

Minimum Security Requirements in a Pick/Multivalue Environment

Pick/Multivalue databases, such as D3, Universe, Unidata, jBase, etc., have security features built into them. An IT manager or business owner needs to make sure that security features are turned on and security procedures are being followed. With the passage of laws, such as the Sarbanes Oxley Act (SOA or SOX), security is being checked very carefully by auditors. Here are some suggested requirements if you are using a Pick/MultiValue database environment:

1. Log off users after a period of inactivity and especially at night. A logged on user is an open gateway into your data for individuals that are walking around your site.
2. Control access to the Terminal Control Language (TCL). At the TCL prompt, a person is capable of destroying/changing data with such commands as the ED Editor.
3. Do not allow your normal users the BREAK their session so that they can get to TCL.
4. All accounts should have passwords (especially system standard accounts) and these passwords should be periodically changed
5. Each user should have a separate login ID with a unique id and password. This way, different users can be tracked separately. Passwords should be changed regularly.
6. The ACC file should be reviewed periodically by an IT Manager or business owner to spot undesired user activity. The ACC file and its login options offer the ability to track each time a user logs in; for how long and on what port.
7. A system wide login procedure should be implemented, which is executed by all users when they log in, regardless of where they log in.
8. Educate your users on the importance of security. Constantly remind them of the need to change passwords and logging off their screens when going to lunch.
9. Make programming changes to get around some of the shortcomings of a Pick/MultiValue database such as no field-level permissions, no built-in password rules (such as how a password must be constructed) and no password aging (forcing a user to change it at various intervals).
10. Have an outside consulting company perform a yearly audit on your system security and provide recommendations for improvement.

This article focuses on database security, but physical system/network and operating system security are equally important. These are covered in other TRG articles. If you need any assistance in implementing any of the above security requirements, contact TRG at (714) 818-8112, www.picktrg or info@picktrg.com. TRG is expert at Pick/Multivalue databases.