# Course Change Proposal

## Form A

<table>
<thead>
<tr>
<th>Academic Group (College):</th>
<th>Academic Organization (Department):</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering and Computer Science</td>
<td>Computer Science</td>
<td>January 18, 2011</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type of Course Proposal:</th>
<th>Department Chair:</th>
<th>Submitted by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>New ___ Change X ___ Deletion ___</td>
<td>Cui Zhang</td>
<td>Isaac Ghansah</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Does this course fulfill a requirement for single-subject or multiple subject credential students?</th>
<th>For Catalog Copy:</th>
<th>Semester Effective:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes ___ No X ___</td>
<td>Yes X ___ No ___</td>
<td>Fall X ___ Spring ___, 2011</td>
</tr>
</tbody>
</table>

This course replaces experimental course Subject Area (prefix) and Catalog Nbr (course number): 

<table>
<thead>
<tr>
<th>If changing an existing course, should new version be considered a repeat of the original version? If so, the same Course ID will be maintained. If not, a new Course ID will be assigned. Note: In PeopleSoft terminology, the Course ID is the unique system identifier, not the Catalog Nbr.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes X ___ No ___</td>
</tr>
</tbody>
</table>

## Change from:

<table>
<thead>
<tr>
<th>Subject Area (prefix) &amp; Catalog Nbr (course no.):</th>
<th>Title:</th>
<th>Units:</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC 114</td>
<td>Digital Evidence and Computer Crime</td>
<td>3</td>
</tr>
</tbody>
</table>

## Change to:

<table>
<thead>
<tr>
<th>Subject Area (prefix) &amp; Catalog Nbr (course no.):</th>
<th>Title:</th>
<th>Units:</th>
</tr>
</thead>
<tbody>
<tr>
<td>same</td>
<td>same</td>
<td>same</td>
</tr>
</tbody>
</table>

## JUSTIFICATION:

Change in prerequisite only. Current catalog prerequisite is: CSC 10, CSC 80. The new catalog prerequisite is: CSC 1 and one of the following: CSC 8 or CSC 8S or CSC 80; or instructor’s permission. The current prerequisites are too restrictive. This change will allow non-major students more flexibility in taking this service course.

NEW COURSE DESCRIPTION: (Not to exceed 80 words, and language should conform to catalog copy. See http://www.csus.edu/ummanual/acad.htm - Guidelines for Catalog Course Description)

N/A

## Note:

Prerequisite: CSC 1 and one of the following: CSC 8 or CSC 8S or CSC 80; or instructor’s permission

Enforced at Registration: Yes X ___ No ___

Corequisite:

Enforced at Registration: Yes ___ No ___

Graded: Letter ___ Credit/No Credit ___

Instructor Approval Required? Yes ___ No ___

Course Classification (e.g., lecture, lab, seminar, discussion):

Title for CMS (not more than 30 characters)

Cross Listed?

Yes ___ No ___

If yes, do they meet together and fulfill the same requirement, and what is the other course.

How Many Times Can This Course be Taken for Credit?

Can the course be taken for Credit more than once during the same term? Yes ___ No ___
FOR NEW COURSE PROPOSALS OR SUBSTANTIVE CHANGES ONLY:

Description of the Expected Learning Outcomes: Describe outcomes using the following format: “Students will be able to: 1), 2), etc.” See the example at http://www.csus.edu/acaf/example.htm

**Attach a list of the required/recommended course readings and activities [Note: it is understood that these are updated and modified as needed by the instructor(s).] This attachment should be forwarded only to your Dean’s office, not Academic Affairs.

Assessment Strategies: A description of the assessment strategies (e.g., portfolios, examinations, performances, pre-and post-tests, conferences with students, student papers) which will be used by the instructor to determine the extent to which students have achieved the learning outcomes noted above:

---

For whom is this course being developed?
Majors in the Dept __ Majors of other Depts __ Minors in the Dept __ General Education __ Other __
Is this course required in a degree program (major, minor, graduate degree, certificate)? Yes __ No __
If yes, identify program(s):

Does the proposed change or addition cause a significant increase in the use of College or University resources (lab room, computer facilities, faculty, etc.)? Yes __ No __
If yes, attach a description of resources needed and verify that resources are available.

Indicate which department or programs will be affected by the proposed course (if any). __________________________

The Department Chair’s signature below indicates that affected programs have been sent a copy of this proposal form.

---

Accessibility: Following course approval, and prior to the start of the semester in which the new or revised course will be taught for the first time, an accessibility checklist [available at http://www.csus.edu/accessibility/checklist.html] shall be completed and submitted to the appropriate Dean’s office. An accessible syllabus shall also be made available online, preferably prior to the start of that semester’s open registration period.

