Why should the directory of one user not be generally accessible to other users (not even for read-only access)?

Step 1:

The ability to read, write, alter, delete, or otherwise access a computer file; change configurations or settings; or add or remove applications is known as having access rights.

Step 2:

The majority of networks will be configured with "access rights." This indicates that the administrator has granted specific files and directories access to each user who can log on. For instance, you might have access to a personal folder where you are able to add, edit, and delete files.

The idea of limiting user, account, and computing process access permissions to only those resources that are absolutely necessary to carry out regular, legal actions is known as least privilege. The word "privilege" itself refers to the right to avoid a certain security measure.

User access rights are unique to each user.

User-based access, often known as user-based permissions, is a technique for protecting software and its functionality on a per-user basis. A straightforward login and password combination that either gives or refuses access is the most fundamental type of user-based access. A feature of more sophisticated software systems is the ability to give users particular permissions.

Look for software that has user-based access as a feature if you want to be able to determine exactly which areas of a database or software system each employee can access. Companies with security concerns or responsibilities that require a lot of flexibility in the team would probably choose this kind of authorization arrangement.