CYBER LAW course deals with some of the major legal aspects of computing which are related to the various aspects of law. Some leading topics include cybercrimes, electronic and digital signatures, intellectual property, data protection and privacy and crimes in Information communication and technology. Students are exposed to the cyber laws in Malaysia which governs the process and dissemination of information digitally. This course also teaches students the importance of adhering to cyber laws and regulation in order to regulate and protect the ICT industry from misuse and illegal activities.

COURSE LEARNING OUTCOMES (CLO)

Upon completion of this course, students should be able to:

1. determine the various cyber laws, theoretically and practically, and importance of knowledge of the current cyber laws. (C3, PLO1)

2. response constructively to various issues pertaining to cyber law implementation. (C3, A2, PLO1, PLO3)

3. adhere to cyber law rules and regulation in handling security issues. (C4, A3, PLO1, PLO8)
SUMMARY

1.0 INTRODUCTION TO CYBER LAW

This topic focuses on Cyber Law and its needs. Students are required to understand the regulatory framework governing cyberspace.

2.0 THE CYBER CRIMES

This topic covers the cyber crimes and steps to be taken to prevent cyber crimes. Students are exposed to cyber crimes against persons, property and government.

3.0 UNDERSTAND THE ELECTRONIC AND DIGITAL SIGNATURES

This topic covers the electronic and digital signatures. Students will learn about the legal requirements in digital signatures and implantation of digital signatures in an electronic document.

4.0 INTELLECTUAL PROPERTY

This topic focuses on the intellectual property rights concepts. Students are exposed to the areas of Intellectual Properties such as copyrights, trademarks, laws, licenses and patterns.

5.0 PROTECTION, PRIVACY AND CRIMES IN ICT

This topic covers about data protection and privacy. Students will also be exposed to the crimes in Information Communication Technology, the crime acts and explain on computer related crimes.

DEPENDENT LEARNING COURSEWORK ASSESSMENT

RTA – Recommended Time Allocation
SST – Suggested Sequence of Topics
SYLLABUS

1.0  INTRODUCTION TO CYBER LAW

1.1  Understand the Cyber Law.
   1.1.1  Define Cyber Law.
   1.1.2  Explain the need for Cyber Law.
   1.1.3  Discuss the Cyber Law laws related to:
          a.  Cyber Crimes
          b.  Electronic and Digital Signatures
          c.  Intellectual Property
          d.  Data Protection and Privacy
   1.1.4  Differentiate between Cyber Law, Conversional Law and
          Conventional Law.

1.2  Discover the regulatory frameworks governing cyberspace.
   1.2.1  Explain the regulatory instruments provided by government:
          a.  Digital Signature Act 1997
          c.  Telemedicine Act 1997
          d.  Communications and Multimedia Act 1998
   1.2.2  Discuss the importance of regulatory frameworks.

2.0  CYBER CRIMES

2.1  Understand Cyber Crimes.
   2.1.1  Define Cyber Crimes.
   2.1.2  List the categories of cybercrime:
          a.  cybercrimes against persons
          b.  cybercrimes against property
          c.  cybercrimes against government
   2.1.3  Discuss the cybercrimes against persons:
          a.  trafficking
          b.  distribution
          c.  posting
          d.  dissemination of obscene material including pornography
             and indecent exposure
   2.1.4  Discuss the cybercrimes against property:
          a.  computer vandalism (destruction of others’ property)
          b.  transmission of harmful programmed
          c.  siphoning of funds from financial institutions
          d.  stealing secret information and data.
   2.1.5  Discuss the cybercrimes against government:
          a.  threaten the international governments
          b.  growth of global terrorism cracking on defense
             and government sites
          c.  intra-bank transfer of funds for terrorist activities
2.1.6 Relate the cyber crime categories to appropriate cyber laws govern by Malaysian Law.

2.2 Understand Cybercrime prevention.
2.2.1 Identify the preventative measures to avoid cybercrimes:
   a. increased awareness and capacity regarding information security
   b. adopted legal and regulatory frameworks to promote information security and address cybercrime.
   c. regional arrangements to address cybercrime and promote information security
   d. increased trust regarding internet-based transactions
   e. increased levels of network security.

2.2.2 Discuss preventative measures to be taken for a case study given.

3.0 ELECTRONIC AND DIGITAL SIGNATURES

3.1 Distinguish Electronic and Digital Signatures.
3.1.1 Explain the Electronic Signatures and Digital Signatures.
3.1.2 Describe the need for Electronic Signatures and Digital Signatures.
3.1.3 Compare Electronic Signatures and Digital Signatures.

