# School of Information Technology

# Department of Computer Science

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA
Faculty of Engineering, Built Environment and Information Technology

## COS720 Computer Information & Security I

## Project Specification 2025

## Release Date: 16 February 2025

## Submission Date: 17 May 2025

**Lecturer: Mr S.M. Makura**
**Moderator: Ms S. Rananga**
**Total: 100 Marks**

**Instructions**

1. This project must be completed on an individual basis. **No group work is allowed**. It must be the **student's own work**. **You must clearly indicate if you have objects / components coming from other resources. You must clearly show the uniqueness of your solution in comparison to other existing solutions.**
2. An anti-plagiarism approach will be strictly enforced. Please familiarise yourself with the UP-Plagiarism Prevention policy. All plagiarism cases pertaining to any aspect of the project will be handled over to UP Legal for further investigation. You will have to submit a signed form acknowledging that you have read and are in agreement with the **UP Plagiarism Prevention policy which can be read here:** https://www.up.ac.za/media/shared/1/ZP_Files/s5106-19-plagiarism-prevention-policy.zp181077.pdf ).

3. Online submission of project supporting documentation:
   - Submit the following:
     - 1 page **research overview (in your own words)** that relates to your solution. Include literature references.
     - A detailed bibliography (separate from the 1 page above). (This must be your detailed bibliography compiled by yourself).

- 0.5 - 1 page requirements specification of your OWN unique solution
- **UML design diagrams** of your OWN unique solution.
- A Turnitin report for your submissions.
- Your submissions must be in Word or PDF (.doc .docx .pdf file).
- All design diagrams must be in formal UML notation.

**NO LATE submissions** will be accepted after the submission date has lapsed regardless of whatever reason you give.

**Project Topic: AI-Powered Phishing Email Detection System**

**Objective:**

Develop a lightweight AI-powered prototype that identifies **phishing emails** based on text analysis and metadata features.

**Project Tasks:**

1. **Research Overview (part of the documentation submitted at the end)**:
    - Provide a **10-line summary** of how AI is used to detect phishing attacks and its advantages over traditional methods.
    - Define **phishing detection using AI** in 2–3 lines, focusing on its role in combating email-based threats.

2. **Dataset Preparation**:
    - Use a publicly available dataset of emails specifically Kaggle's phishing email dataset. You can download the dataset from here: https://www.kaggle.com/datasets/naserabdullahalam/phishing-email-dataset
    - Preprocess the dataset to extract features such as subject lines, sender information, and email content.

3. **Model Development**:
    - Implement a **machine learning model** (e.g., Logistic Regression, Random Forest, or Neural Network) to classify emails as phishing or legitimate.
    - Train the model on your dataset and evaluate its performance using metrics like accuracy, precision, recall, and F1-score.

4. **Prototype Implementation**:
    - Create a simple web-based interface where users can upload an email (text file) or paste email content. You can use any programming language you are comfortable with.
    - The prototype should output whether the email is **phishing** or **legitimate**, along with a confidence score.

5. **AI Explainability**:
    - Add a feature to the prototype to explain the AI's decision (e.g., highlight suspicious phrases or sender metadata).

6. **Testing Scenarios**:
    - Test the prototype using real-world phishing emails (ensure no sensitive data is used).
    - Document cases where the prototype succeeds and fails.
7. **Documentation**:
    - Include a **1-page explanation** of the model selection process.
    - Provide UML diagrams for the system architecture and workflows.
    - Document potential limitations of the AI model and suggest improvements.

**Submission Requirements:**

1. **Codebase**:
    - Submit the code with comments and instructions for running the prototype.
2. **AI Model**:
    - Save and submit the trained model (if applicable).
3. **Testing Report**:
    - Provide results from testing the prototype on different phishing and legitimate emails.
4. **Documentation**:
    - UML diagrams for system design.
    - A summary of AI principles applied in phishing detection.

**Evaluation Criteria:**

1. **Model Performance**:
    - Accuracy and effectiveness of the phishing detection system.
2. **Prototype Functionality**:
    - Usability, clarity of output, and explainability of AI decisions.
3. **Documentation**:
    - Clarity, completeness, and insightfulness of research and design documents.

The documentation for the project that you must compile counts for 50% of the marks for the project. The project demonstrations will then count the other 50% of the marks for the project. The demonstrations will be done either physical face-to-face hands-on demonstrations to the lecturers or using an online demonstration. Students should therefore ensure that their uploaded documentation includes a well-structured design of their solution (it must be in UML notation). The due date for

the project assignment is **17 May 2025**. No late submissions or extensions allowed.