- • Where many of the basic system changes and configurations can be made with a Windows operating system **Click Start-> Control Panel**
- Controls security settings on user computers within a network **Click System and Security → Administrative Tools → Local Security Policy**
- Modify policies to require users create strong passwords - Remember CLOUDS Not SUN (Unit Four) **Click Account Policies → Password Policies**

Policies:	Recommended settings:
Password history: the number of old passwords the computer remembers and does not allow a user to reuse	5 passwords remembered
Maximum password age: how long a user can keep the same password	90 days for users, 30 for admins
Minimum password age: how long a user must keep a password before changing it	10-30 days
Minimum password length: how many characters passwords must be	8 characters
Complexity requirements: whether users must use at least three of the following in their passwords: upper case letters, lower case letters, numbers, symbols	Enable
Reversible encryption: whether the password file on the computer can be decrypted	Disable

- Even if you have the strongest password possible, if you give hackers unlimited attempts to break it, they eventually will. Account policies govern unsuccessful attempts to log into an account. **Click Account Policies → Account Lockout Policies**
- Notifies you if Windows identifies problems with or updates for: - Windows Updates - Internet security settings - Network firewall - Spyware and related protection - User Account Control - Virus protections - Windows Backups - Windows Troubleshooting. **Click Start → Control Panel → System and Security → Action Center**
- Anti-malware programs should be updated regularly. Windows Defender is a very basic built-in spyware protection program on Windows - It only protects against known spyware, not viruses, worms or other malware. Download a supplementary antivirus program - Windows offers a free program called Windows Security Essentials - If you choose a different anti-malware program, disable Windows Defender first to avoid compatibility issues. **Control Panel->System and Security->Action Center**
- Reject or allow data packets through to users based on custom settings. Essential to security and should always be turned ‘on’. **Control Panel → System and Security → Action Center → Turn on now.**
- Allow trusted programs to connect without being blocked by adding them to your Windows Firewall Exceptions list. For each network type, you can customize whether you want the programs allowed through.It’s much safer to allow only certain programs through your firewall than to open an entire port to traffic.Ports are numbers that identifies one side of a connection between two computers. **Control Panel->System and Security->Windows Firewall.**
- Prevent or fix known problems in Windows software or improve user experience.Should be installed regularly.To avoid missing updates, allow Windows Update to check for them daily and install them automatically. **Control Panel->System and Security->Windows Update.**

- Windows categorizes accounts as user or administrator accounts so that it can automatically apply the relevant permissions and rights. Define a user's level of access by categorizing his or her account as a user or administrator. To set up the Local Users and Groups Console: **Start Menu->Search "mmc"->Click "yes" to allow changes to computer->Click File->Add or Remove Snap-ins->Select "Local Users and Groups-> When prompted, select "Add to Local Computer".**