3.2 Understand legal requirements in Digital Signatures.
3.2.1 Explain the three major legal requirements in Digital Signature:
   a. Signer authentication
   b. Message authentication
   c. Message integrity

3.2.2 Describe the implementation of Digital Signatures.
3.2.3 Examine the safety in a digital signature and handwritten signatures.
3.2.4 Explain legal effect in Electronic and Digital Signatures.
3.2.5 Point out the use of Digital Signature in an electronic document.

4.0 INTELLECTUAL PROPERTY

4.1 Understand the Intellectual Properties Rights concept.
4.1.1 Define Intellectual Properties Rights.
4.1.2 Identify the areas of Intellectual Properties:
   a. Copyright law: relating to computer software, source code, websites, cell phone content etc.
   b. Trademark law with relation to domain names, meta tags, mirroring, framing, linking etc.
   c. Semiconductor law which relates to the protection of semiconductor integrated circuits design and layouts.
   d. Patent law in relation to computer hardware and software.

4.1.3 Adhere to Intellectual Property Rights in computing aspects
4.2 Understand the Copyrights concept.
   4.2.1 Define Information Highway and Copyright
   4.2.2 Explain types of copying
      a. Literal copying
      b. Non-literal copying
   4.2.3 Discuss the use of Copyright Act 1987 in the following purpose:
      a. Software protection
      b. Multimedia protection
   4.2.4 State the advantages and disadvantages of protection under Copyright Act 1987.
   4.2.5 Define Copyright Infringement.
   4.2.6 Identify the three theories in Copyright Infringement:
      a. Direct infringement
      b. Contributory infringement
      c. Vicarious infringement

4.3 Understand the Trade Marks Law.
   4.3.1 Define trademark.
   4.3.2 Identify classifications of trademarks.
   4.3.3 Explain trademark infringement.
   4.3.4 Describe the areas of concern with respect to trademark infringement:
      a. Deep linking
      b. Metatags
      c. Framing
   4.3.5 Discuss the roles of the following bodies in trademark laws:
      a. WIPO (World Intellectual Property Organisation)
      b. ICANN (Internet Corporation for Assigned Names and Numbers)
      c. IAHC (The International Ad-Hoc Committee)

   4.4.1 Describe the structure of patent law
   4.4.2 Discuss the use of Patent Law in:
      a. Patentable invention
      b. Biotechnological invention
   4.4.3 Explain the infringement of patent.
   4.4.4 Explain the need to register for industrial design.
   4.4.5 Explain the infringement of industrial design and remedies.

5.0 PROTECTION, PRIVACY AND CRIMES IN ICT

5.1 Understand data protection and privacy.
   5.1.1 Define the data protection and privacy.
   5.1.2 Explain the purpose of data protection and privacy in:
      a. Collection Data
      b. Storing Data
      c. Transmitting Data
5.1.3 Discuss the use of the following laws for data protection and control:
   a. Personal Data Protection Act 2009
   b. Communication and Multimedia Act 1998

5.2 Discover the crimes in Information Communication Technology.
   5.2.1 Identify types of computer crimes.
   5.2.2 Explain authority, information and proceedings in computer crimes.
   5.2.3 Discuss Computer Crimes Act 1997.
   5.2.4 Give current examples of computer related crime cases
   5.2.5 Discuss the roles of crime controlling bodies:
       a. Communications and Multimedia Commission
       b. The Controller of Certification Authority
       c. Cyber Security Malaysia
       d. others
REFERENCES

Main:


Additional:


**MATRIX OF COURSE LEARNING OUTCOMES (CLO) VS PROGRAMME LEARNING OUTCOMES (PLO)**

<table>
<thead>
<tr>
<th>Course Learning Outcome (CLO)</th>
<th>Compliance to PLO</th>
<th>Recommended Delivery Methods</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Determine the various cyber laws, theoretically and practically, and importance of knowledge of the current cyber laws</td>
<td>√ PLO1, PLO2, PLO3</td>
<td>Interactive Lecture and Discussion</td>
<td>Test and Quiz Final Examination</td>
</tr>
<tr>
<td></td>
<td>PLO4, PLO5, PLO6, PLO7, PLO8, PLO9</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>C3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Response constructively to various issues pertaining to cyber law implementation.</td>
<td>√ PLO1, PLO2</td>
<td>Interactive Lecture, Discussion and Presentation</td>
<td>Test, Case Study, Discussion. Final Examination</td>
</tr>
<tr>
<td></td>
<td>PLO3, PLO4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>C3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Adhere to cyber law rules and regulation in handling security issues.</td>
<td>√ PLO1, PLO2, PLO3</td>
<td>Interactive Lecture, Discussion and Presentation</td>
<td>Quiz, Case Study, Discussion. Final Examination</td>
</tr>
<tr>
<td></td>
<td>PLO4, PLO5, PLO6, PLO7, PLO8, PLO9</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>C4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Remark:**
- LD 1 Knowledge
- LD 2 Practical Skills
- LD 3 Communication Skills
- LD 4 Critical Thinking and Problem Solving Skills
- LD 5 Social Skills and Responsibilities
- LD 6 Continuous Learning and Information Management Skills
- LD 7 Management and Entrepreneurial Skills
- LD 8 Professionalism, Ethics and Moral
- LD 9 Leadership and Teamwork Skills

