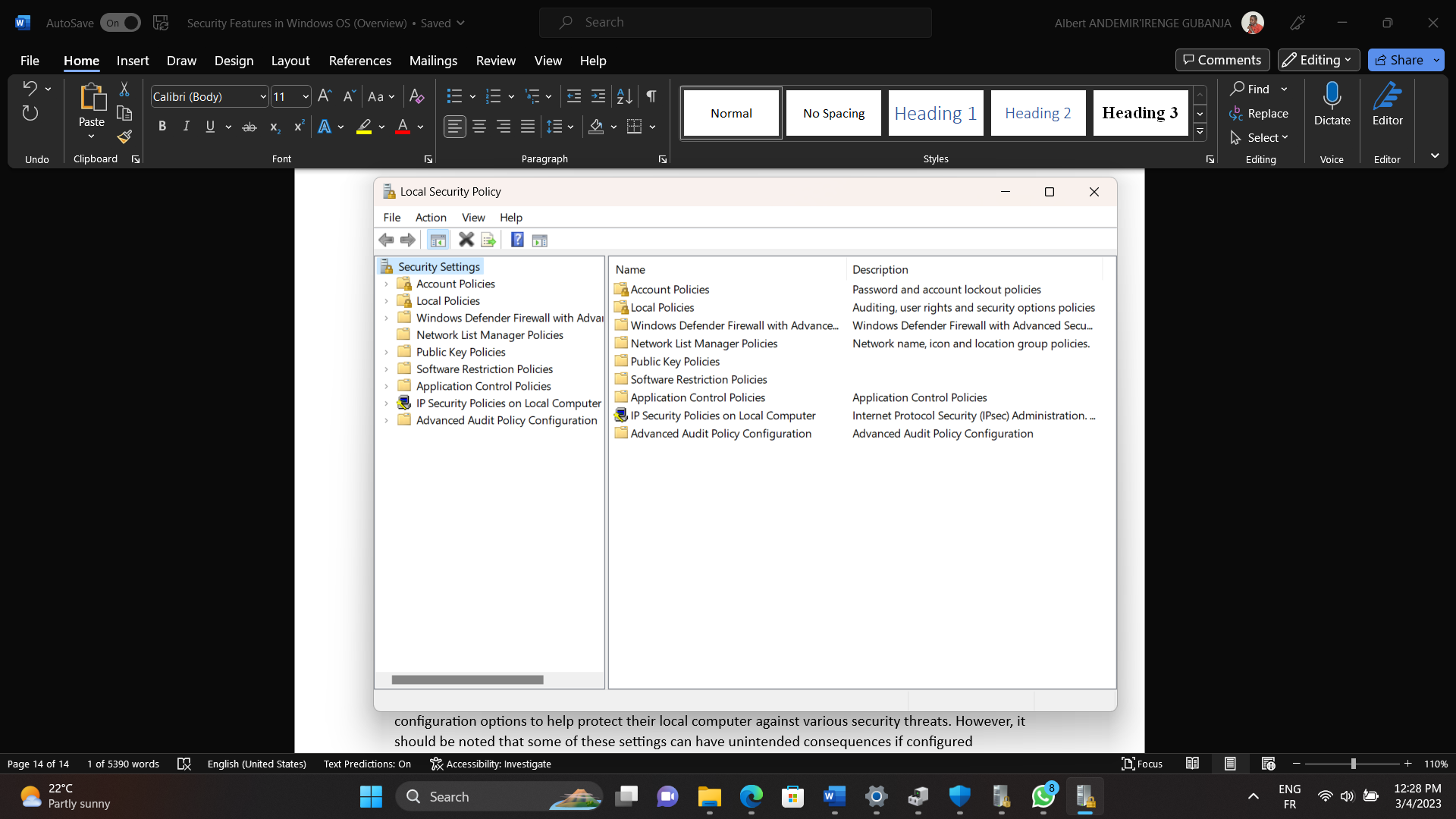
**Local Security Policy in Windows 11**

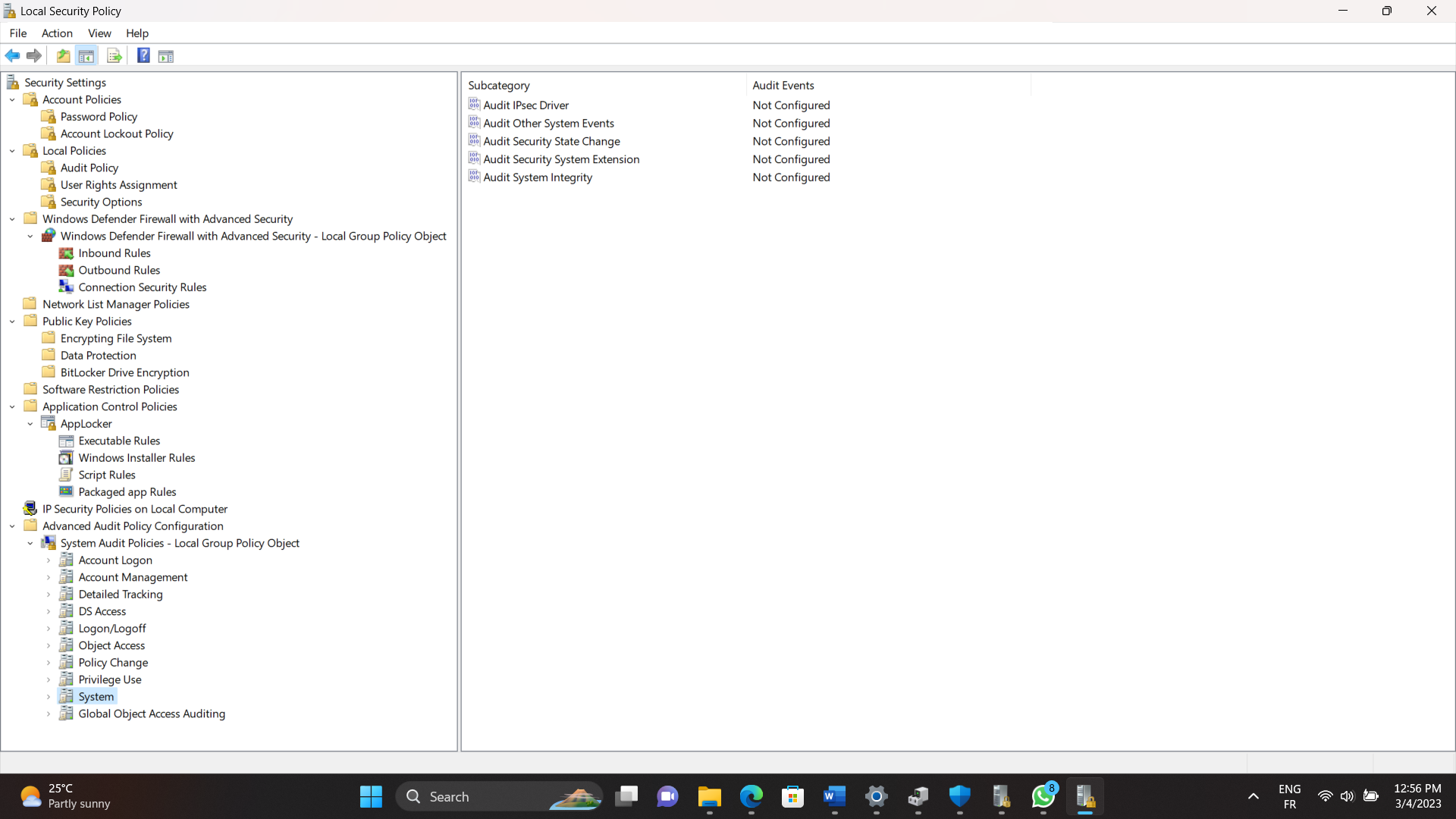
Local Security Policy in Windows 11 is a tool that allows users to configure security settings on their local computer. It is a part of the Microsoft Management Console (MMC) and can be accessed by typing "secpol.msc" in the Run dialog box or by searching for it in the Start menu.



Using the Local Security Policy tool, users can configure a wide range of security settings, including password policies, account lockout policies, user rights, security options, audit policies, and more. These settings can help improve the security of a computer and protect it against various security threats.

