Software Development Unit 3, 3.1

Anna Legaspi

# I can describe what access rights and issues others may have in using collaborative technologies.

In project collaboration, members of the team will each have a specific role to fulfil. As a result, each team member will need to have specific access depending on their role. The best example I can provide is in my current work place.

I work for a building society with over a few hundred employees. It has a hierarchy and is split down to various departments, with the tasks completed by the Team members. The Team members are then managed by Managers, the Managers managed by Senior managers, the Senior managers report to the Head of Department who then report to the leadership and executive team.

All of these employees will have a work profile which will need to have the right access for them to be able do their job effectively and efficiently. It's important that each employee is given the right access so they do their day-to-day job, no more, no less.

Ill elaborate by example between two profiles (manager and team member).

|  |  |  |
| --- | --- | --- |
| **Access** | **Manager** | **Team member** |
| Transferring money to another account without passing full security with customer.  *Banking software* | Read/Write/Execute | No access |
| Viewing and amending customer account information  *Banking software* | Read/Write/Execute | Read/Write |
| Creating a note on the customer’s account  *Banking software* | Read/Write/Execute | Read/Write |
| Logging and managing complaints on customer’s account  *Banking software* | Read/Write/Execute | Read-only |
| Archived weekly email confirming messages for the week  *In-house website* | Read/Write | Read-only |

|  |  |
| --- | --- |
| **Access** | **Definition** |
| Read-only | Allows the user to read the document or information, but have no ability to edit or change the content. |
| Read and Write | Allows the user to read and make amendments to the document or information. |
| Read, Write and Execute | Allows the user to read, make amendments and run executable files. |

I’ve noted above specific tasks above, most of which are completed or processed in the Banking software. Despite using the same software, managers have more access than team members. This is because managers have higher clearance in processing certain transactions for customers compared to team members.

If a team member was accidentally given more access than what’s needed, they could accidentally transfer money to another bank without going through full security with a customer. To avoid this from happening, the system will present a ‘hard stop’ if a team member doesn’t complete full security. Giving more access than what is needed means that employees might end up doing things they shouldn’t be doing or accessing data that isn’t for them to see. This can affect the company’s reputation, loss of funds and be fined for negligence.

Although my example above is specific, the same concept applies to other scenarios. People should only access what they’re allowed within their remit and job profile.