1.0) AIM: Explore Security Features of Windows OS.

2.0) Objective:

To understand how built-in Windows security features (User Accounts, UAC, Firewall, and Antivirus) help protect an Information System.

3.0) SCOPE:

- This practical covers **basic security mechanisms** provided by Windows OS.
- It helps to **explore real-world system protections** that prevent unauthorized access, malware infections, and misuse of applications.
- The knowledge gained is applicable for **personal computers, enterprise systems, and cyber hygiene practices**.

4.0) FACILITIES/ APPARATUS:

- **Windows OS**

5.0) THEORY

In modern operating systems, security features are essential for protecting the confidentiality, integrity, and availability of data.

Windows provides several built-in tools for this purpose:

User Accounts & UAC (User Account Control)

Multiple user accounts (Administrator, Standard User, Guest) help in access control.

UAC prompts for admin approval before critical system changes, thus preventing malware from silently installing software.

Windows Defender Antivirus

Provides real-time protection against viruses, malware, spyware, and ransomware.

Regular scans and definition updates ensure continuous defense.

Windows Firewall

A network security feature that monitors and controls incoming/outgoing traffic.

Blocking specific applications prevents them from accessing the internet, reducing risk of unauthorized communication.

Event Viewer (Security Logs)

Logs every significant security event (logon attempts, privilege escalation, blocked applications).

Useful for auditing and forensic investigation in case of security breaches.

These features together provide a layered security model, ensuring that even if one control is bypassed, others continue to protect the system.

Task 1 – User Account & UAC

Open Control Panel → User Accounts.

Create a new Standard User account.

Try installing software from this account → Windows will ask for Administrator password.

Observe how UAC (User Account Control) prevents unauthorized installations.

Task 2 – Windows Defender Antivirus

Open Windows Security → Virus & Threat Protection.

Run a Quick Scan of the system.

Show students how to check the Scan History and quarantined items.

Task 3 – Windows Firewall: Block an Application (Chrome/Edge)

Open Control Panel → Windows Defender Firewall → Advanced Settings.

Go to Outbound Rules → New Rule.

Select Program → Browse → chrome.exe (or msedge.exe).

(Default path: C:\Program Files\Google\Chrome\Application\chrome.exe)

Select Block the connection → Finish.

Try to open Chrome/Edge → It opens but no website loads.

Now disable or delete the rule → Browser works normally again.

Task 4 – Observing Security Logs

Open Event Viewer (eventvwr.msc).

Go to Windows Logs → Security.

Check entries for failed logins or blocked application.

We will observe how Windows security features (UAC, Antivirus, Firewall, Logs) protect the system.

6.0) CONCULSION:

This practical demonstrates that built-in Windows security features form the first line of defense in safeguarding information systems.

By performing these tasks, we gain hands-on experience in applying preventive, detective, and corrective security measures — an essential foundation for Information Security management.