## Security Planning

### Karim Ahmed

### Week3

### CIS433/CIS533

### Spring 2022

# Question 1:

Investigate your university’s or employer’s security plan (If not possible, search the web for a plan, some organizations have them in their website) to determine whether its security requirements meet all the conditions below List any that do not. Provide a link to the plan if possible, when was the plan written? When was it last reviewed and updated?

* I will be using my employer’s security plan. The plan is available on a secure link that is accessed only by the employees of the company in their Knowledge Base. There is no date that indicates when the plan was written. The plan is updated on an average of one time per month. These updates are very minor.
* Correctness
  + Individual requirements are not fully correct. This part is tied to how some aspects of the security plan are vague.
* Consistency
  + There are some inconsistent patterns in the security plan. This is due to the dependency on the legacy architecture of some models. As the company grows, they tend to add more requirements and patterns to be followed in building the system, but some parts of the system violate this due to the dependency on an old architecture which can be an undiscovered vulnerability.
* Completeness
  + There are some aspects of the security plan that are not documented. This includes the responsibilities of interns and different roles.
* Realism
  + In my opinion, most parts of the security plan are realistic. There are no requirements that are unrealistic
* Need
  + All requirements satisfied
* Verifiability
  + Some requirements are not verifiable as there is no implementation of a way to verify them. Example of this is (All updates must be backwards compatible)
* Traceability
  + All requirements satisfied

If you discover an unusual situation at your university or employer, to whom should you report it? Can you report something any time day or night? Does the security plan address that?

* The security plan does not address that. This would depend on the unusual situation. If this is a technical security risk that I found, I will address this to the Head of the Product Development. This has been the case before in some parts of the system where I discovered security vulnerabilities that I addressed and proposed solutions to the Head of Product Development. If this is a behavioral situation where there is a suspicious behavior/activity, I am more likely to report this behavior directly to this person’s manager. I will most likely file a report during my working hours.

# Question 2:

A perfect security will never exist, we implement different policies to try and mitigate the risks. That’s why your security plan should satisfy the conditions mentioned above. Give an example for the following:

1. A Security requirement that is not realistic
   1. Having all employees always monitored: This is unrealistic in today’s world where almost all companies are shifting to remote work.
2. A security requirement that is not verifiable.
   1. All layers of the system must be robust.
   2. All updates must be backwards compatible.
3. Two security requirements that are inconsistent.
   1. Automated tests should cover all different cases before deployment.
   2. Ignore testing user access to a specific module because of the dependency on an old architecture.