Approvals: If proposed change, new course or deletion is approved, sign and date below. If not approved, forward without signing to the next reviewing authority, and attach an explanatory memorandum to the original copy.

Signatures: Date
Department Chair: ___________ 2/1/2011
College Dean or Associate Dean: ___________
CPSP (for school personnel courses ONLY) ___________
Associate Vice President and Dean for Academic Programs ___________

Distribution: Academic Affairs (original), Department Chair and College Dean. Dean’s office to send original after approval to Academic Affairs, at mail zip 6016. An electronic copy must also be sent.

5/20/2010
COURSE DESCRIPTION

Dept., Number  CSC 114  Course Title  Digital Evidence and Computer Crime  
Semester hours  3  Course Coordinator  Isaac Ghansah  
     URL (if any):  http://gaia.ecs.csus.edu/~ghansahi/

Catalog Description

Topics include technology and law, computer basics for digital investigations, network basics for 
digital investigations, investigation of computer crime and the handling of digital evidence. 
Prerequisite: CSC 1 and CSC 8 or CSC 8S or CSC 80 or Instructor’s permission

Textbook

Mark Merkow and James Breithaupt, Information Security: Principles and Practices, Prentice- 
Hall, 2006.

References


Course Goals

1. To develop knowledge of information security and assurance best practices.
2. To develop understanding of the importance of securing information efficiently, the threats, 
risks, and vulnerabilities to information, and the controls available to address these threats.
3. To study management practices and proficiency in the use of selected software tools for 
securing systems.

Prerequisites by Topic

Thorough understanding of:
• Webpage design and layout including HTML tables and forms.

Basic understanding of:
• Fundamental properties of algorithms and programming.
• How to use Windows and/or Linux operating systems.

Exposure to:
• Elementary working knowledge of a commonly used applications programming language.
• Internet protocols such as HTTP and TCP/IP.
Major Topics Covered in the Course

1. Introduction to Information Assurance and Security, threats to information, importance of information security (3 hours).
2. Risk assessment and security management (3 hours).
3. How contemporary computer systems are organized (1 hour).
4. Access control techniques and models including 2-factor authentication, social engineering, and biometrics (3 hours).
5. Telecommunications, network security and network fundamentals: logical and physical topologies, introduction to TCP/IP, and hardware architecture (6 hours).
6. Cryptography including Advanced Encryption Standard (3 hours).
7. Security architecture and models (3 hours).
8. Operations security (3 hours).
9. Applications, system development, and database security (3 hours).
10. Business continuity planning – disaster recovery planning (3 hours).
11. Law, investigation, ethics, U.S. Patriot Act, Digital Millennium Copyright Act (DMCA), and recent rulings (3 hours).
12. Introduction to host-based perimeter detection and network-based perimeter detection, physical security (3 hours).
13. Methods of attacks, Honeypots and Honeynets, firewalls and perimeters, trap and trace tools such as Echelon (3 hours).
14. Government information assurance regulations (3 hours).
15. System security engineering, future threats and countermeasures (2 hours).

Outcomes

Thorough understanding of:
- Information Assurance and Security best practices.
- Threats, risks, and vulnerabilities to information systems; countermeasures available to address these threats.

Basic understanding of:
- Internet/web security.
- Host security.
- Tools for information security.

Exposure to:
- Cyber forensics.
- TCP/IP protocol suite.
- Career paths in information security.
- Ethical issues related to information security.
- Policy and administration of site security.
Laboratory Projects

1. Windows and Linux/Unix vulnerability analysis.
2. Internet research and reporting on security topics such as biometrics, computer system laws, certifications, security advisories, etc.
3. Linux and Windows security tools and techniques.
4. Security reporting, monitoring and auditing.
5. File system security and cryptography.
6. Use of hands-on hacking tools such as nmap.
7. Firewalls, personal and commercial grade.

Estimated Curriculum Category Content (Semester hours)

<table>
<thead>
<tr>
<th>Area</th>
<th>Core</th>
<th>Advanced</th>
<th>Area</th>
<th>Core</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithms</td>
<td></td>
<td></td>
<td>Data Structures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Design</td>
<td></td>
<td></td>
<td>Prog. Languages</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp. Arch.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Oral and Written Communications

Students will be required to write a term paper on information security issues.

Social and Ethical Issues

It will be made clear that the students should not use their knowledge and skills with any malicious intent against the university network, any other networks, physical computing resources, or humans. Students will be required to sign an agreement to observe a set of legal and ethical guidelines.

Theoretical Content

The course covers an overview of cryptographic algorithms and applies cryptography to secure communication applications. Access control principles are also covered.

Problem Analysis

A given configured system will be analyzed in a rigorous manner to determine to what extent it is secure.

Solution Design

Students will learn how to discover security weaknesses and mitigate the identified weakness in the system.

/sj