TRIAL COURSE OR NEW COURSE PROPOSAL

SUBMITTED BY:

<table>
<thead>
<tr>
<th>Department</th>
<th>College/School</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Systems Technologies, IT Specialist Program</td>
<td>CRCD</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prepared by</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keith Swarner</td>
<td>455-2820</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Email Contact</th>
<th>Faculty Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:keith.swarner@uaf.edu">keith.swarner@uaf.edu</a></td>
<td><a href="mailto:keith.swarner@uaf.edu">keith.swarner@uaf.edu</a>/455-2820</td>
</tr>
</tbody>
</table>

See [http://www.uaf.edu/uafgov/faculty/cd/cdman.html](http://www.uaf.edu/uafgov/faculty/cd/cdman.html) for a complete description of the rules governing curriculum & course changes.

1. ACTION DESIRED (check one):
   - Trial Course
   - New Course
   - X

2. COURSE IDENTIFICATION:
   - Dept: CITS
   - Course #: 261
   - No. of Credits: 3

Justify upper/lower division status & number of credits:

This course will provide students with an introduction to computer and information security and would be appropriate for students entering their second semester of the IT Specialist associate degree program.

Approximately the following amount of instructional time will be delivered in each of the following major topic areas (Note: the terminology used in the following list is generic language and will not necessarily match perfectly with the topics language used on the sample syllabus being submitted with this new course form): Information Security Overview, 1 hr.; Importance of Network Security, 1 hr.; Professional Certifications and Careers in Information Security, .5 hrs.; Attacker Profiles and Attacker Motives, .5 hrs.; Identity Attacks, Denial of Service Attacks, and Malicious Code (Malware), 2.5 hrs.; Information Security Responsibilities, .5 hrs.; Creating and Maintaining Information Security Schemes, 1.5 hrs.; Security Principles, .5 hrs.; Authentication Methods and Access Control Methods, 1 hr.; System Auditing Schemes, .5 hrs.; Security Baselines, 1 hr.; Disabling and Removing Non-Essential Services, Applications and Systems, 1 hr.; Hardening Operating Systems, Applications, and Networks, 2 hrs.; Securing Network Infrastructure and Hardening Network Devices, 2 hrs.; Designing Secure Network Topologies, 1 hr.; Attacks Against: E-Mail Systems, Web Applications, and Instant Messaging Applications, 1 hr.; Securing Web Communications, Instant Messaging, and Other Communication Applications, 2 hrs.; Hardening File Transfer Protocol (FTP), .5 hrs.; Securing Remote Access, .5 hrs.; Protecting Directory Services, .5 hrs.; Securing Digital Cellular Telephony, .5 hrs.; Hardening Wireless Local Area Networks (WLAN), .5 hrs.; Encryption Overview, 1 hr.; Cryptography Hashing Algorithms, .5 hrs.; Symmetric Encryption Algorithms, .5 hrs.; Asymmetric Encryption Algorithms, 1 hr.; Cryptography Strengths and Vulnerabilities, 1 hr.; Public Key Encryption (PKI), 1 hr.; Digital Certificates and Key Management, 1 hr.; Physical Security Perimeters, .5 hrs.; Social Engineering, .5 hrs.; Access Controls, .5 hrs.; Business Continuity Plans, 1 hr.; Information Security Policies and Procedures, 1.5 hrs.; Security Policy Cycle, .5 hrs.; Asset and Risk Identity, .5 hrs.; Security Policy Development, .5 hrs.; Security Policy Establishment, Compliance, and Evaluation, 1 hr.; Identity Management, .5 hrs.; Change Management, .5 hrs.; Digital Rights Management, 1 hr.; Training and Education, .5 hrs.; Computer Forensics, 1.5 hrs.; Responding To Computer Forensic Incidents, 1 hr.; Security Careers and Required Job Skills, .5 hrs.

3. PROPOSED COURSE TITLE:
   - Computer and Information Security

4. CROSS LISTED? YES/NO
   - No
   - If yes, Dept: NA
   - Course #: NA

(Requires approval of both departments and deans involved. Add lines at end of form for such signatures.)

5. STACKED? YES/NO
   - No
   - If yes, Dept: NA
   - Course #: NA
**6. FREQUENCY OF OFFERING:**
As Demand Warrants
(Every or Alternate) Fall, Spring, Summer — or As Demand Warrants

**7. SEMESTER & YEAR OF FIRST OFFERING**
Fall 2009

**8. COURSE FORMAT:**
NOTE: Course hours may not be compressed into fewer than three days per credit. Any course compressed into fewer than six weeks must be approved by the college or school's curriculum council. Furthermore, any core course compressed to less than six weeks must be approved by the core review committee.