There nine categories of the features and options available in the Local Security Policy tool in Windows 11.

1. Account Policies: This section allows users to configure password policies, account lockout policies, and Kerberos policies. Users can set password complexity requirements, minimum password length, maximum password age, account lockout duration and threshold, and more.
2. Local Policies: This section contains a variety of security options that can be configured, including user rights, security options, audit policies, and more. Users can enable or disable certain features or behaviors, set security options such as network security, and configure audit policies to log various security events.
3. Windows Defender Firewall with Advanced Security: Windows Defender Firewall with Advanced Security is a set of security policies that can be configured using the Local Security Policy tool in Windows 11. These policies allow users to manage and customize the firewall settings on their computer, helping to prevent unauthorized access to their network.
4. Network List Manager Polices: The Network List Manager Policies are a set of security policies that can be configured using the Local Security Policy tool in Windows 11. These policies allow users to control the behavior of the Network List Manager service, which is responsible for detecting and managing network connections on a Windows computer.
5. Public Key Policies: Public Key Policies are a set of security policies that can be configured using the Local Security Policy tool in Windows 11. These policies are related to public key cryptography and digital certificates, which are used to secure communication and verify the identity of users and systems in a network.
6. Software Restriction Policies: Software Restriction Policies (SRP) are a set of security policies that can be configured using the Local Security Policy tool in Windows 11. These policies allow users to control which software can be run on their computer, based on factors such as file path, publisher, or hash value.
7. Application Control Policies: Application Control Policies are a set of security policies that can be configured using the Local Security Policy tool in Windows 11. These policies allow users to control which applications can run on their computer, based on factors such as file hash, file path, publisher, or other criteria.
8. IP Security Policies on Local Computer: IP Security (IPSec) Policies are a set of security policies that can be configured on a Local Computer using the Local Security Policy tool in Windows 11. IPSec policies help to secure network communications by providing authentication, integrity, and confidentiality for IP packets.
9. Advanced Audit Policy Configuration: Advanced Audit Policy Configuration is a set of security policies that can be configured using the Local Security Policy tool in Windows 11. These policies allow users to audit specific events on their computer or network, helping to monitor for security breaches and other issues

