B.C.A (6th Semester)

030010608: SEC1 Fundamentals of Cyber Security

Assessment Policy

Assessment:

The weightage of CIE and University examination shall be as per the University regulations.

- Composition of CIE shall be

Assessment Code	Assessment Type	Duration of each	Occurren ce	Each of marks	Weightage in CIE of 20 Marks	Remarks
A1	Quiz	1 hours	1	20	2 x 1 = 2	Shall be taken at the end of 1st unit of syllabus
A2	Open Book	1 hours	1	20	2 x 1 = 2	Shall be taken at the end of 3rd Unit
A3	Unit Test	1.5 hours	2	30	3 x 2 = 6	Shall be taken at the end of 1st and 2nd unit of syllabus Shall be taken at the end of 4th and 5th unit of syllabus
A4	Internal Examination	1.5 hours	1	30	7 x 1 = 7	Covers all Units
A5	Presentation	20 minutes	1	30	3 x 1 = 3	Covers all Units

Assessment Type Classification:

Assessment Code :	A1	**Weightage of Content :**	**Unit** **(%)** 1 100
Assessment Type :	Quiz	**Tentative Date :**	02/01/2018
Kind of Question Format:	Q-1: Choose most appropriate answer from the options for questions (1 X 20 =20 Marks)		
To measure :	Knowledge		
Outcome :	CO1: Describe cyber crime and its importance including the act of cyber criminals along with its types.		
Programme Outcomes:	PO1: Ability to understand the concepts of key areas in computer science. PO2: Ability to design and develop system, component or process as well as test and maintain it so as to provide promising solutions to industry and society. PO4: Ability to understand professional and ethical responsibility. PO5: Recognition of the need for life-long learning.		

Assessment Code :	A2	**Weightage of Content :**	**Unit** **(%)** 1 to 2 30 3 70
Assessment Type :	Open Book	**Tentative Date :**	07/02/2018
Kind of Question Format:	Q-2: Do as directed. (5 X 4 = 20 Marks)		

To measure :	Knowledge
Outcome :	CO1: Describe cyber crime and its importance including the act of cyber criminals along with its types. CO2: Classify various types of cyber attacks. CO3: Classify and relate methods used in cybercrime along with security mechanism. CO4: Describe basics of cryptography, digital signature and public-key infrastructure in context of cyber security.
Programme Outcomes:	PO1: Ability to understand the concepts of key areas in computer science. PO2: Ability to design and develop system, component or process as well as test and maintain it so as to provide promising solutions to industry and society. PO4: Ability to understand professional and ethical responsibility. PO5: Recognition of the need for life-long learning

Assessment Code :	A3	**Weightage of Content :**	**Unit** **(%)** 1 10 2 40 3 50
Assessment Type :	Unit Test 1	**Tentative Date :**	During 5th week
Kind of Question Format:	Q-1: (A) Short answer questions (4 out of 4) [Each of 1 mark] (B) Short answer questions(3 out of 4) [Each of 2 marks] Q-2: (A)Scenario Based questions (2 out of 1)[Each of 5 marks] (B)Scenario Based questions (2 out of 1)[Each of 5 marks] Q-3: Answer the question in detail(2 out of 3)[Each of 5marks]		
To measure :	Knowledge		
Outcome :	CO1: Describe cyber crime and its importance including the act of cyber criminals along with its types. CO2: Classify various types of cyber attacks. CO3: Classify and relate methods used in cybercrime along with security mechanism.		
Programme Outcomes:	PO1: Ability to understand the concepts of key areas in computer science. PO2: Ability to design and develop system, component or process as well as test and maintain it so as to provide promising solutions to industry and society. PO4: Ability to understand professional and ethical responsibility. PO5: Recognition of the need for life-long learning		

Assessment Code :	A3	**Weightage of Content :**	**Unit** | **(%)** 1 | 40 2 | 60
Assessment Type :	Unit Test 1	**Tentative Date :**	16/01/2018
Kind of Question Format:	Q-1: (A) Short answer questions (4 out of 4) [Each of 1 mark] (B) Short answer questions(3 out of 4) [Each of 2 marks] Q-2: (A)Scenario Based questions (2 out of 1)[Each of 5 marks] (B)Scenario Based questions (2 out of 1)[Each of 5 marks] Q-3: Answer the question in detail(2 out of 3)[Each of 5marks]		
To measure :	Knowledge		
Outcome :	CO1: Describe cyber crime and its importance including the act of cyber criminals along with its types. CO2: Classify various types of cyber attacks. CO3: Classify and relate methods used in cybercrime along with security mechanism.		
Programme Outcomes:	PO1: Ability to understand the concepts of key areas in computer science. PO2: Ability to design and develop system, component or process as well as test and maintain it so as to provide promising solutions to industry and society. PO4: Ability to understand professional and ethical responsibility. PO5: Recognition of the need for life-long learning		