<table>
<thead>
<tr>
<th>COURSE FORMAT:</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>X</th>
<th>6 weeks to full semester</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTHER FORMAT (specify)</td>
<td>NA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mode of delivery (specify lecture, field trips, labs, etc)</td>
<td>Lecture</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**9. CONTACT HOURS PER WEEK:**

| LECTURE hours/weeks | 3 |
| LAB hours/week | 0 |
| PRACTICUM hours/week | 0 |

Note: # of credits are based on contact hours. 800 minutes of lecture=1 credit. 2400 minutes of lab in a science course=1 credit. 1600 minutes in non-science lab=1 credit. 2400-4800 minutes of practicum=1 credit. 2400-8000 minutes of internship=1 credit. This must match with the syllabus. See [http://www.uaf.edu/uafgov/faculty/cd/credits.html](http://www.uaf.edu/uafgov/faculty/cd/credits.html) for more information on number of credits.

| OTHER HOURS (specify type) | NA |

**10. COMPLETE CATALOG DESCRIPTION including dept., number, title and credits (50 words or less, if possible):**

**CITS F261  Computer and Information Security**
3 Credits    Offered As Demand Warrants
This course teaches students the fundamental concepts of computer and information security. Course topics include: understanding threats to a computing infrastructure; securing a computing and network infrastructure; understanding encryption technologies; securing communications and applications; security policies and responding to incidents. **Prerequisite:** CITS 204 or 241 or instructor approval. (3+0)

**11. COURSE CLASSIFICATIONS:** (undergraduate courses only. Use approved criteria found on Page 10 & 17 of the manual. If justification is needed, attach on separate sheet.)

<table>
<thead>
<tr>
<th>H = Humanities</th>
<th>N = Natural Science</th>
<th>S = Social Sciences</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>X</td>
<td>NO</td>
</tr>
</tbody>
</table>

IF YES, check which core requirements it could be used to fulfill:

<table>
<thead>
<tr>
<th>O = Oral Intensive, Format 6</th>
<th>W = Writing Intensive, Format 7</th>
<th>Natural Science, Format 8</th>
</tr>
</thead>
</table>
### 12. COURSE REPEATABILITY:

<table>
<thead>
<tr>
<th>Is this course repeatable for credit?</th>
<th>YES</th>
<th>NO</th>
</tr>
</thead>
</table>

Justification: Indicate why the course can be repeated (for example, the course follows a different theme each time).

| | NA |

How many times may the course be repeated for credit?

| | NA TIMES |

If the course can be repeated with variable credit, what is the maximum number of credit hours that may be earned for this course?

| | NA CREDITS |

### 13. GRADING SYSTEM:

<table>
<thead>
<tr>
<th>LETTER</th>
<th>PASS/FAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

### 14. PREREQUISITES

CITS 204 or 241 or instructor approval

These will be *required* before the student is allowed to enroll in the course.

#### RECOMMENDED

None

#### RECOMMENDED

Classes, etc. that student is strongly encouraged to complete prior to this course.

### 15. SPECIAL RESTRICTIONS, CONDITIONS

None

### 16. PROPOSED COURSE FEES

None

### 17. PREVIOUS HISTORY

Has the course been offered as special topics or trial course previously? Yes/No

<table>
<thead>
<tr>
<th>Yes/No</th>
<th>No</th>
</tr>
</thead>
</table>

If yes, give semester, year, course #, etc.:

| NA |

### 18. ESTIMATED IMPACT

**WHAT IMPACT, IF ANY, WILL THIS HAVE ON BUDGET, FACILITIES/SPACE, FACULTY, ETC.**

It is anticipated that an adjunct instructor will be hired to teach this course. If course enrollments are not sufficient to meet the costs of hiring an adjunct, the course will not be offered; or depending on enrollments in other courses, the teaching load of a full-time faculty may be adjusted.

### 19. LIBRARY COLLECTIONS

Have you contacted the library collection development officer (ffklj@uaf.edu, 474-6695) with regard to the adequacy of library/media collections, equipment, and services available for the proposed course? If so, give date of contact and resolution. If not, explain why not.