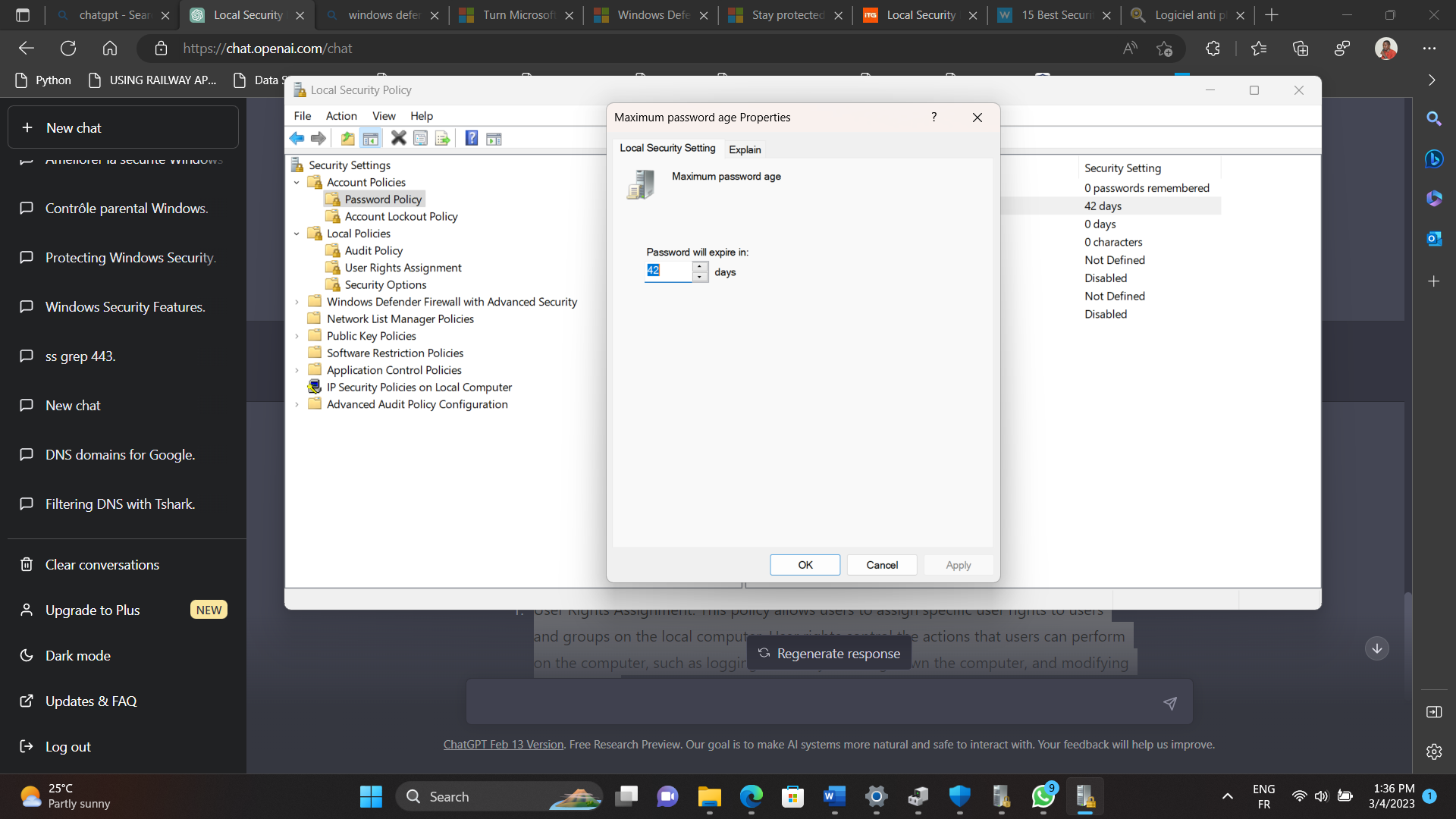


Let us go through the two key features of the Local Security Policy tool: Account Policies and Local Policies:

