Student: Tania Diaz
Date: 09/27/25
Course: CIST-2881-D1
Assignment: Group Policies for Security

Introduction

Group Policies are settings in Windows that let administrators control how computers and users behave on a network. They are really important for keeping computers safe from hackers and stopping people from accidentally (or intentionally) doing things they shouldn't. In this assignment, I researched ten Group Policies that help improve security, explained what they do, and why they are used.

10 Security Group Policies

1.- Account Lockout Policy. This policy locks a user account if someone tries to log in with the wrong password too many times. It is used to prevent hackers from guessing passwords and to protect user accounts from unauthorized access.

2.- Password Complexity Requirements. This policy requires users to create passwords that include uppercase letters, lowercase letters, numbers, and symbols. It makes passwords harder to guess and keeps accounts more secure.

3.- Minimum Password Length. This policy sets a minimum number of characters for passwords. Longer passwords are harder to crack, which increases security.

4.- Audit Object Access. This policy tracks when users access files, folders, and other system objects. It is used so administrators can monitor if anyone is trying to access files they shouldn't.

5.- User Rights Assignment Deny Logon Locally. This policy prevents certain accounts from logging in on specific computers. It helps protect important computers from unauthorized use.

6.- Windows Firewall Rules via GPO. This policy sets firewall rules on all computers in the network. It protects computers from network attacks and makes sure all systems have the same security settings.

7.- Software Restriction Policies / AppLocker. This policy controls which programs users are allowed to run. It helps prevent users from accidentally or intentionally running dangerous or unauthorized software.

8.- Disable USB Drives / Removable Storage. This policy blocks USB drives and other removable devices. It reduces the risk of malware spreading and prevents data theft.

9.- Enforce Screen Saver Lock. This policy automatically locks a computer after a period of inactivity. It protects the computer when someone walks away without logging out.

10.- User Account Control (UAC). This policy asks for administrator approval when changes are made to the system. It prevents unauthorized changes and protects against malware.

Conclusion

These Group Policies help keep computers and networks safe. Each one protects against different security threats, like hackers, malware, and unauthorized access. Using Group Policies makes sure all computers in the network follow the same rules, which is important for keeping data and systems secure.

References

- **Microsoft Learn**. *Group Policy Overview for Windows Server*. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview

- **Microsoft Learn**. *Security Baselines Guide*. https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines

- **Microsoft Learn**. *Group Policy Settings Reference Spreadsheet for Windows Server 2022*. Retrieved from https://www.microsoft.com/en-us/download/details.aspx?id=104005

- **Microsoft Learn**. *System Audit Policy Recommendations*. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

- **Microsoft Learn**. *Group Policy Management Console*. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-management-console