<table>
<thead>
<tr>
<th>No</th>
<th>Yes</th>
<th>X</th>
</tr>
</thead>
</table>

Karen Jensen, the collection development officer for the library, was contacted by email on 9/29/2008. We don’t anticipate the need for any...
20. IMPACTS ON PROGRAMS/DEPTS
What programs/departments will be affected by this proposed action?
Include information on the Programs/Departments contacted (e.g., email, memo)

ITS. All CRCD CIOS faculty from the following campus have been contacted regarding this change:
IAC, KuC, NWC, TVC.

21. POSITIVE AND NEGATIVE IMPACTS
Please specify positive and negative impacts on other courses, programs and departments resulting from the proposed action.

Positive Impacts: This course will serve as a required course for the Network and System Administration concentration of the IT Specialist A.A.S. degree program. The addition of this course will provide IT Specialist degree students with a greater comprehensive understanding of security topics, issues and concerns that are covered with brevity in other coursework within the degree program. CITS 204 Introduction to Network Support and Administration, CITS 212 Server Operating Systems, and CITS 241 Networking and LAN Infrastructure Basics are examples of course that include security topics; however the scope coverage in each course is brief and focused only on security as it relates to the specific technologies covered within each course.

JUSTIFICATION FOR ACTION REQUESTED
The purpose of the department and campus-wide curriculum committees is to scrutinize course change and new course applications to make sure that the quality of UAF education is not lowered as a result of the proposed change. Please address this in your response. This section needs to be self-explanatory. Use as much space as needed to fully justify the proposed course.

Over the past nine month faculty within the IT Specialist program have been actively collaborating and seeking input from our community advisory council, recent graduates, and the UAF Computer Science department with the goal of streamlining and improving the educational opportunities provided through the certificate and associate degree programs. One of the significant outcomes of this process was the decision to offer three concentrations that will enable students to develop a comprehensive and an in-depth set of skills and knowledge within specific area of information technology; rather than a less comprehensive set of skills and knowledge over a broader range of information technology areas.

As was mentioned under item 21, this course will serve as a required course for the Network and System and Administration concentration of the IT Specialist A.A.S. degree program. Increasingly, information technology employers expect the individuals they hire to poses a fundamental knowledge of computer and information security. The addition of this comprehensive computer and information security course will enable us to prepare graduates that meet these employer expectations.
<table>
<thead>
<tr>
<th>Signature, Chair, Program/Department of:</th>
<th>IT Specialist Program</th>
<th>Date: 10/6/2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature, CRCD Division Coordinator for:</td>
<td>Business Systems Technology</td>
<td>Date:</td>
</tr>
<tr>
<td>Signature, Chair, College/School Curriculum Council for:</td>
<td>College of Rural and Community Development</td>
<td>Date:</td>
</tr>
<tr>
<td>Signature, Dean, College/School of:</td>
<td>College of Rural and Community Development</td>
<td>Date:</td>
</tr>
<tr>
<td>Signature of Provost (if applicable)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Offerings above the level of approved programs must be approved in advance by the Provost.

| Signature, Chair, UAF Faculty Senate Curriculum Review Committee | Date: |

**ADDITIONAL SIGNATURES: (If required)**

<table>
<thead>
<tr>
<th>Signature, Chair, Program/Department of:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature, Chair, College/School Curriculum Council for:</td>
<td>Date:</td>
</tr>
<tr>
<td>Signature, Dean, College/School of:</td>
<td>Date:</td>
</tr>
</tbody>
</table>
ATTACH COMPLETE SYLLABUS (as part of this application).

Note: syllabus must follow the guidelines discussed in the Faculty Senate Guide http://www.uaf.edu/uafgov/faculty/cd/syllabus.html.
The department and campus wide curriculum committees will review the syllabus to ensure that each of the items listed below are included. If items are missing or unclear, the proposed course change will be denied.

SYLLABUS CHECKLIST FOR ALL UAF COURSES
During the first week of class, instructors will distribute a course syllabus. Although modifications may be made throughout the semester, this document will contain the following information (as applicable to the discipline):

1. **Course information:**
   - Title, number, credits, prerequisite, location, meeting time 
   (make sure that contact hours are in line with credits).

2. **Instructor (and if applicable, Teaching Assistant) information:**
   - Name, office location, office hours, telephone, email address.

3. **Course readings/materials:**
   - Course textbook title, author, edition/publisher.
   - Supplementary readings (indicate whether required or recommended) and any supplies required.

4. **Course description:**
   - Content of the course and how it fits into the broader curriculum;
   - Expected proficiencies required to undertake the course, if applicable.
   - Inclusion of catalog description is strongly recommended, and 
   - Description in syllabus must be consistent with catalog course description.

