ISYS90002 Cyberlaw

Credit Points:	12.50
Level:	9 (Graduate/Postgraduate)
Dates & Locations:	2011, Hawthorn This subject commences in the following study period/s: Semester 1, Hawthorn - Taught on campus. Semester 2, Hawthorn - Taught on campus. Intensive mode
Time Commitment:	Contact Hours: 24 hours of face-to-face contact over an eight-week semester plus at least eight hours of pre-seminar reading Total Time Commitment: It is anticipated that students will need to allocate around 80 hours to undertake the assessable components of the subject to be completed in the three months encompassing the eight-week semester.
Prerequisites:	nil
Corequisites:	nil
Recommended Background Knowledge:	nil
Non Allowed Subjects:	nil
Core Participation Requirements:	For the purposes of considering requests for Reasonable Adjustments under the Disability Standards for Education (Cwth 2005), and Students Experiencing Academic Disadvantage Policy, academic requirements for this subject are articulated in the Subject Description, Subject Objectives, Generic Skills and Assessment Requirements of this entry. The University is dedicated to provide support to those with special requirements. Further details on the disability support scheme can be found at the Disability Liaison Unit website: http://www.services.unimelb.edu.au/disability/
Contact:	Melbourne Consulting and Custom Programs Level 3, 442 Auburn Rd Hawthorn VIC 3122 Phone: 9810 3148 Email: **mccp.enquiries@mccp.unimelb.edu.au (mailto:mccp.enquiries@mccp.unimelb.edu.au)**
Subject Overview:	**This course is no longer taking new enrolments. The last intake into this program was Semester 2, 2009.** This subject takes a comparative approach by examining Australian, United States and European law as it relates to the investigation and policing of electronic crime. The subject explores historical and current attempts to prevent, regulate and punish criminal activities involving information and communication technologies. Students are expected to contribute to the debate of issues raised throughout the subject. Topics covered include: • Recent law reforms such as the Cybercrime Act (Cth Australia), USA PATRIOT Act, Council of Europe Cybercrime Treaty; • Case studies of important court decisions; • Preparation of briefs of evidence for incidents involving digital evidence; • Admissibility and reliability of digital evidence in court proceedings.
Objectives:	Students who complete this subject successfully should be able to: • Demonstrate a thorough understanding of past and current law aimed at controlling electronic crime, including criminal law, privacy and data protection regimes and intellectual property laws; • Identify challenges to the law posed by electronic crime; • Analyse important court decisions affecting the interpretation of statute cyberlaw; • Identify civil remedies available to individuals and businesses; and • Identify and apply rules of evidence relating to the admissibility and reliability of digital evidence to evaluate practical issues in e-crime investigation.

Assessment:	Two written assignments and a practical exam totalling 6000 words.
Prescribed Texts:	NA
Recommended Texts:	nil
Breadth Options:	This subject is not available as a breadth subject.
Fees Information:	Subject EFTSL, Level, Discipline & Census Date, http://enrolment.unimelb.edu.au/fees
Generic Skills:	Please refer to MCCP website.
Links to further information:	http://www.mccp.unimelb.edu.au/courses/award-courses/masters/e-forensics-enterprise-security
Related Course(s):	Master of e-Forensics and Enterprise Security