INSTITUTE OF TECHNOLOGY CARLOW

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTING

PROJECT EXAMINATIONS

COURSE CODE: CW258 **DATE: Weeks 15 to 20**

Course Title: **Bachelor of Science in Cybercrime and IT Security**

Course Year: **3**

Subject: **Cybercrime Legislation, Cryptography, Software Engineering**

Examiners: **Dr James Egan, Dr Martin Harrigan, Dr Christopher Staff**

Marks: **(20% Cybercrime Legislation)**
(15% Cryptography)
(25% Software Engineering)

Submission Date and Time: March 6th @ 11.55pm

NOTE: A Q&A has been created for this project here. Put questions you have about this project here.

Link to Q&A Document

Scenario 1

Upload an antigen test with a photo.

Our national health service has decided to create a portal that will allow citizens to report a positive antigen test for COVID-19 and to list their close contacts online. Citizens who have symptoms of the virus or are a close contact of a confirmed case can use store-bought test kits and upload any positive results to the portal. The system will require citizens to create an account with a username and password, to provide personal information including full name, address, date of birth and phone number, and to upload an image of a positive antigen test. They can also provide a list of close contacts, including their full names and phone numbers.

Scenario 2

IT Carlow clubs and societies wish to establish an online registration system for students and staff.

The system will require students to create an account with a username and password. To join a club/society students will need to include, student ID, phone number, email, date of birth and upload a photo. Students will also need to provide a medical declaration and provide information on any medical conditions, doctor information and next of kin contact information.

Deliverables

- An application should be developed that implements one of the above scenarios. This developed application must be fully GDPR compliant. The system should use cryptographic methods to ensure GDPR compliance. The personal data (e.g., the names and phone numbers) should be encrypted using a secure block cipher. The passwords should be hashed using a secure hashing algorithm. The application should be developed using the XAMPP stack.
- A 1500 word report on the most important aspects of GDPR that need to be considered for ICT developers when handling personal data.
- Provide the necessary design documents to prove that the application meets the “Data Protection by Design” criteria of GDPR. Motivation: If the organisation that you are building this application for has a data breach and the Data Protection Commission comes knocking at that organisation’s door then they will have to show that data security and data protection were key aspects during the design stages of the product development. If security and privacy was not included in the design stage and only added as an afterthought then your company could be in line for large fines. The company needs to create some design documents that show how data security and data protection are embedded in their application. Aspects of UML (e.g., Use Case Diagrams, Misuse Case Diagrams, etc.) which, in your opinion, can be used to show a data protection officer the planning that went into data protection, data encryption, password protection, retention of data, etc in the development of the application.
- Assume that you are the Project Manager of a team of five people brought together to analyse, design, implement, and test the solution for your chosen scenario. The project has now reached the implementation stage, which is expected to last ten weeks. Create a GANTT chart and PERT chart that covers the implementation and testing activities and tasks. Assume that about half-way through the implementation stage there is a 20% over-run in one of the tasks on the critical path. Explain how you would manage the resources

allocated to the remaining tasks to ensure the project completes on time.

Marking

20% Cybercrime Legislation: This module will use the average mark of all project elements.

15% Cryptography: This module will use the average mark of all project elements.

25% Software Engineering: This module will use the average marks of all project elements.

Submission

You need to submit one document that includes:

- a link to a video, preferably on YouTube, demonstrating the system (maximum 7 minutes),
- a link to a GitHub repository with your code,
- a report on GDPR, and
- the software engineering diagrams, including the PERT or GANTT chart.

Please upload the document at a Turnitin link in the assessments section of the Cybercrime Legislation Blackboard page. A second link is available for you to upload any additional material you wish to upload but can't in the Turnitin link.