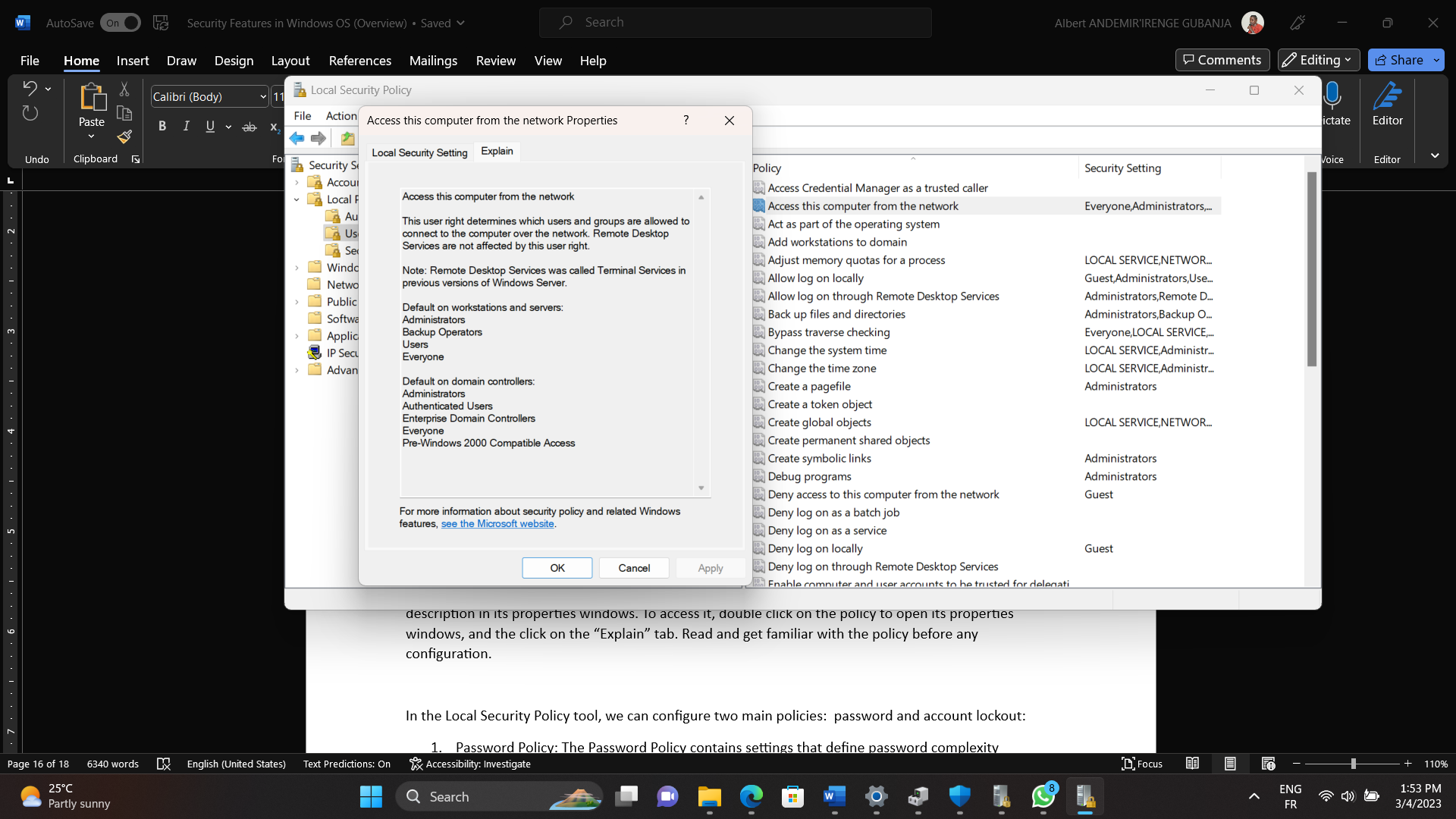
* + - 1. **Account Policies**

Account policies are an important component of the Local Security Policy tool in Windows 11. They allow users to define password and account lockout policies for local user accounts. By configuring account policies, users can help ensure that their local user accounts are secure and protected against unauthorized access. Note that these policies