Preventive Vigilance

Computer Safety

AIUCBOF Empowerment Series

Chapter 28

Preventive Vigilance

Do's & don't RELATING TO Computer Safety

DO's:-

1. Do use only your unique User-id for login.
2. Do logout when you go away from the system
3. Do maintain strict privacy of your password
4. Do use passwords difficult to guess
5. Do change passwords often
6. Do get proper guidance before using sensitive menus such as account closing & interest posting etc.
7. Do give right inputs and verify before confirming the transaction
8. Do place batch/transaction numbers and initials on the voucher
9. Do read, understand and record error messages for future reference
10. Do read & preserve manuals and circulars carefully
11. Do answer customer queries correctly
12. Do present neat passbook entries and with legible statements
13. Do maintain prescribed register of inventory & update periodically
14. Do use maker-checker concept
15. Do preserve voucher properly
16. Do authenticate printouts and preserve

17. Do check vouchers with statements/supplementary/day books daily without fail
18. Do check system generated transactions carefully
19. Do check system generated interest-with sampling of high values accounts
20. Do check Exceptional Transaction Report daily
21. Do sample check for Revenue Leakage
22. Do ensure periodical job rotation
23. Do check staff accounts for high value transactions
24. Do be familiar with computer generated balance reports
25. Do use variation techniques to access data integrity, income-expenditure movements etc.
26. Do monitor large value transactions/collection instruments – especially in newly opened accounts
27. Do monitor transactions in Inoperative accounts
28. Do monitor concessions in commission/interest/waiver of charges
29. Do ensure proper insurance/warranty/insurance
30. Do preserve audit trails/Transaction Logs/Access Logs
31. Do use Anti Virus and updates
32. Do rectify computer audit objections
33. Do oversee proper upkeep of computer systems
34. Do take proper "Fall Back Reports" for next day before closing

DON'T's :-

1. Do not allow anyone to peep while you type password
2. Do not use obvious passwords viz. your Userid; spouse or sibling name
3. Do not use other's password under express/implied authority
4. Do not leave logged-in system unattended
5. Do not allow others to use your password
6. Do not allow anyone to peep while you type your password
7. Do not use higher level/passing powers unless authorized
8. Do not ignore error & warning messages on the screen

9. Do not experiment with menus
10. Do not give input without supporting vouchers
11. Do not allow customers/outsiders to operate computer terminals
12. Do not reveal transactions/operations of any customer to others not authorized to receive such information.
13. Do not destroy old records without proper verification for prescribed periodicity
14. Do not allow movement of inventory without proper knowledge/authority/necessity
15. Do not allow obsolete inventory lye idle
16. Do not allow environment conducive to tampering/pilferage
17. Do not permit games software usage
18. Do not get panicky in error situations