt of bags

Bags received either addressed to the office receiving it or to other offices can be entered using the menu **Receipts – Receipt of Bags**. While receiving the bags, the bag barcode must be scanned. However, in case of bags which do not contain the barcode, the check box bag without barcode to be selected and the bag received.

Of the bags received, those that need to be despatched to

other offices should be segregated and mail list prepared using the menu **Issues – Despatch of bags**. If there are any TBs which need to be opened, the menu **Receipts – Opening of TBs** is used.

b) Opening of bags

The bags received should be opened and the contents scanned for further handling. The menu **Receipts – Opening of bags** is used for this purpose.

An office can open only those bags addressed to it and received as above. On using the menu and scanning the bag, the Article Details tab becomes active and the operator can scan all the articles received.

However, if virtual scanning is enabled and the bag data is already received from the central server, the articles in the bag will be listed and the operator can click Finish button to receive all articles without resorting to individual scanning.

c) Issue of articles for delivery

Articles received and those in deposit are segregated for delivery through the office and through linked offices.

Articles for delivery through the offices are sorted according to beats and scanned for the respective beats using the menu **Delivery - Invoicing – Speed Post or Express Parcels - Articles or Parcels for delivery**. When the articles are scanned, sender and addressee data would be automatically available, if it is received from the central server.

On completion of scanning, delivery slip can be printed from within this window by using the **F10** function key or using the menu **Reports – Delivery – Speed Post or Express Parcels – Delivery slip**.

Using the menu **Delivery – Invoicing – Money Orders – MOs transferred**, the speed post MOs received can be transferred to the linked office from where payments are to be made.

In a networked environ

ment, if articles for delivery to be entered are found to be heavy and need to be attended to by more than one operator, there is no need for individual transfer of articles. Any operator who is authorized to work in the set can handle these articles. On completion of such entries, the operator who received these articles can make bulk transfer and the other operator can receive such transfers using the menu **Tools – Bulk transfer**.

d) Despatch of articles to linked offices

If there are articles to be despatched to linked offices, use the menu **Delivery – Invoicing – Speed Post or Express Parcels – Articles or Parcels for other offices**. The invoice of these articles can be generated from within this window using **F12** function key or using the menu **Reports – Delivery – Speed Post or Express Parcels – To Other Offices**.

e) Entry of returns

Returns of Speed post and Express parcel articles are entered using the menu **Delivery – Returns – Speed Post or Express Parcels**. Here we select those undelivered articles and enter reasons. When we complete the returns other articles are marked as delivered. Additional data like the time of delivery and the person to whom delivered can be entered to provide correct inputs to the sender when it is tracked.

f) Remarks for Articles sent to other offices

Using the menu **Delivery-> Remarks From Other Offices** option, return remarks of the articles sent to other offices have to be entered. It can be entered to any previous day as and when office receives remarks from other offices.

g) Remarks for MOs sent to PO for payment

On receipt of intimation of MOs paid by Post offices, remarks of payment has to be entered using the menu **Delivery -> MO Remarks**. If MOs are paid by SPC itself, then Supervisor has to enable the option under Supervisor menu

Delivery -> General Information -> SPMO delivery option. Then MOs can be invoiced similar to the steps mentioned above for other articles.

h) Despatch of articles returned undelivered

If any article entered into Delivery option has to be closed in a bag, for returning to Sender or redirection or for any other reason, then such article has to be scanned under **Delivery -> Dispatch** option. If not done, such article cannot be closed in the bag as the article is shown as deposit in Delivery.

i) Delivery info of articles not handled through Speednet

There is provision to enter the return remarks for articles that are not at all entered into this package.

It is done under **Delivery-> Other Office Article- Delivery Data**.

This option can be used by any of the offices, which has to collect the delivery information for speed articles and feed the data. This is important since it is used to provide the delivery information to customer.

j) Supervisor's role –

Can use **Modification-> Alter Bags Opened** option and add or delete articles of the Bag.

Can modify the source from which the bag is received under **Modifications -> Bags Received Data -> Modify Bag** option.

4. BNPL:

1 Supervisor will do the BNPL Customer Master entry and other configuration like distance slab for cities, Customer OB etc.

1 If any BNPL customer is willing to use a Booking package called Corporate Customer then supervisor has to provide Configuration file to customer using his BNPL option. The Corporate customer package can be installed in the customer's system. Customer can book the articles at his premise and bring Floppy Data or CD Data to SPC along with

articles.

1 Operator collects BNPL articles under **BNPL – Collect BNPL Articles**. Articles can be collected with or without floppy/CD data. If there is no floppy data and there is no time to make detailed data entry at the time of collecting the articles, operator can collect the articles without detailed data entry under this option. If so, he has to make detailed data entry later under **Tools-> Article Data Entry** option. If detailed data entry is not there, billing cannot be done.

1 Rest of the treatment for the article, ie., dispatch or delivery is same as explained earlier.

1 If the SPC does the billing for the BNPL articles, supervisor has to make sure that the BNPL Billing option is ticked under **Master->Environment -> My Office details**.

1 Operator will prepare the Bill under **BNPL->Customer Monthly Bill** option. Latest version includes the service tax calculation also.

1 Under **BNPL->Customer Advance Payment**, any advance entry can be made.

1 Supervisor has to verify such Generated Bill and Advance Payment under Supervisor menu option **BNPL->BNPL Bill Verification**. Only after such verification the amount is accounted as paid. If the payment is through Cheque or Draft then supervisor has to make realization entry. Only then the payment will be accounted.

1 BNPL Reports are available under **Reports -> BNPL** option.

5. Collection Agent:

1 Supervisor will do collection agent master data entry under his options, like Localities, Agent details, Issue of Barcodes, Agent Commission etc.

1 If Collection agent is using a Booking package called Collection Agent package then supervisor has to provide Configuration file to Agent to configure his package. Agent can book articles and bring

Floppy/CD Data to SPC. The Agent package also calculates service tax for the articles he books.

1 Operator will collect the Agent articles under **Collection Agent -> Collect Articles from Agent**. Only Floppy/CD data can be accepted under this option. No manual entry of the article is possible.

Note: If Agent books article manually then he has to get those articles rebooked at Point of Sale. SpeedNet can upload the data from POS.

1 If articles are collected from Agent in SpeedNet, Monthly Revenue from Agent can be generated through this package by the operator using **Collection Agent -> Monthly Revenue**.

1 Supervisor has to verify such Monthly Revenue under **Collection Agent->Monthly Revenue Verification**. Only after such verification agent commission can be paid.

1 After monthly revenue is generated and verified, Monthly commission can be paid under Operator option **Collection Agent->Payment of Commission**.

1 Supervisor has to verify this payment entry under **Collection Agent -> Payment of Commission Verification**.

1 Agents Reports are available under **Reports -> Collection Agent**

Contact Info:

PTC runs a help desk to provide solutions on problems being faced in using software developed by PTC Mysore. The contact details are given below

Contact details of help desk

Email id:

ptcdesk@hotmail.com;
ptcdesk@gmail.com;
ptchelpdesk@rediffmail.com

Telephone number :

0821 – 2449015

Responses to this Bulletin may be sent to srk65in@gmail.com

TechnoTalk issues can be downloaded from PTC Mysore website