CASES LUXEMBOURG

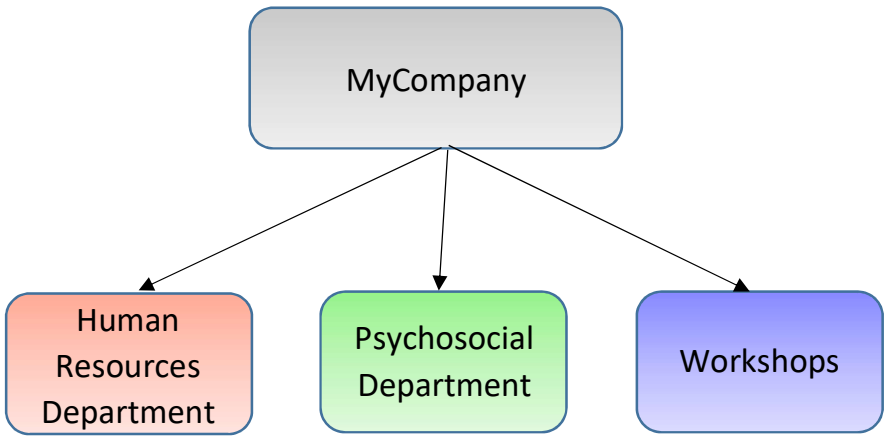
MONARC Training

MyCompany

Company context

MyCompany is a non-profit organisation, which professionally reintegrates vulnerable people having a psychological disorder by giving to them some particular attention. During recent years, and despite some staff rotation, the company has the same amount of 40 employees.
The risk analysis done for all the present information systems. But, with all the medical data, it has become crucial to be compliant to the modified law of the august, 2nd 2002, which is related to the protection of personal data. The loss of medical records is the biggest threat to the company.
MyCompany has no competitors, but has already known an incident. Indeed, all their data before 2005 has been lost. Their office is in the centre of Luxembourg City, in an extremely calm district. There was no attempted burglary, or geological hazards.
One of the key employees of this risk analysis is Michael, accountant and system administrator for the association. He uses the same account for his two tasks, though. There are also other external system administrators.

MyCompany does not have a user charter, any procedure or trainings available concerning field of information security. Every employee has administrative rights on their computer. Moreover, they remain logged into their sessions, even if absent, so the administrator could just manually do all the update. Luckily, the employees take their own responsibility and watch over the administrator whil the update are performed. They use Apple MAC Computers without antivirus, but they dispose of a virtual machine with Windows and Bitdefender installed.
There is no NDA signed with subcontractors that have access to medical records. Besides, the administrator has access to this data, even though he has not officially the right to. There is no control on a download, and all passwords are in an Excel file on the server.
The office has some automatic doors that open from 8 a.m. to 4 p.m. In November, the IT room was around 30 °C, and there is no air conditioning. It is also used to store personal belongings, and many people have some extra keys to open it.
Backups are realised three times daily on local storage and once a week on another decentralised location. The retention time is not known, even if sufficient. There is no one responsible for the backups, and so there is no contract in case of dispute with the subcontractor. The network is correctly managed, with one unique account per user, and no Wi-Fi.



Human Resources Department: Two full-time employees are sharing the same password and the same skills. They know enough about the software they use to understand and correctly use every functionality. Physical access is correctly managed, even though the cleaning staff are doing their tasks while there is no one on the office. Integrity of data is quite important for the team.

Psychosocial Department: Six full-time employees are sharing the same password. They have enough skills for the use of their software. Some employees are occasionally teleworking, and sometimes, send non-encrypted e-mail with medical records. Physical access is correctly managed, even though the cleaning staff are doing their tasks while there is no one on the office. Confidentiality and Integrity seems to be important criteria for the team.

Workshops: They are 3 workshops where people with psychological disorder can work. As they are based on the same scheme, they could be considered the similar. The best-known one is the carpentry. There are 25 to 35 employees, and 3 workshop managers who can decide to give computer access to their workers. Fortunately, the computer as no sensible data stored on it. Workshops are well protected enough physically. There is no third party in the process, and everything is done internally. Management have said that there is no data, which is critically important in their workshops, but they need to be available during work hours.