should be carefully configured to avoid unintended consequences, such as users being locked out of their accounts due to too many failed login attempts or password requirements that are too complex for users to remember.

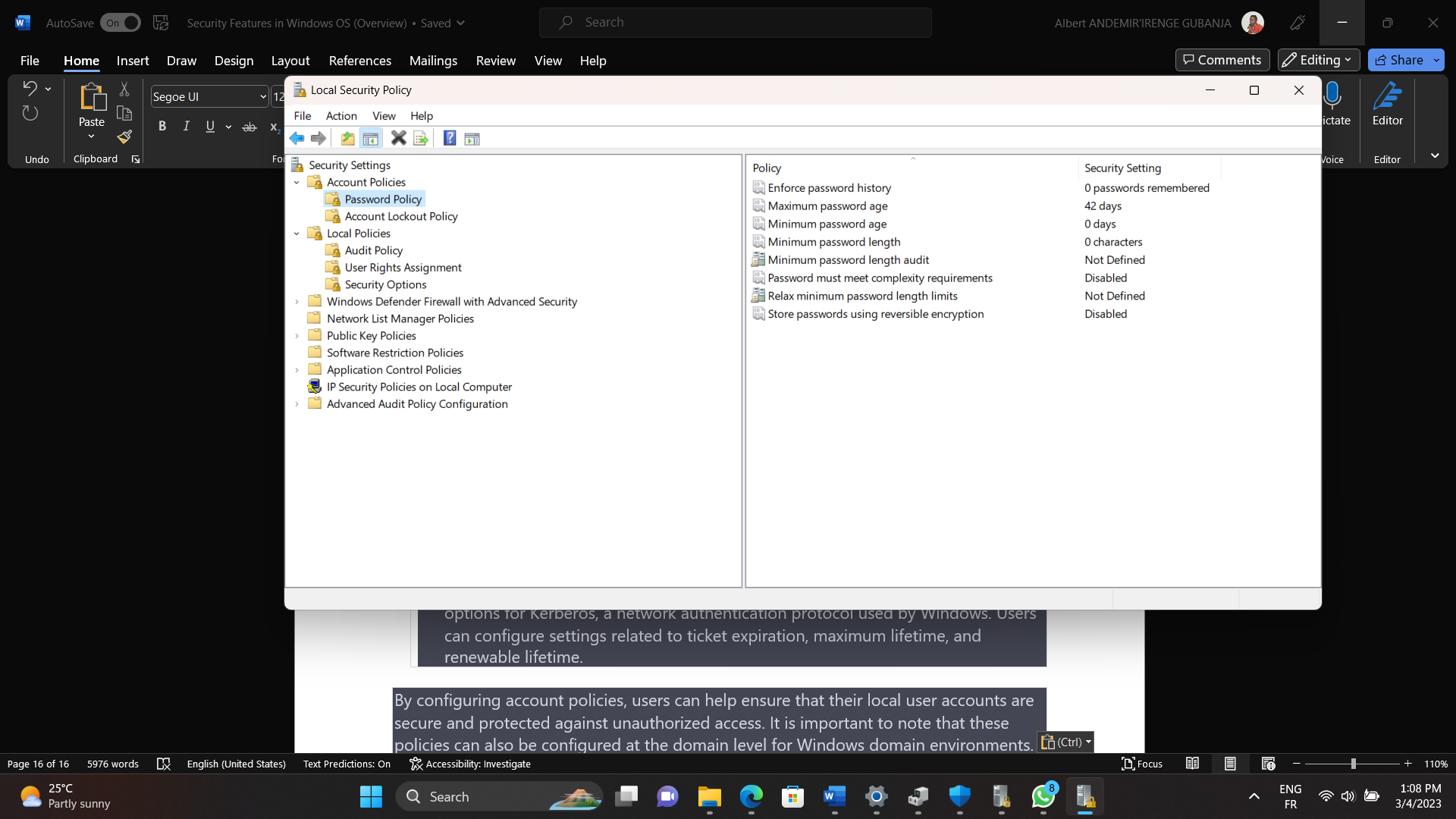
To define or edit a policy, double-click on the policy to open its properties window, define or make changes and click on “Apply” and then “OK” to save.



