

The Depository Trust Company

IMPORTANT

Executive Important Notice

B#: 1747

DATE: April 09, 2001

TO: All Participants, Customers, Transfer Agents and other users of DTC's application

CATEGORY: Executive Notices

FROM: Corporate Information Security Office

ATTENTION: All Access Coordinators and Operators

SUBJECT: Network Security Precautions

Each Participant, customer, transfer agent or other user of DTC's applications is responsible for controlling its communications network link(s) with DTCC. We urge you to periodically review and test your company's controls over your organization's use of DTCC's communications links. We also urge you to reinforce the need for all employees who are authorized to access DTC's applications to be security conscious and to take appropriate steps to protect your organizations own processing environment. The Network Security Precautions listed below are some suggested safeguards.

Network Security Precautions

1. Assure the integrity of the employees and consultants who are authorized by your organization to access DTC's applications.
2. Restrict and monitor access to the areas or sites where terminals, PCs, other computers or links used to establish a connection to DTCC's network are located.
3. For any application where passwords are not systematically forced to be changed, periodically arrange a password change by contacting DTCC's Customer Support Center at 888-382-2721. (Note: CCF, CCFII and MDH users should contact Participant Interface Planning directly via email at pjp@DTCC.com for assistance with password changes.)

4. Immediately change a password by contacting DTCC's Customer Support Center at 888-382-2721, if a password becomes known to an unauthorized individual or if an individual with knowledge of a password leaves your organization or assumes other responsibilities. (Note: PTS users may use the "PASS" function to change their passwords).
5. Prohibit users from displaying passwords and DTCC's dial-in telephone numbers in public, such as taped to terminals or PCs. Maintaining passwords in written format should be discouraged.
6. Prohibit employees from programming or storing passwords and/or user IDs in electronic formats.
7. Assign separate user IDs/passwords and functions to each individual user based on assigned job responsibilities to assure segregation of duties and individual accountability.
8. Where applicable (e.g., PTS, PTS Jr.), require users to invoke their own password changes. Allowing someone else to perform this function could result in unauthorized use.
9. Where applicable (e.g., CCFII), restrict and monitor access to files and/or libraries that contain job control statements.
10. Consider prohibiting the use of remote control software where it could be used to establish a connection to DTCC's network.
11. Consider DTCC's dial-in telephone numbers and TCP/IP addresses confidential and make them available only to individuals having a functional "need to know."
12. Consider DTCC's User Manuals confidential and make them available only to individuals having a functional "need to know."
13. Review and take appropriate action on security violations reported by your Access Coordinators and/or reported to you by your DTCC Relationship Managers, Agent Liaisons and/or Corporate Information Security Office.
14. Review the disposal practices for sensitive documents and magnetic media at your terminal, PC and/or computer sites. Imprudently disposing of printed material (including obsolete manuals) and/or magnetic media could supply an unauthorized individual with sensitive information.
15. Periodically review the functionality assigned to each user to help ensure their access is commensurate with their processing responsibilities.
16. Prohibit the use of programs that negate the time-out features in force in DTCC's systems.

These network security precautions represent important security controls and are intended to help reinforce the importance of safeguarding your communications link(s) with DTCC. Please distribute copies of this document to all individuals who use or are responsible for administering/assessing security and controls over your company's communications link(s) with DTCC. Questions regarding controls over passwords or other network security safeguards should be directed to Diana King, Director, Corporate Information Security at (212) 855-3313 or via email at dking@dtcc.com.