Customizing Permissions

Objectives:

At the end of this episode, I will be able to:

1. Describe how file permissions are maintained in macOS.
2. Define the standard POSIX permissions used in UNIX-based operating systems.
3. Configure access control lists to restrict access to folders and files.

> Additional resources used during the episode can be obtained using the download link on the overview episode.

- Files and folders are assigned permissions to control user access
- Allows multiple users to store data on the same drive safely and securely
- Permissions are managed in three methods:

  1. Owner

     - The person who created the file
     - Has complete access to the file by default
     - Can be changed to another user
     - Defaults to *Read & Write*

  2. Group

     - A collection of users granted access to the file based on their membership in a group
     - In Mac OS all users are added to a group named "staff" by default so you see will it most often
     - Defaults to *Read Only*

  3. Everyone (Other)

     - The permissions apply to everyone else
     - Any user who does not fit in #1 or #2
     - Guest
     - Sharing Users
     - Defaults to *Read Only*

- Permissions can be accessed in the finder by:

  - `Command-I -> Sharing & Permissions`
  - Allows viewing and changing the permissions

- Permission Inheritance

  - Folder permissions apply to child objects by default
  - Can be overridden if desired

- Permission Definitions

  - Read & Write

    - Applies to files and folders
    - Allows reading of any content in a file/folder
    - When applied to a folder, indicates the folder contents can be listed, and new items can be created
    - When applied to a file, indicates data may be appended

  - Read Only

    - Applies to files and folders
    - Allows reading of any content in a file/folder
    - when applied to a folder, indicates the folder contents can be listed

- Write Only
  - Applies only to folders
  - Used for *drop boxes*
  - A drop box is a folder someone can add contents to, but cannot retrieve those same contents later on.
  - Read permissions are not granted
- No Access
  - Applies to files and folders
  - Indicates permission denied
  - Cannot read, write or list contents
- Execute
  - Applies only to files
  - Not visible in the GUI
  - Indicates that a user may "execute" an application or script
  - Mainly used for applications launched from the terminal
  - Native macOS applications are managed by the OS
- Access Control Lists
  - Normal permissions are limited to User, Group and Other (Everyone)
  - ACLs allow adding permissions beyond the standard Unix UGO method
  - Can add multiple users and groups
  - From the GUI
    - Use the +/- buttons to add and remove users and groups to the list