Linnaeus University
Department of Computer Science
OF

Information Security

Practical work #3, 1DV700, HT21

In this assignment, you will continue to work with the company *Loco News.* Your group now is to investigate the information security of the company. The teaching assistants (acting CTO) will be your contact persons for the company. Interactions with them can be in forms of e-mail, booked interviews and the scheduled lab sessions. You also have some written documentation about the company, start reading extra material that is posted with the assignment.

Your title will be Information Security Consultants and your task is to evaluate the company's interactions with information from all possible aspects and develop policies that will carry the company to **ISO/IEC 27002** compliance. For that, you first have to study standard, which is the framework for achieving ISO/IEC 27002 compliance. You also need to investigate what they need to do to comply with the **GDPR** regulation. Determine locations and/or special categories of personal data.

You will continue to work in the groups created for Assignment #2. Each group will create their own work on the company separately.

First line of information security will start with yourself. From company's standpoint, you are outsourced personnel and have enough access to cause harm to their operational status. In a real-world situation, you would probably have to sign an **NDA (Non-disclosure Agreement)**. In addition to that, you will already assess the relations of the company with other outsourced personnel and develop necessary policies under Organizational Security - Outsourcing section.

Task 1

Within their busy business tempo, companies may rarely be able to spare time for you and your requests. Therefore, interview time with the company is golden and you should make good use of this time. You should have a very good grasp of ISO/IEC 27002 standard in advance, and a huge list of questions that you should be asking.

Study the ISO/IEC 27002 standard (and any supporting information you find useful on Internet). In the group, discuss all the areas of controls that the standard covers and what they cover. Then divide them between the group members (each member having at least two areas each, possibly with some overlap).

Write an individual 2 pages summary of the security controls that you are responsible of. Try to come up with as many questions/requests as possible to be directed to company personnel, include only around 8-10 of them in your summary for us to assess that you are on the right track. Also study the GDPR regulation and discuss in your group about how it may affect the company (e.g., when should personal data be destroyed). Again, think about questions you need to have answered.

Submit the individual report at latest **12 December**.

Task 2

It is time to make use of the knowledge you gained in Task 1. Book up meeting with the CTO. Contact to the company via email or slack, request any material you need and ask questions. Then each team-member prepares the policy document for the specific security control that he/she is responsible for.

In the end, all team-members combine their work and generate one complete INFOSEC (information security) policy document. For example, detect issues that compromise information security such as misuse of data, networks, computer systems and applications; ensure that the company has a series of controls around the three principles of information security: confidentiality, integrity, and availability (CIA). At this stage all members should discuss the entire document until you all agree on all parts of it. At the end each of you will have to stand behind the entire document if we find any problems with it like plagiarism.

Team-leaders have to submit the final work on Moodle according to the deadline.

Submit the group report at latest **16 January**.

You can check the policy document template on the following link.

Security Policy Document Template