Requirements

Requirement	Security Property	Implemented By
Only teachers & principal can view grades	Confidentiality	Local groups + NTFS
Grades not modified by unauthorized users	Integrity	Permissions + Auditing
Teachers can access when needed	Availability	Backups + Stable access
Strong password usage	Preventive Control	Password policy

Three Security Properties (CIA Triad)

1 Confidentiality

Only assigned teachers and the principal can view the grades.

Meaning:

Confidentiality ensures that sensitive information is accessible **only to authorized users**.

Applied here by:

- Local security groups
- NTFS permissions
- Restricted file sharing

2 Integrity

Grades cannot be changed by students or unauthorized persons during storage or transfer.

Meaning:

Integrity ensures that data is **not altered without authorization**.

Applied here by:

- Write permissions limited to teachers
- No access for students
- Auditing of changes

3 Availability

Teachers can access the system whenever they need to input final marks.

Meaning:

Availability ensures data and systems are **accessible when needed**.

Applied here by:

- Backups
- Proper permissions (no accidental lockout)
- Stable local access

The Primary Role of Non-Technical Staff

The **primary role of staff** is **compliance**.

They must:

- Follow school security policies
- Use strong passwords
- Protect login credentials
- Access only data needed for their job
- Report suspicious behavior or incidents

Step 1 — Create Local Security Groups

```
PS C:\WINDOWS\system32> New-LocalGroup -Name "Grades_Teachers"
>> New-LocalGroup -Name "Grades_Principal"

Name             Description
----             -----------
Grades_Teachers
Grades_Principal
```

The Grades_Teachers are allowed to access and modify grades

The Principal has full control over grades

Step 2 — Create Local User Accounts

```
PS C:\WINDOWS\system32> New-LocalUser "teacher1" -Password (Read-Host -AsSecureString) -FullName "Teacher One"
>> New-LocalUser "principal1" -Password (Read-Host -AsSecureString) -FullName "School Principal"


Name       Enabled Description
----       ------- -----------
teacher1   True
principal1 True
```

Add users to groups:

```
PS C:\WINDOWS\system32> Add-LocalGroupMember -Group "Grades_Teachers" -Member "teacher1"
>> Add-LocalGroupMember -Group "Grades_Principal" -Member "principal1"
>>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Get-LocalGroupMember -Group "Grades_Principal"
>>

ObjectClass Name                      PrincipalSource
----------- ----                      ---------------
User        DESKTOP-KG1AC6E\principal1 Local


PS C:\WINDOWS\system32> ^C
PS C:\WINDOWS\system32> Get-LocalGroupMember -Group "Grades_Teachers"

ObjectClass Name                     PrincipalSource
----------- ----                     ---------------
User        DESKTOP-KG1AC6E\teacher1 Local
```

Step 3 — Create the Secure Grades Folder

```
PS C:\WINDOWS\system32> New-Item -Path "C:\StudentRecords\Grades" -ItemType Directory -Force
>>


    Directory: C:\StudentRecords


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        12/31/2025   3:40 PM                Grades
```

Step 4 — Apply NTFS Permissions

First we must Remove inherited and public permissions

```
>> icacls $path /inheritance:r
>> icacls $path /remove "Users" "Everyone" "Authenticated Users"
processed file: C:\StudentRecords\Grades
Successfully processed 1 files; Failed processing 0 files
processed file: C:\StudentRecords\Grades
Successfully processed 1 files; Failed processing 0 files
PS C:\WINDOWS\system32> $path = "C:\StudentRecords\Grades"
>> icacls $path /inheritance:r
>> icacls $path /remove "Users" "Everyone" "Authenticated Users" 2>$null
>>
processed file: C:\StudentRecords\Grades
Successfully processed 1 files; Failed processing 0 files
processed file: C:\StudentRecords\Grades
Successfully processed 1 files; Failed processing 0 files
PS C:\WINDOWS\system32> icacls $path /grant "Grades_Teachers:(OI)(CI)M"
>> icacls $path /grant "Grades_Principal:(OI)(CI)F"
>>
processed file: C:\StudentRecords\Grades
Successfully processed 1 files; Failed processing 0 files
processed file: C:\StudentRecords\Grades
Successfully processed 1 files; Failed processing 0 files
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> icacls C:\StudentRecords\Grades
>>
C:\StudentRecords\Grades DESKTOP-KG1AC6E\Grades_Principal:(OI)(CI)(F)
                         DESKTOP-KG1AC6E\Grades_Teachers:(OI)(CI)(M)

Successfully processed 1 files; Failed processing 0 files
PS C:\WINDOWS\system32>
```

NTFS permissions were configured using PowerShell. Permission inheritance was disabled, default public groups were removed, and role-based access was enforced by granting Modify rights to the Grades_Teachers group and Full Control to the Grades_Principal group. This implementation ensures confidentiality and integrity of student grades.

Integrity During Data Transfer

Integrity and Confidentiality During Transfer

To protect student grades while being accessed over the network, secure file sharing mechanisms must be used. File transfer integrity is ensured by restricting access to authorized users only and enabling encrypted file sharing. This prevents unauthorized modification or interception of data while it is being transmitted.

Applied by:

- Restricted SMB file sharing
- Encrypted network access
- Controlled user permissions

This ensures that grades cannot be altered or intercepted during transfer

.

Verification of Security Controls

Verification of Access Controls

After configuring permissions, verification is required to ensure security controls are correctly applied.

Verification steps include:

- Checking NTFS permissions to confirm only authorized groups have access
- Verifying group membership for teachers and principal
- Confirming that public user groups do not have access