Set ‘Enforce password history’ to ’24 or more password(s)’ & Set ‘Minimum password age’ to ‘1 or more day(s)’

A couple of improvements can be made to our password policy. Go through and explain why these changes are important and then outline the processes you would follow to enable and enforce the policy.

The set ‘Enforce password history’ to ’24 or more password(s)’ policy determines the number of unique new passwords that are required before an old password can be reused in association with a user’s account. Password reuse is a major concern in any organization, and a lot of employees will want to use the same password for their accounts over a long period of time for convenience. Trying to use the same password could put the organization at risk and completely defeats the purpose of resetting and cycling passwords. This also makes brute force attacks much easier for attackers to get into an account. It is also possible that old passwords could be exposed in a data breach and attackers will have much more success if there is no enforcement for password history. Enforcing a longer password history will make it less convenient to cycle back to the old password and make an employee’s account much more secure.

Setting the minimum password age to 1 or more day(s) determines the number of days that you must use a password before you can change it, 1 day in this specific policy. This policy works well with the enforcing password history policy. The two policies together make it so that employees can’t just change their password, change it as many times as the

password history policy enforces, then change it back to their old password again in a matter of minutes. They won't be able to do that if they need to have their password for at least a day. If they wanted to wait and reset to their old password, then it would take a minimum of 25 days with both policies in place. These changes would encourage employees to come up with unique passwords from the first reset because it would be more convenient than waiting 25 days to switch back to the old password.

To enable and enforce this policy I would start by sending a message out to all effected users a couple weeks before actually implementing the new policies. I'd let them know what policy is changing, why this policy is changing, new guidelines that I'd like them to follow, and the exact date that it's supposed to take effect. Then as that date comes around, I would like to enforce the policy in groups instead of making everybody change all at once. This makes it so that in the event that everybody is having trouble with it then it wouldn't be the whole organization asking IT for help, but it would be smaller groups at a time. This makes it more manageable for IT and makes help more accessible to all the employees who are going through this policy change. After the policy is completely rolled out to all employees then I would monitor any tickets or lockouts that are related to the policy. Then adjust the policy if employees are having a really hard time with it.

To change these password settings I will need to enforce them through Group Policy. To get to group policy editor I will need to press Windows + R to open the run command. From there I will type "gpedit.msc" to open the Local Group Policy Editor. Then navigate to

Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy. In this group policy editor, I can change the policies regarding password history and minimum password age. I am also able to change other things like maximum password age, minimum password length, minimum password length audit, password must meet complexity requirements, relax minimum password length limits, and store passwords using reversible encryption. The “Enforce password history” needs to be changed from 5 passwords remembered to 24 passwords remembered. The “Minimum password age” needs to be changed from 0 days to1 day.