5. **Course Goals (general) and Student Learning Outcomes (more specific)**

6. **Instructional methods:**
   - Describe the teaching techniques (eg: lecture, case study, small group discussion, private instruction, studio instruction, values clarification, games, journal writing, use of Blackboard, audio/video conferencing, etc.).

7. **Course calendar:**
   - A schedule of class topics and assignments must be included. Be specific so that it is clear that the instructor has thought this through and will not be making it up on the fly (e.g. it is not adequate to say “lab”. Instead, give each lab a title that describes its content). You may call the outline Tentative or Work in Progress to allow for modifications during the semester.

8. **Course policies:**
   - Specify course rules, including your policies on attendance, tardiness, class participation, make-up exams, and plagiarism/academic integrity.

9. **Evaluation:**
   - Specify how students will be evaluated, what factors will be included, their relative value, and 
   - how they will be tabulated into grades (on a curve, absolute scores, etc.)

10. **Support Services:**
    - Describe the student support services such as tutoring (local and/or regional) appropriate for the course.

11. **Disabilities Services:**
    - The Office of Disability Services implements the Americans with Disabilities Act (ADA), and insures that UAF students have equal access to the campus and course materials.
    - State that you will work with the Office of Disabilities Services (203 WHIT, 474-7043) to provide reasonable accommodation to students with disabilities.
Course Syllabus
CITS F261 Computer and Information Security
University of Alaska Fairbanks

Course Information
Course Number-Section, Title: CITS F261 TE1 Computer and Information Security
Number of Credits: 3.0
Prerequisite: CITS 204 or 241 or permission of the instructor.
Class Location: UAF Downtown Center, Room 210
Meeting Days & Time: Thursday, 6:00-9:00 PM, 9/4 – 12/18.
This course will consist of one 3-hour class lecture delivered to students once a week for 14 weeks. Students can expect to spend an additional six to nine hours per week outside of scheduled classroom lecture studying lecture material, completing reading assignments and homework. A final exam will be given during the 15th week.

Instructor Information
Name: Keith Swarner
Office Location: UAF Downtown Center, 510 Second Ave, Fairbanks AK, room 210B
Office Hours: 2:00 pm – 4:30 pm Monday, Tuesday and Thursday or by appointment
Telephone: 455-2820
Email: keith.swarner@uaf.edu

Course Readings/Materials
Required textbook/materials:
Title: Security+ Guide to Network Security Fundamentals
Author(s): Mark Ciampa
Publisher: Course Technology

Recommended textbook/materials: None

Course Description
This course teaches students the fundamental concepts of computer and information security. Course topics include: understanding threats to a computing infrastructure; securing a computing and network infrastructure; understanding encryption technologies; securing communications and applications; security policies and responding to incidents.

Course Goals
Upon successful completion of this course, the student will be able to define, explain, or perform tasks related to the following:
1. Threat Analysis and Risk Assessment
2. Authorization, Access Control, and Auditing
3. Security Baselines
4. Hardening Information Systems Hardware and Software
5. Encryption Technologies and Public Key Infrastructure (PKI)
6. Network Infrastructure Security
7. Securing Communication Applications
8. Security Policies, Procedures
9. Security Management
Student Learning Outcomes
Upon successful completion of this course, the student will be able to:

1. Describe the components of risk assessment
2. Identify common threats to a computing infrastructure
3. Describe common types of attacks and malicious code
4. List common defenses against threats
5. Identify and differentiate access control and authentication methods
6. Choose authentication and access control strategies
7. Describe trusted computing bases
8. Explain the role of security baselines and establish, monitor, and maintain a security baseline
9. Explain how to harden network devices
10. Explain how to harden server operating systems
11. Secure removable media; secure mobile devices; securely dispose of equipment
12. Describe basic principles and uses of cryptography
13. Explain the uses of symmetric encryption; the uses of hash functions; and the uses of public key encryption
14. Describe how cryptography is applied
15. Explain what certificates are and how they are used
16. Describe how a public key infrastructure (PKI) distributes cryptographic keys
17. Describe the certificate life cycle
18. Explain how trust models allow a PKI to function
19. Describe practical applications of a public key infrastructure (PKI)
20. Describe how features of TCP/IP relate to network security
21. Explain vulnerabilities that occur at various TCP/IP layers
22. Describe security for network cabling; as well as, security for network connectivity devices
23. Explain how to secure remote connections
24. Describe how to secure wireless communications
25. Describe how to use Internet Protocol Security (IPSec) to secure network communications
26. Establish secure topologies—secure network perimeters; implement firewalls
27. Identify common attacks against Web servers; explain how to protect against these attacks
28. Identify common attacks against Web browsers; explain how to protect against these attacks
29. Identify common attacks against common Internet applications; explain how to protect against these attacks
30. Identify common attacks against databases; explain how to protect against these attacks
31. Identify common attacks against Domain Name System (DNS); explain how to protect against these attacks
32. Identify common attacks against DHCP; explain how to protect against these attacks
33. Explain basic concepts of Internet messaging and how to secure instant messaging (IM)
34. Describe how to secure mail servers and mail clients
35. Identify methods for protecting business continuity
36. Identify steps for establishing site security
37. Maintain documentation, policies, and procedures
38. Apply basic security guidelines
39. Respond to security incidents
40. Describe procedures for detecting intrusion attempts
41. Assess risks
42. Establish security education
43. Resolve ethical dilemmas

