# **Module 4 Homework 4: 10 Common/Useful Group Policies**

**Part 1: Researching AD Group Policies on Microsoft Learn**

Microsoft Learn provides valuable documentation and resources on Active Directory Group Policies. It's a trusted source for IT professionals looking to understand and implement these policies effectively. The documentation at the provided link offers comprehensive information on configuring and managing Group Policies in Windows Server environments.

**Part 2: Gathering Insights from the Community**

While Microsoft Learn is an excellent source for official documentation, it's also beneficial to gather insights from the IT community regarding their favorite and most useful Group Policies. Many IT professionals and administrators share their experiences and recommendations on various forums, blogs, and community websites. These insights can help in understanding the practical applications and real-world benefits of different Group Policies.

**Part 3: Identifying the 10 Most Useful Group Policies**

In an enterprise environment, there are numerous Group Policies available, each serving a specific purpose. Here are my picks for the 10 most useful Group Policies, along with their definitions and benefits:

Password Policy (Password Policy): This policy defines password complexity requirements, including length, complexity, and expiration. It enhances security by ensuring strong passwords are used.

Account Lockout Policy (Account Lockout Policy): This policy determines the number of failed login attempts before an account is locked. It helps protect against brute force attacks.

Software Installation (Software Installation): This policy allows administrators to deploy and manage software installations across the network, ensuring consistent software configurations.

Folder Redirection (Folder Redirection): This policy redirects user folders (e.g., Documents, Desktop) to network locations, enhancing data backup and centralization.

Group Policy Preferences (Group Policy Preferences): It provides advanced configuration options, allowing administrators to map network drives, set local admin passwords, and more.

Security Options (Security Options): This policy lets administrators configure security settings such as account policies, user rights assignments, and security options for computers.

Windows Firewall (Windows Firewall with Advanced Security): This policy controls Windows Firewall settings, allowing administrators to define inbound and outbound traffic rules.

Audit Policy (Audit Policy): It enables auditing of various events, providing visibility into system and security-related activities for compliance and security monitoring.

Internet Explorer Maintenance (Internet Explorer Maintenance): Useful for managing Internet Explorer settings, ensuring consistent browser configurations.

Remote Desktop Services (Remote Desktop Services): This policy governs Remote Desktop access, allowing administrators to control remote connections to servers and workstations.

These Group Policies are crucial for maintaining security, user productivity, and network management in an enterprise environment. They provide granular control over various aspects of the Windows environment, ensuring that the organization's IT infrastructure remains efficient and secure.

**References:**

Jithukrishnan. (n.d.). *Top 10 password policy recommendations for system administrators in 2023*. Securden. Retrieved September 17, 2023, from https://www.securden.com/blog/top-10-password-policies.html#:~:text=Addin