Faculty of Engineering and Technology			
Ramaiah University of Applied Sciences			
Department	Computer Science and Engineering	Programme	B. Tech. in CSE
Semester/Batch	6/2018		
Course Code	19CSC315A	Course Title	Information Security and Protection
Course Leader	Prof. N. D. Gangadhar / Dr. Vaishali R. Kulkarni / Dr. Suvidha K. V.		

Assignment-01			
Reg.No.		**Name of Student**	

Marking Scheme		**Marks**		
		Max Marks	**First Examiner Marks**	**Moderator**
1	Identification of the assets to be protected and actors involved	**3**		
2	Design of the specific Confidentiality, Integrity and Availability security services required for the assets	**4**		
3	Analysis of the threats to the system based on the determined security requirements	**4**		
4	Recommending specific security policies to counter the threats and attempt a synthesis of them into an overarching policy	**4**		
5	Identify specific security mechanisms to implement the recommended policy/policies with the goal of prevention of attacks	**4**		
6	Discussion on the assumptions and role of trust in the recommendations	**3**		
7	Discussion of the role of law and University Regulations	**3**		
	Part-A Max Marks	**25**		

Course Marks Tabulation				
Assignment	**First Examiner**	**Remarks**	**Moderator**	**Remarks**
1				
Marks (out of 25)				

Please note:

1. Documental evidence for all the components/parts of the assessment such as the reports, photographs, laboratory exam / tool tests are required to be attached to the assignment report in a proper order.
2. The First Examiner is required to mark the comments in RED ink and the Second Examiner's comments should be in GREEN ink.
3. The marks for all the questions of the assignment have to be written only in the **Component – CET B: Assignment** table.
4. If the variation between the marks awarded by the first examiner and the second examiner lies within +/- 3 marks, then the marks allotted by the first examiner is considered to be final. If the variation is more than +/- 3 marks, then both the examiners should resolve the issue in consultation with the Chairman BoE.

Assignment 1

Instructions to students:

1. Maximum marks is **25**.
2. The assignment has to be neatly word processed as per the prescribed format.
3. The maximum number of pages should be restricted to 1**0**.
4. The printed assignment must be submitted to the course leader.
5. **Submission Date: 22nd May 2021**
6. **Submission after the due date is not permitted.**
7. **IMPORTANT**: It is essential that all the sources used in preparation of the assignment must be suitably referenced in the text.
8. Marks will be awarded only to the sections and subsections clearly indicated as per the problem statement/exercise/question

Preamble

This course is aimed at preparing the students to understand, design, analyze, implement and integrate security provisions in an IT environment. Students are taught elements of information

security, known attacks and counter measures. The module also introduces the students to IT policies, auditing and standards that enable them to understand and provide information security assurance. Scenario based case studies are employed. Students are trained to analyze a given scenario and propose security measures and policies and develop an analytical report documenting their effort.

Security and Protection of Examination Section on RUAS Portal

RUAS Portal has several overlapping operational sections. One set of functionalities of the portal covers the operation and information flow involving data and information related to the Examinations and Assessment of students. Data and information related to question papers, answer scripts, student reports and presentations, attendance records, time tables, marks sheets and certificates are handled by the section. Owing to the sensitive and confidential nature of the data and information, it is essential that it is well protected with security policies and mechanisms.

The student is required to perform an analysis of the information system along the following lines:

1. Identify the assets to be protected and actors involved
2. Determine the specific Confidentiality, Integrity and Availability security services required for the assets
3. Analyze the threats to the system based on the determined security requirements
4. Recommend specific security policies to counter the threats and attempt a synthesis of them into an overarching policy
5. Determine specific security mechanisms to implement the recommended policy/policies with the goal of prevention of attacks
6. Discuss the assumptions and role of trust in the recommendations
7. Discuss the role of law and University Regulations

The student may refer to Section 4.6 of Bishop (2019) where an example of a University electronic communication security policy and one of its implementation is discussed. This is suggested as a background to a University environment only and the student is not encouraged to attempt at developing a comprehensive security policy along those lines, which is a massive effort involving a large committee.

Reference:

Bishop, M. (2019) Computer Security: Art and Science, 2nd edn., Addison-Wesley.