

Re: On password expiration

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-04/msg00032.html>

- *From:* dstynchula@xxxxxxxxx
 - *Date:* 3 Apr 2006 12:51:58 -0700
-

Hi Martin,

If you are very concerned about the security of the system, simply forcing your users to change their passwords every X number of days is not going to be a viable security strategy. That's not to say it's not a really good idea, it's just that some user education is in order. The average user has no idea about information security. In order to secure the system, if the data is as sensitive as you have suggested, I would suggest implementing an account inactivity expiration time, requiring an admin to re-enable accounts that have been dormant for X numbers of days, an account lockdown policy to prevent brute force attacks, and depending on how secure your environment needs to be, an access log with someone assigned to audit login attempts periodically.

In addition, you should set some expectations regarding the handling of data as a personnel/management issue. For instance implementing an organizational policy prohibiting employees from writing down their passwords will mitigate the "sticky-notes on the VGA monitor" possibility. Ultimately, some employees may choose to disregard this instruction, but at that point you will have some accountability options.

Best Regards,

Dan Stynchula

.