Assessment Code :	A3	**Weightage of Content :**	**Unit** | **(%)** 1 to 3 | 40 4 to 5 | 60
Assessment Type :	Unit Test 2	**Tentative Date :**	28/02/2018
Kind of Question Format:	Q-1: (A) Short answer questions (4 out of 4) [Each of 1 mark] (B) Short answer questions(3 out of 4) [Each of 2 marks] Q-2: (A)Scenario Based questions (2 out of 1)[Each of 5 marks] (B)Scenario Based questions (2 out of 1)[Each of 5 marks] Q-3: Answer the question in detail(2 out of 3)[Each of 5marks]		
To measure :	Knowledge		
Outcome :	CO1: Describe cyber crime and its importance including the act of cyber criminals along with its types. CO2: Classify various types of cyber attacks. CO3: Classify and relate methods used in cybercrime along with security mechanism. CO4: Describe basics of cryptography, digital signature and public-key infrastructure in context of cyber security. CO5: Identify the need for cyber laws, especially in the Indian context. CO6: Describe the fundamentals of digital forensics with its phases, rules and techniques.		
Programme Outcomes:	PO1: Ability to understand the concepts of key areas in computer science. PO2: Ability to design and develop system, component or process as well as test and maintain it so as to provide promising solutions to industry and society. PO4: Ability to understand professional and ethical responsibility. PO5: Recognition of the need for life-long learning		

<table>
<tr><td><b>Assessment Code :</b></td><td>A4</td><td><b>Weightage of Content :</b></td><td><table><tr><th>Unit</th><th>(%)</th></tr><tr><td>1</td><td>14</td></tr><tr><td>2</td><td>16</td></tr><tr><td>3</td><td>20</td></tr><tr><td>4</td><td>20</td></tr><tr><td>5</td><td>12</td></tr><tr><td>6</td><td>18</td></tr></table></td></tr>
<tr><td><b>Assessment Type :</b></td><td>Internal Examination</td><td><b>Tentative Date :</b></td><td>28/03/2018</td></tr>
<tr><td><b>Kind of Question Format:</b></td><td colspan="3"><table>
<tr><th colspan="3">Section-I</th></tr>
<tr><td>Q-1 (A)</td><td>Do as directed:<Very Short Answer&gt;</td><td>[03]</td></tr>
<tr><td>Q-1(B)</td><td>Answer in brief(Any two)<Short Answer -II&gt;</td><td>[02]</td></tr>
<tr><td>Q-2</td><td>Answer the following:<Long Answer with internal option&gt;</td><td>[06]</td></tr>
<tr><td>Q-3</td><td>Answer the following in detail. (Any 2)<Short Answer-I&gt;</td><td>[04]</td></tr>
<tr><th colspan="3">Section-2</th></tr>
<tr><td>Q-4 (A)</td><td>Do as directed:<Very Short Answer&gt;</td><td>[03]</td></tr>
<tr><td>Q-4(B)</td><td>Answer in brief(Any two)<Short Answer -II&gt;</td><td>[02]</td></tr>
<tr><td>Q-5</td><td>Answer the following:<Long Answer with internal option&gt;</td><td>[06]</td></tr>
<tr><td>Q-6</td><td>Answer the following in detail. (Any 2)<Short Answer-I&gt;</td><td>[04]</td></tr>
</table></td></tr>
<tr><td><b>To measure :</b></td><td colspan="3">Knowledge and Analysis</td></tr>
<tr><td><b>Outcome :</b></td><td colspan="3">CO1: Describe cyber crime and its importance including the act of cyber criminals along with its types.
CO2: Classify various types of cyber attacks.
CO3: Classify and relate methods used in cybercrime along with security mechanism.
CO4: Describe basics of cryptography, digital signature and public-key infrastructure in context of cyber security.
CO5: Identify the need for cyber laws, especially in the Indian context.
CO6: Describe the fundamentals of digital forensics with its phases, rules and techniques.</td></tr>
<tr><td><b>Programme Outcomes:</b></td><td colspan="3">PO1: Ability to understand the concepts of key areas in computer science.
PO2: Ability to design and develop system, component or process as well as test and maintain it so as to provide promising solutions to industry and society.
PO4: Ability to understand professional and ethical responsibility.
PO5: Recognition of the need for life-long learning
.</td></tr>
</table>

Assessment Code :	A5	**Tentative Submission Date :**	During semester
Assessment Type :	Presentation		
Kind of Question Format:	Guidelines: ✓ A student team must be of 4 members. ✓ Team shall form by students at the beginning of semester. ✓ Students shall give presentation on topic given by course teacher. Each team will be given 20 minutes time for it. ✓ Students must submit the document of given topic after the completion of presentation. Evaluation will be based on following criteria : Presentation and communication Skill (10 Marks) Quality of content (10 Marks) Viva & document submission (10 Marks)		
To measure :	Knowledge and Analysis		
Outcome :	CO1: Describe cyber crime and its importance including the act of cyber criminals along with its types. CO2: Classify various types of cyber attacks. CO3: Classify and relate methods used in cybercrime along with security mechanism. CO4: Describe basics of cryptography, digital signature and public-key infrastructure in context of cyber security. CO5: Identify the need for cyber laws, especially in the Indian context. CO6: Describe the fundamentals of digital forensics with its phases, rules and techniques.		
Programme Outcomes:	PO1: Ability to understand the concepts of key areas in computer science. PO2: Ability to design and develop system, component or process as well as test and maintain it so as to provide promising solutions to industry and society. PO3: Effective communication and presentation skill. PO4: Ability to understand professional and ethical responsibility. PO5: Recognition of the need for life-long learning		

- **UFM policy**:
  - If two or more submitted papers are too similar for coincidence, a penalty shall be imposed that shall usually be the same for the student who did the original as for the one copying from it.
  - Any ascertained fact of breaking institute policy shall be associated with one or all of the following: (i) zero marks for the work; (ii) report to the Course coordinator; (iii) report to the Director.