

## IST 251 – Chapter 8 – NTFS Permissions

NTFS Permissions are rules associated with file system objects such as files and folders that specify which users can gain access to an object and in what manner.

You can specify which users and/or groups can access files and folders and what they can do with the contents of the file or folder.

NTFS Permissions is different than Share permissions in that it doesn't matter whether the user access the file at the console or over the network.

### NTFS Folder Permissions

1. **Full Control** – enables users to change folder permissions, take ownership, delete subfolder or files plus perform actions permitted by all other NTFS Folder Permissions
2. **Modify** – delete the folder, plus perform all actions permitted by the Write permission and Read & Execute permission.
3. **Read & Execute Permission** – browse through folders, execute programs in those folders, and perform all permissions in the Read, and the List folder contents permission
4. **List Folder Contents** – See the names of the files and subfolders in the folder
5. **Read** – see the files and subfolders in the folder and view the folder ownership, permissions, and file system attributes
6. **Write** – Create new files and subfolders within the folder, change the folder attributes, and view the folder ownership and permissions

**Denying permissions.** You can explicitly deny permission to a user or group. Any Denying permissions override the permission assignments that the user or group has inherited from a parent folder.

### NTFS File Permissions

1. **Full Control** – change file permissions and take ownership of files, plus performs the actions permitted by all of the other NTFS File permissions
2. **Modify** – Modify and delete the file, plus perform all of the actions permitted by Write permission and the Read & Execute permission
3. **Read & Execute permission** – run applications, plus perform all of the actions permitted by the read permission
4. **Read** – Read the file and view the file's attributes, ownership and permissions
5. **write** – overwrite the file, change the file attributes and view the file's ownership and permissions

**ACL – Access control List** – contains a list of all user accounts and groups that have been granted or denied access to the file or folder, as well as the type of access that they have been granted or denied.

**ACE – Access control Entry** – an entry in the ACL for the user account or group. If no ACE exists the user cannot gain access to the resource.

**Permissions are cumulative.**

**File permissions override folder permissions.**

**Deny overrides all other permissions.**

**Inheritance** – by default, the permissions that you assign to a folder are inherited by all subfolders and files. This can be prevented.

Special permissions provide the administrator with additional level of access control.

**SEE CHART on page 295-296**

**You cannot assign anyone ownership of a file or folder.**

**Effective Permissions** – the Sum of all NTFS permissions that you assigned the individual user account or to the groups which the user belongs.

**UNC – Universal Naming Convention** – Network path to the device

**Taking ownership of a folder – Do assignment**