9.4 Access Control

An important area of security policies that usually generates controversy in any organisation is access control. There is always a conflict between users' desire for unrestricted access to any data or resources on the network and the security administrator's desire to protect that data and resources. You cannot simply lock down every resource completely as this would block the users' access to those resources. Conversely, you cannot simply allow anyone and everyone complete access to everything.

It is worth keeping this acronym in mind when thinking about access control. Your goal is to make sure the data is accurate, confidential, and available only to authorised parties.

This is where the least privileges concept comes into play. The ideology here is simple. Each user, including IT personnel, gets the least access they can have to effectively do the job. Rather than asking the question "Why not give this person access to X?" you should ask "Why give this person access to X?" If you do not have a very good reason to grant access, then do not provide the access. This is one of the fundamentals of computer security. The more people who have access to any resource, the more likely a breach of security will occur.

Trade-offs between access and security must be made. One common example involves sales contact information. A company's marketing department will need access to this data. However, what happens if competitors get all of your company's contact information? That information could allow them to begin targeting your current client list. This requires a trade-off between security and access. In this case, you would probably give sales staff access only to the contacts that are within their territory. Nobody apart from the sales manager should have complete access to all contacts.