Instructional Methods
This course teaches students through lectures, demonstrations, and instructor-led discussions. Students are expected to complete required reading assignments prior to each lecture. Students are expected to complete assigned homework during the week that follows that topic’s lecture and to arrive prepared to discuss homework at the beginning of the following week’s class.

Course Policies
Attendance: You are expected to attend classes regularly; unexcused absences may result in a failing grade. You are responsible for coordinating absences and the possibility of arranging to make up missed work with the instructor prior to the absence.

If an unforeseen circumstance prevents you from attending class you are expected to contact the instructor via email or phone prior to the start of the next class.

If you are required to participate in either (a) military or (b) UAF-sponsored activities that will cause you to miss class, you must notify your instructor as soon as possible of your absence. You must notify your instructor of all scheduled UAF-required absences for the semester (e.g., travel to athletic events) during the first week of classes.

Late Assignments: Late assignments will not be accepted unless arranged with the instructor.

Missed Exams: There will be no opportunity to make up exams except for pre-arranged absences with the instructor. Make-up exams must be completed prior to the next class meeting from which the exam was given.

Important Dates: Check the UAF Academic Calendar for important dates related to fee payment, class registration and last day to drop courses. The calendar can be viewed online at: http://www.uaf.edu/catalog/current/acad_calendar.html

Plagiarism/Academic integrity: Plagiarism and cheating are serious offenses and may result in failure on exams, papers, projects, or the course.

Support Services
The TVC Student Assistance and Advising Center provides services that contribute to a successful learning experience and transition to a career. TVC Student Assistance and Advising Center staff recognizes the unique concerns of adult and returning students. Services include pre-admission advising, academic assessment and placement advising, financial aid information and application, and assistance with choosing a major. Students can receive ongoing academic advising, degree planning and assistance with course selections.

Services are available by appointment and on a walk-in basis. Appointments can be scheduled by calling 455-2800 or students can go to the UAF Tanana Valley Campus Center, 604 Barnette Street, room 110.

Disability Services
The UAF Office of Disability Services implements the Americans with Disabilities Act (ADA), and insures that UAF students have equal access to the campus and course materials. The instructor will work the Office of Disability Services to provide reasonable accommodations to students with disabilities that have been documented through the UAF Office of Disability Services. Information about available services is available online at http://www.uaf.edu/disability/. The office can be reached by phone at 474-7043 or students can go to 203 WHIT on the UAF main campus.
**Evaluation:**

Final grades are calculated from the points earned in the following areas:

**Chapter Homework** ........................................................................................................................................... 15%

The purpose of these assignments is to provide an opportunity to complete and receive regular instructor feedback on course topics that will be assessed on mid-term and final exams. The tasks and questions in each homework assignment are based on textbook, supplemental reading and activities located on the Blackboard class site.

**Chapter Quizzes** ........................................................................................................................................... 25%

Chapter quizzes are designed to reinforce and measure retention of information covered in reading assignments and in lecture. Chapter quizzes will be available at the class Blackboard site must be completed outside of class the week following the completion of the class lecture for that chapter.

**Midterm Exam** ........................................................................................................................................... 25%

The midterm exam will provide an assessment of the students use and retention of course material covered in weeks 1-6.

**Final Exam** ........................................................................................................................................... 35%

The Final Exam is a comprehensive assessment of the student’s use and retention of course material covered in weeks 1-15. Exam will consist of both short answer and scenario-based multiple choice questions designed to measure student competency in the student learning outcomes defined for this class.