Note: It is important to be familiar with every policy before any configuration. Every policy has a detailed description in its properties windows. To access it, double click on the policy to open its properties windows, and the click on the “Explain” tab. Read and get familiar with the policy before any configuration from the policy settings tab.



In the Local Security Policy tool, we can configure two main policies: password and account lockout:

1. Password Policy: The Password Policy contains settings that define password complexity requirements, password length, and password age. Users can define policies that require users to use strong passwords that include a combination of uppercase and lowercase letters, numbers, and special characters. They can also set the minimum length of a password and the length of time before a password expires and must be changed. 
2. Account Lockout Policy: The Account Lockout Policy contains settings that define the conditions under which a user account will be locked out due to repeated failed login attempts. Users can set the number of failed attempts that will trigger an account lockout and the duration of the lockout period.

Graphical user interface, text, application

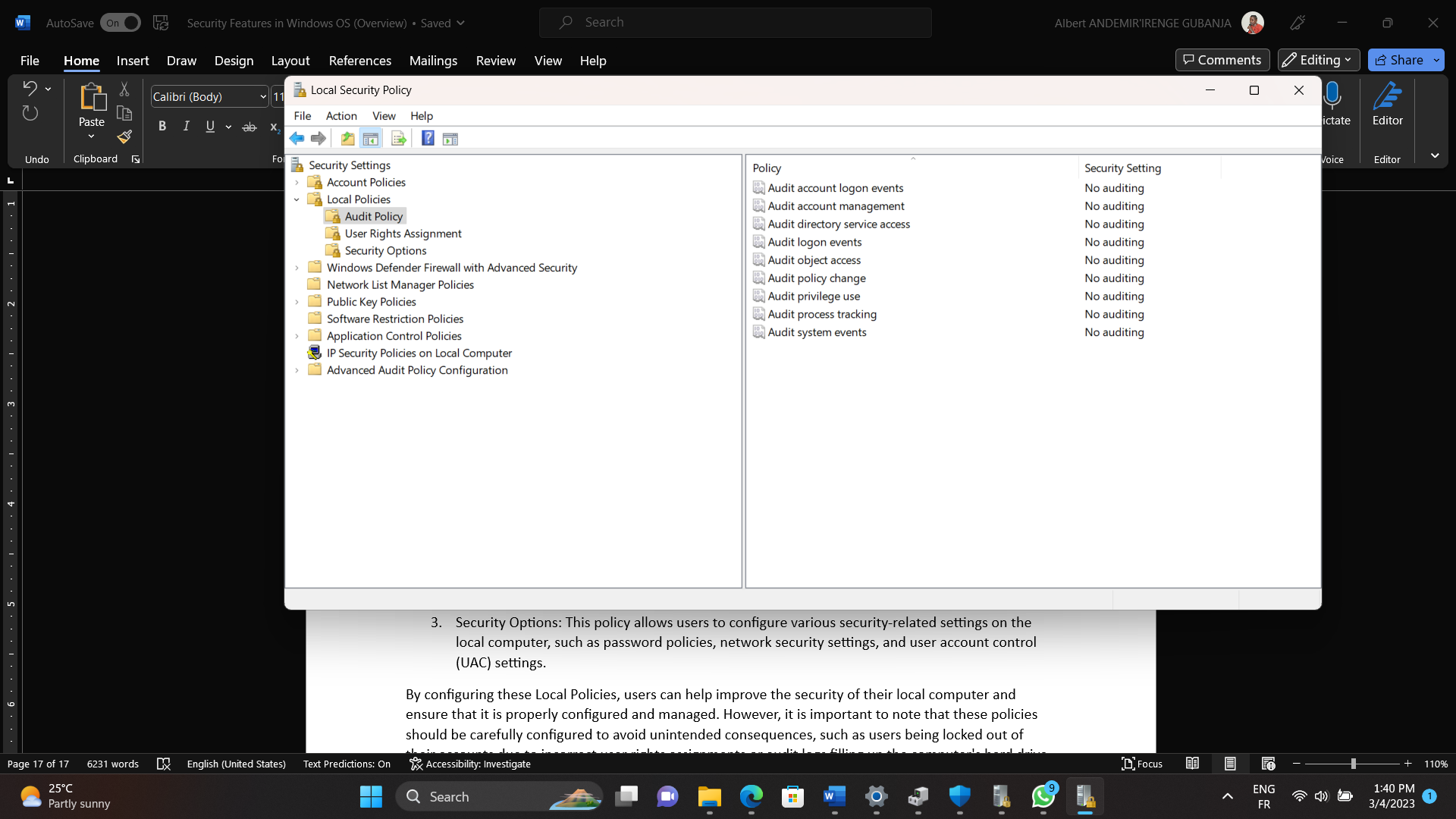
Description automatically generated

Note: It is important to note that these policies can also be configured at the domain level for Windows domain environments.

