Assignment 5 – Daniel Høyland

One security models/mechanisms that is applicable to our project is something called access control. Access control is something that ensures data confidentiality by ensuring that a user has just some authorizations based on the intent of what users like that user are allowed to. Some commonly used security models are the discretionary access control (DAC) model, the mandatory access control (MAC) model, and the role-based access control (RBAC) model. We can implement this by implementing role-based access control (don't know how to do it with our database from the text but know the basics of this) which will assignee permission based on the responsibilities or the RBAC model.

Another security models/mechanisms that is applicable to our project is encryption. Encryption is basically "masking" or converting something over to something else based on a key. It is especially important to apply this to passwords or other sensitive data. The way we implement this is to make sure that sensitive information is being encrypted by probably the database program or something else, but I would guess there is a function for it.

Something else that we should probably have but would not be very mandatory for our project would be backup and a recovery mechanism that ensures availability and durability of data. We will 100% make a backup but we won't have it automatically probably. But this ensures that if the data becomes corrupt or that someone deletes all of the data or it gets lost because of someone stealing the pc with the database, then we could restore it from an earlier point and not lose all our data.

Of course, this is very little of what we need to do if we are working on a big database because of many other more complex threats like complexity of the database, insider threats and the constantly evolving threats against databases. But this is at least the minimum amount you have to do for the database or else the database will 100% not be used for anything actually serious.