BCA (Semester- 6)

Assessment Policy

030010608: SEC1 Fundamentals of Cyber Security

Assessment Types: Theory:

Assessment Type	Duration of each Occurrence	Each of marks	Weightage in CIE of 20 marks
Quiz	1	20	2
Unit Test	1	30	6
Internal Examination	1	30	8
Technical Report Writing	2	10	4

Course Outcomes: Upon completion of the course, the student shall be able to
CO1: Recognize the cyber crime and its importance including the act of cyber criminals along with its types.
CO2: Classify passive and active types of cyber-attacks and prevent them by using different techniques such as strong password, protect identity online, protect computer with security software.
CO3: Classify and relate methods used in cybercrime along with common security mechanism.
CO4: Describe basics of cryptography, digital signature and public-key infrastructure in context of cyber security.
CO5: Identify the cyber laws against cyber crime, especially in the Indian context.
CO6: Investigate the importance 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.

Mapping with Assessment:

Assessment Type	Course Outcome	Programme Outcome
Quiz	CO1	PO1
Unit Test	CO1, CO2, CO3	PO1, PO2
Internal Examination	All	PO1, PO4, PO5
Technical Report Writing	All	PO1, PO3, PO5

Assessment Type Classification:

<table>
<tr><td>Assessment Type</td><td colspan="6">Quiz</td></tr>
<tr><td>Objective</td><td colspan="6">To identify that student can able to understand different types of cyber crime ad motive behind them.</td></tr>
<tr><td>Tentative Date</td><td colspan="6">24-12-2019</td></tr>
<tr><td>Unit Weightage</td><td colspan="6"><table><tr><th>Unit</th><th>Content Weightage (%)</th></tr><tr><td>1</td><td>100</td></tr></table></td></tr>
<tr><td>Question Paper Format</td><td colspan="6"><table><tr><th>Q.No</th><th>Question Nature</th><th>Mark of Each</th><th>Category</th><th>Remark</th><th>Total Marks</th></tr><tr><td>1</td><td>Multi choice questions.</td><td>01</td><td>Understanding (70%)
Analysis (30%)</td><td>Attempt All</td><td>10</td></tr></table></td></tr>
</table>

	2	Short answer questions.	01	Understanding (60%) Analysis (40%)	Attempt All	10
					Total	20

Assessment Type	Unit Test
Objective	To identify that student can able to: • Understand passive and active types of cyber-attacks and prevent them by using different techniques such as strong password, protect identity online, protect computer with security software. • Classify and relate methods used in cybercrime along with common security mechanism.
Tentative Date	28-01-2020

Unit Weightage

Unit	Content Weightage (%)
1	20
2	50
3	30

Question Paper Format

Q.No	Question Nature	Mark of Each	Category	Remark	Total Marks
Q:1(a)	Answer in short.	1	Understanding	4 out of 4	04
Q:1(b)	Answer in brief.	2	Understanding	3 out of 4	06
Q:2	Scenario-based Question	4	Analysis	A or A, B or B	10
Q:3	Answer in detail	5	Remembering	2 out of 3	10
				Total	30

<table>
<tr><td>Assessment Type</td><td>Internal</td></tr>
<tr><td>Objective</td><td>Measure the course objective attainment.</td></tr>
<tr><td>Tentative Date</td><td>31-03-2020</td></tr>
<tr><td>Unit Weightage</td><td>
<table>
<tr><th>Unit</th><th>Content Weightage (%)</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>Question Paper Format</td><td>As per external examination</td></tr>
</table>

Assessment Type	Technical Report Writing
Objective	• To enhance reading and technical writing skill. • To improve communication skill. • To motivate students toward punctuality and group learning.
Tentative Date for Assessment Parameter	Parameter-1: 25-02-2020 Parameter-2: 02-03-2020 onwards
Assessment Parameter	Parameter-1: Document Submission [10 Marks] Paramter-2: Viva [10 Marks]

<table>
<tr>
<td>Guideline</td>
<td>

Students have to write technical paper with basics and advanced concept of the syllabus or outside the syllabus.
A Team consists of 3 students. Team shall be formed by students in a 1st week after commencement of semester.
Title shall be submitted to course teacher in 2nd week of semester and course teacher will be approved title in 3rd week of semester.
Students shall be followed format of document give by the course teacher.
Late submission of document shall be penalized as 2% of total marks of each parameter per day for maximum five days after the deadline. In case, if a student has failed to meet the deadlines, he/she shall receive zero marks in particular parameter.
After submission of the document, the course teacher will verify the document and give suggestion. Students will resubmit the document after 10 days of the suggestive document given by the course teacher.
The detail evaluation of the Parameter-1 is mentioned below:
<table>
<tr><th>Parameter</th><th>Marks (10)</th></tr>
<tr><td>Problem Identification and Prevention Technique</td><td>4</td></tr>
<tr><td>Content Coverage</td><td>4</td></tr>
<tr><td>Document Formation</td><td>2</td></tr>
</table>

The detail evaluation of the Parameter-2 is mentioned below:
<table>
<tr><th>Parameter</th><th>Marks (10)</th></tr>
<tr><td>Incorporate suggestion given in documentation</td><td>2</td></tr>
<tr><td>Communication Skill</td><td>2</td></tr>
<tr><td>Technical Knowledge</td><td>6</td></tr>
</table>

</td>
</tr>
<tr>
<td>Document Format</td>
<td>Below format should be followed for the technical report

i. Title Page / Front Page
ii. Institute Certificate
iii. Declaration
iv. Table of Contents with page numbering
v. List of Tables, Figures, schemes
1. Abstract</td>
</tr>
</table>

[An abstract summarizes, usually in one paragraph of at least 300 words, the major aspects of the entire report in a prescribed sequence that includes: 1) the overall purpose of the study 2) major findings or trends found as a result of your analysis; and, 3) a brief summary of your interpretations and conclusions.]

2. Introduction
   [The main purpose of the introduction is to give a description of the topic. It should provide more detailed and specific information that is given further.]

3. Comparative study (Any three research paper)
   [Write overview of three research paper regarding the topic and write conclusion by comparing all the research paper.]

4. Case happened in India (Any three)
   [Write three cases happed in India based on the topic selection. The detail should be included in each case.]

5. Prevention Technique
   [After the studying all three research paper, identify the best prevention techniques and give detailed description of it in your own word.]

6. References
   [Enter the reference i.e. web, book or any other reference document taken. Reference Style: IEEE referencing standards shall be followed.]

Guideline for Report Formatting:

- Use A4 size page with 1" margin all sides.
- Header should include paper tile and footer should contain page number and enrollment numbers.
- Chapter Name should be of Cambria font, 20 points, Bold.
- Main Heading should be of Cambria font, 16 points, Bold.
- Sub Heading should be of Cambria font, 12 points, Bold.
- Sub heading of sub heading should be of Cambria font, 12 points, Bold, Italic.
- Paragraph should be of Cambria font, 12 points.
- Line spacing - 1.5 lines, before - 0, after - 0.

Refer following Title/front-page format.

<<TITLE IN CAPITAL LETTERS>>

Submitted By,

<<Student's Name (Enrollment Number)>>,

<<Student's Name (Enrollment Number)>>,

<<Student's Name (Enrollment Number)>>

Guided By,

<< Course Teacher Name>>

in partial fulfillment of the requirements

for the 6th Semester

Subject 030010608- SEC1 Fundamentals of Cyber Security

of Bachelor of Computer Application

Bhulabhai Vanmalibhai Patel Institute of Computer Science,

Uka Tarsadia University.

April, 2020.