integrated systems

How to Create a Strong Password Policy for Your Organization

Incorporate the following policies into your organization's comprehensive password policy to reduce the risk of cyber attacks against your network.

Enforce Password History
This will set how often an old password can be reused.
Recommendation starting point – 24 Passwords

Minimum Password Age
This will determine how long users must keep a password before they can change it.
Recommendation starting point – This setting is up to the organization

Maximum Password Age
This determines how long users can keep a password before they are required to change it.
Recommendation starting point – 90 Days

Minimum Password Length
This determines the minimum number of characters needed to create a password.
Recommendation starting point 8-10 characters

Passwords Must Meet Complexity Requirements
This typically means that Passwords can't contain the user name or parts of the user's full name, such as their first name. Passwords must also use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols.

Password Audit
Enabling the Password Audit policy allows you to track all password changes. By monitoring the modifications that are made it is easier to track potential security problems. This helps to ensure user accountability and provides evidence in the event of a security breach.

Administrator Password
Administrator password should be reset every 180 days for greater security.

E-Mail Notifications
This will send e-mail notifications prior to password expiry to remind your users when it's time to change their passwords before they actually expire.