*Version :090514_1.0_Effective: Jun 2014*
ASSESSMENT

The course assessment comprises two components namely:

i. Coursework Assessment (CA) – 50%
   Coursework assessments that measure knowledge, practical skills and generic skills are carried out in the form of continuous assessment. Coursework assessments total score comprises the knowledge and practical marks ONLY. It does not include the mark of generic skills.

ii. Final Examination Assessment (FE) – 50%
    Final examination is carried out at the end of the semester.

ASSESSMENT SPECIFICATION TABLE (AST)

<table>
<thead>
<tr>
<th>TOPICS</th>
<th>ASSESSMENT TASKS FOR COURSEWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CONTEXT</td>
</tr>
<tr>
<td>1. Determine the various cyber laws, theoretically and practically, and importance of knowledge of the current cyber laws. (C3, PLO1)</td>
<td>1</td>
</tr>
<tr>
<td>2. Response constructively to various issues pertaining to cyber law implementation. (C3, A2, PLO1, PLO3)</td>
<td>1</td>
</tr>
<tr>
<td>3. Adhere to cyber law rules and regulation in handling security issues. (C4, A3, PLO1, PLO8)</td>
<td>1</td>
</tr>
</tbody>
</table>

Remark

Topic 1 : Introduction To Cyber Law
Topic 2 : Cyber Crimes
Topic 3 : Electronic And Digital Signatures
Topic 4 : Intellectual Property
Topic 5 : Protection, Privacy And Crimes In Ict

Refers to the CLO to be assessed through the indicated assessment task.

*(#) # refers to the quantity of assessment

Indicates the topic (s) to be covered under the assigned/ identified assessment tasks. For merged topics, lecturers have the options of choosing the preferred topic (s).

The generic skills are to be assessed separately. The total score for generic skills is 100%. However, it is NOT PART of the coursework assessment mark.
# DISTRIBUTION OF STUDENT LEARNING TIME
## ACCORDING TO COURSE LEARNING - TEACHING ACTIVITY

<table>
<thead>
<tr>
<th>No.</th>
<th>Learning and Teaching Activity</th>
<th>SLT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DEPENDENT LEARNING</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>Delivery Method</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Lecture</td>
<td>30</td>
</tr>
<tr>
<td>1.2</td>
<td>Practical</td>
<td>0</td>
</tr>
<tr>
<td>1.3</td>
<td>Tutorial</td>
<td>30</td>
</tr>
<tr>
<td>2.0</td>
<td>Coursework Assessment (CA)</td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Lecture-hour-assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Test</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Quiz</td>
<td>3</td>
</tr>
<tr>
<td>2.2</td>
<td>Practical-hour-assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>None</td>
<td>3</td>
</tr>
<tr>
<td>2.3</td>
<td>Tutorial-hour-assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Discussion</td>
<td>2</td>
</tr>
<tr>
<td><strong>INDEPENDENT LEARNING</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.0</td>
<td>Coursework Assessment (CA)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Case Study</td>
<td>1</td>
</tr>
<tr>
<td>4.0</td>
<td>Preparation and Review</td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>Lecture</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Preparation before theory class eg: download lesson notes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Review after theory class eg: additional references, discussion group,discussion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Preparation for quizzes.</td>
<td></td>
</tr>
<tr>
<td>4.2</td>
<td>Practical</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Preparation before practical class/field work /survey eg: review notes, checklist/ labsheets and/or tools and equipment.</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Post practical activity eg: lab report, additional references and discussion session</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Preparation before studio work presentation/critique.</td>
<td></td>
</tr>
<tr>
<td>4.3</td>
<td>Tutorial</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Preparation for tutorial</td>
<td></td>
</tr>
<tr>
<td>4.4</td>
<td>Assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Preparation for Test.</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Preparation for final examination.</td>
<td>2</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>120</td>
</tr>
<tr>
<td></td>
<td>Credit</td>
<td>SLT/40</td>
</tr>
</tbody>
</table>

**Remark:**
1. Suggested time for
   - Quiz : 10 - 15 minutes
   - Test : 30 - 60 minutes
2. Laboratory Exercises are conducted during practical hours
3. 40 hours is equivalent to 1 credit