Access Controls

Access control is needed to restrict access to resources, such as files, folders, applications & physical resources. Access control on computers has three main areas, authentication, authorisation and audit.

We looked at authentication in the lesson “User Authentication”. However just authenticating the user isn’t enough.

Once a user is authenticated this will authorise them to access certain resources. This includes the files that they can access (and what level of access), the software they can access, and the functionality they can perform (such as installing software).

Organisations should work on the “principle of least privilege”. This means users can only access the data, software and functionality they need to do their job.

Finally, after authorisation there is audit. We will maintain an audit log of how users use the network, including when and where. This can ensure appropriate use and help identify where a threat has occurred.

Further Thought

Research the different types of file permission a user can be assigned to files & folders. Also, what privileges are usually restricted to the average user in an organisation?