ADMINISTRATIVE PASSWORD LIST MANAGEMENT

Keeping up-to-date password lists for your network is a top priority. A password list should be maintained by at least two trusted library staff and/or technology professionals. This will help maintain the accuracy of the list to ensure it is kept up-to-date.

It is recommended that a master hard-copy of the list be stored in an onsite safe accessible only by upper management. The hard copy list should be replaced after any password change. A digital copy should be kept securely in a network location accessible only to the individuals that maintain the list. The digital list should be encrypted and password protected at the local file level.

- ✓ Passwords should be changed at a minimum of every 90 days.
- ✓ In the event of a staff change, in regards to those who maintain or have access to the list, all passwords should be changed immediately.
- ✓ Lists can be created and maintained using programs such as Microsoft Excel 2007 or Microsoft Access 2007. Security options within these programs should also be used to password protect and encrypt the information.
- ✓ The list need only contain an administrative level of passwords. Individual/Personal user passwords should not be kept in the list.
- ✓ Never print the list for any reason other than replacing the Master Hard-Copy.
- ✓ When printing the Master Hard-Copy, print to a locally attached printer within sight.
- ✓ Never store the password list on removable media (i.e. USB Drives, CD-ROMs, Floppy Disks, etc.)
- ✓ Never write down passwords from the list.
- ✓ Create protected sub-lists to share with other IT staff based on their need-to-know criteria. A Microsoft administrator does not need to know the passwords to the Linux servers or Network equipment unless he/she is also the Linux/Network administrator.
- ✓ Share passwords with outside vendors or contractors on a need-to-know basis dependent on their technology responsibility for your library. In an Directory based environment, create special user accounts for vendors with their own unique user accounts allowing only privileges needed for their role. Deactivate the account when no longer used.

MINIMUM PASSWORD COMPLEXITY

The password should at least:

- Contain eight characters ***or more***
- Contain characters from ***two*** of the following ***three*** character classes:
  1. Alphabetic (a-z, A-Z)
  2. Numeric (0-9)
  3. Punctuation and other symbols (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

Password Checker: https://www.microsoft.com/protect/fraud/passwords/checker.aspx