Assessment Brief

Module Title: **Secure Design and Development**
Module Code: **7032CE**

Assessment Type: Coursework	Assessment Number: 1	Study Mode: Full-time	Weighting: 70%
Submission Date: **01/03/2025**	Submission Time: 20:00	Campus: PSB Academy	

Completion of this assignment will address the following learning outcomes:	
LO1	Evaluate a range of platforms for systems and applications, against standards and methodologies for secure development, incorporating issues raised by the legal and ethical context of the development, such as IP law, privacy and data-protection.
LO2	Design applications that adhere to secure development methodologies.
LO3	Develop applications that implement secure principles and are fully tested against software security and quality guidelines.
LO4	Critically evaluate existing software, using methods such as code review, static and dynamic analyses.
LO5	Apply formal methods to different stages of the system development life-cycle like system specification, design, development and testing.

Overview
This assignment requires you to design and develop a functional secure system. The assignment consists of two elements: 1. A practical element that requires you to work on the development of a secure web-based system. The assessment will be evidenced via a 10 - 15 minutes presentation explaining all the considerations around the developed system. 2. An individual report of 2500 words that will describe the development process and report on its success, evaluation and fitness for purpose must be written by every student. That report needs to be submitted via Blackboard Turnitin by the assignment deadline. The weighting is 70% including both elements. Both the practical work and report will be assessed against the same grading rubric table.

Task:
Practical Element Brief A **Performance and dance group** has hired you to develop a **web-based application/software** that enables the directors and coaches to keep records of the training and performance data using personal accounts, enter and store the statistics and personal information of the artists, update attendance and injury records and also perform other club activities. The group includes children and adults from the age of 7 up to 70. The requirements for the system are as follows: • Design the system under consideration incorporating the principles of secure design and development • Develop the designed system complying with the required standards and methodologies. • Apply testing and analysis techniques to the developed system. • Apply Formal Methods to different stages of the system development life cycle. **Individual Report Brief** You are asked to write an individual report that will consider the following issues in relation to the web-based system developed in the practical element of the assignment: • System documentation: Explanation of the methods and techniques followed in the practical task for the development of the system. Discuss all the stages of the development life-cycle (e.g. specification, design, development, etc.). • Legal consideration: Legislation considered with respect to the system developed in the practical part.

Individual Report Information

At the end of the module, you will be expected to submit an individual report. This must be entirely your own work. The report is based on the practical element that you have completed and should generally report on the development process and the evaluation of the system. This element is **not** assessed separately from the practical one. Therefore, your report will be marked using the same grading rubric as that of the practical element.

Submission

You are required to submit a 2000-word individual report in a PDF format via Blackboard Turnitin submission.

Marks break-up

1) **Design (25%):**
   a. Produce a prototype for the system to be implemented and explain what design and security principles have been considered and why.
   b. Describe how the chosen principles or features enhance the functioning and security of that system in this stage of the development life-cycle.

2) **Development (25%):**
   a. Produce an application that complies with the design provided in the previous task.
   b. Demonstrate the proper functioning and security mechanisms of the developed system in accordance with the existing secure development standards and methodologies.

3) **Security (25%):**
   a. Demonstrate the use of testing and analysis techniques applied to the developed system, such as code testing, static and dynamic analysis, etc.
   b. Propose solutions for the issues discovered during the testing and analysis process showing how they can mitigate the detected problems.

4) **Formal Methods (25%):**
   a. Use formal methods, specifically automata, to produce the behavioural model of the system that will be based on the design or development stage of the system life-cycle.
   b. Convert the automata model into the respective Petri net model and then verify the correctness of the system with respect to its specification using the appropriate verification techniques and tools.

Guidance notes and considerations

Late Submission

- If you are not able to complete your coursework on time due to extenuating circumstances, the ONLY way to receive an extension (up to 5 working days) or a deferral (anything longer than 5 working days) is to contact your module lecturer or Email to *PG_SET@psb-academy.edu.sg*
- Extenuating circumstances are defined by CU as 'genuine circumstances beyond your control or ability to foresee, and which seriously impair your assessed work'.
- Please note that you will need to provide third party evidence to support your reasoning for requiring an extension or deferral.

Plagiarism and Malpractice

- You are encouraged to check the originality of your work by using the draft Turnitin links on your Blackboard.
- Collusion between students (where sections of your work are similar to the work submitted by other students in this or previous module cohorts) is taken extremely seriously and will be reported to the academic conduct panel. This applies to all coursework and exam answers.
- A marked difference between your writing style, knowledge and skill level demonstrated in class discussion, any test conditions and that demonstrated in a coursework assignment may result in you having to undertake a Viva Voce in order to prove the coursework assignment is entirely your own work.
- If you make use of the services of a proofreader in your work you must keep your original version and make it available as a demonstration of your written efforts.
- You must not submit work for assessment that you have already submitted (partially or in full), either for your current course or for another qualification of this university, unless this is specifically provided for in your assignment brief or specific course or module information.
- Where earlier work by you is citable, i.e., it has already been published/submitted, you must reference it clearly. Identical pieces of work submitted concurrently will also be considered to be self-plagiarism.

Submission Guidelines

There should be a title page which clearly identifies the following:

* Name of the module * Title of the Assessment

* Assessment number * Word count

The word count identified includes quotations, but excludes the bibliography and unless specifically stated, encompasses a discrepancy of + or – 10%.

Marking Rubric

Grade / Criteria		0 – 39	40 – 49	50 – 59	60 – 69	70 – 79	80 – 100
F2F Presentation and Report Submission	**System Design (25%)**	No system design built or incomplete design provided.	System design meets the basic requirements. Short discussion in the report.	System design incorporates the principles required for the proper functioning and security of the system. Adequate discussion in the report.	System design incorporates an extensive range of principles, which are very well discussed in the report.	Detailed system design fully based on the secure design methodologies and standards. Thorough and well-justified documentation.	A system design of professional standards, which is optimized for the given scenario. Fully documented design process.
	System Development (25%)	No system developed or incomplete implementation of the system.	System development complies with the requirement of a basic design. Short discussion in the report.	System development considers basic functioning and limited security of the system with good explanation of the development stage.	System development fully complies with the proposed design, but partially with the secure development methods and standards. Process is very well described in the report.	System development fully complies with the secure development methods and standards. Thorough and well-justified documentation.	System development is professionally executed, fully complying with all the respective methods and standards. Fully documented development process.
	Security Testing and Analysis (25%)	No or very poor system security and testing carried out with no recommended solutions.	Very limited security analysis and testing of the system with very few solutions provided. Short discussion in the report.	A small range of security analysis and testing techniques have been used providing the respective solutions. Adequate discussion in the report.	A medium range of security analysis and testing techniques have been used providing effective solution for the detected problems. Process is very well described in the report.	An extensive security analysis and testing has been conducted providing mitigation techniques for the identified security issues. Thorough and well-justified documentation.	Professional standard security analysis and testing followed by security measures that significantly improve the overall system security and functioning. Fully documented security process.

	Formal Methods (25%)	No or very poor application of formal methods to the system analysis.	A very basic attempt of modelling the behaviour of the system and then verify it. Short discussion in the report.	Behavioural model presents the basic functioning of the system incorporating security aspects as well. Verification examines the basic security issues. Adequate discussion in the report.	Formal modelling and verification processes extensively examine a wide range of functioning and security issues. The formal analysis is very well described in the report.	Formal modelling and verification processes fully examine the functioning and security issues of the system. The formal analysis is very well justified in the report.	Formal modelling and verification processes are professionally applied to the system covering and examining all the potential issues. The process is fully documented.