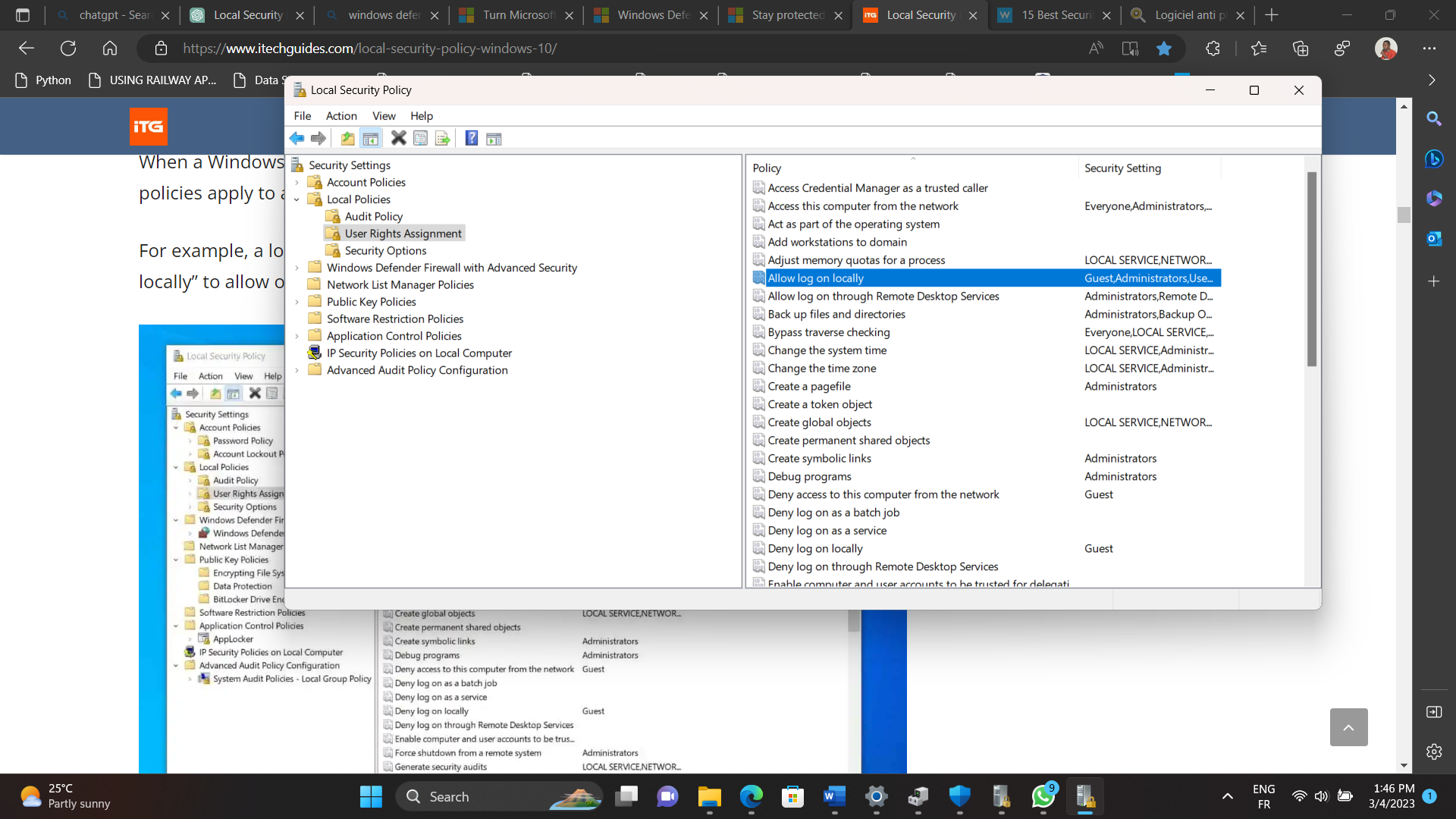
* + - 1. **Local Policies**

Local Policies are a set of security policies that can be configured using the Local Security Policy tool in Windows 11. These policies allow users to manage various aspects of the local computer's security, including user rights, audit policies, and security options.

1. Audit Policy: This policy allows users to configure the audit settings for various security events on the local computer. For example, users can configure the computer to log events such as logon and logoff attempts, file and folder access, and system shutdowns.



1. User Rights Assignment: This policy allows users to assign specific user rights to users and groups on the local computer. User rights control the actions that users can perform on the computer, such as logging on locally, shutting down the computer, and modifying system time. For example, a local administrator may modify the Local Security Policy, “Allow Log on locally” to allow only administrators to log on to the computer. This policy will be enforced on the local computer. So, when a non-administrator tries to log in to the computer, the computer will deny the user access.



1. Security Options: The security options are many. They allow users to configure various security-related settings on the local computer, such as password policies, network security settings, and user account control (UAC) settings. You can go through each policy to learn about and make right security configurations for your computer.

By configuring these Local Policies, users can help improve the security of their local computer and ensure that it is properly configured and managed. However, it is important to note that these policies should be carefully configured to avoid unintended consequences, such as users being locked out of their accounts due to incorrect user rights assignments or audit logs filling up the computer's hard drive.

Overall, the Local Security Policy tool in Windows 11 provides users with a powerful set of security configuration options to help protect their local computer against various security threats. However, it should be noted that some of these settings can have unintended consequences if configured improperly, so users should exercise caution and carefully review any changes before implementing them. If your computer belongs to a Windows network or domain, the IT administrator can apply some of the security policies from the server. In a domain network, the IT administrator will apply these policies using a “Group Policy”, available also in windows 11.