Letter grades for the course will be determined as follows and will reflect the Grading System and Grade Point Average Computation policy stated in the current UAF Catalog.

<table>
<thead>
<tr>
<th>Grade</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+</td>
<td>100–97%</td>
</tr>
<tr>
<td>A</td>
<td>96–93%</td>
</tr>
<tr>
<td>A-</td>
<td>92–90%</td>
</tr>
<tr>
<td>B+</td>
<td>89–87%</td>
</tr>
<tr>
<td>B</td>
<td>86–83%</td>
</tr>
<tr>
<td>B-</td>
<td>82–80%</td>
</tr>
<tr>
<td>C+</td>
<td>79–77%</td>
</tr>
<tr>
<td>C</td>
<td>76–73%</td>
</tr>
<tr>
<td>C-</td>
<td>72–70%</td>
</tr>
<tr>
<td>D+</td>
<td>69–67%</td>
</tr>
<tr>
<td>D</td>
<td>66–63%</td>
</tr>
<tr>
<td>D-</td>
<td>62–60%</td>
</tr>
<tr>
<td>F</td>
<td>less than 60%</td>
</tr>
</tbody>
</table>

**Withdrawal** – Course withdrawals may be either student-initiated or faculty-initiated. A faculty-initiated withdrawal will be initiated if you don't meet prerequisites for a course or if you haven’t participated substantially in the course. An attempt will be made to contact students prior to initiating a faculty-initiated withdrawal. It is the responsibility of the student to maintain current contact information (phone number and email address) within UA Online system.

**Incomplete** - An incomplete is a temporary grade used to indicate that the student has satisfactorily completed (C or better) the majority of work in a course but for personal reasons beyond the student’s control, such as sickness, has not been able to complete the course during the regular semester. An incomplete will only be assigned in a case when the student is current in the class until at least the last three weeks of the course. Negligence or indifference is not acceptable reasons for an “I” grade. If an incomplete assigned, it must be made up within one year or it will automatically be changed to an “F” grade.
Course Syllabus: CITS 261 Computer and Information Security

Course Calendar:
The following course calendar provides a weekly schedule of major course topics, reading assignments, homework assignments, and quizzes and exams. Students are expected to complete the reading assignment prior to the week in which the assignment is listed. Homework assignments are to be completed outside of schedule class time during the week after the course topic has been covered in class. Students should be prepared to discuss homework at the beginning of the following class.

Week 1 – Class 1
Reading Assignment: Chapter 1 Information Security Fundamentals
Topics: Overview of information security and associated terminology; Importance of network security; Professional Certifications Overview; Careers in Information Security
Chapter Homework: Homework Assignment 1
Chapter Quiz: Chapter 1 Quiz on Blackboard

Week 2 – Class 2
Reading Assignment: Chapter 2 Attackers and their Attacks
Topics: Attacker profiles; Attacker motives; Overview of types of attacks; Identity attacks; Denial of service attacks; Malicious code (malware)
Chapter Homework: Homework Assignment 2
Chapter Quiz: Chapter 2 Quiz

Week 3 – Class 3
Reading Assignment: Chapter 3 Security Basics
Topics: Information Security Responsibilities; Overview of creating and maintaining information security schemes; Security Principles; Authentication methods; Access Control methods; System auditing schemes
Chapter Homework: Homework Assignment 3
Chapter Quiz: Chapter 3 Quiz on Blackboard

Week 4 – Class 4
Reading Assignment: Chapter 4 Security Baselines
Topics: Overview of security baselines; Establishing security baselines; Disabling and removing non-essential services, applications and systems; Hardening operating systems; Hardening applications; Hardening networks.
Chapter Homework: Homework Assignment 4
Chapter Quiz: Chapter 4 Quiz on Blackboard

Week 5 – Class 5
Reading Assignment: Chapter 5 Securing the Network Infrastructure
Topics: Securing network infrastructure; hardening communication links; securing removable media; Network devices and security; Hardening network devices; Designing secure network topologies
Chapter Homework: Homework Assignment 5
Chapter Quiz: Chapter 5 Quiz on Blackboard
Week 6 – Class 6
Reading Assignment: Chapter 6 Web Security
Topics: Overview of communication applications and their vulnerabilities; Types of attacks against: e-mail systems, Web applications, and instant messaging applications. Securing communication applications overview; Securing Web communications; Secure instant messaging
Chapter Homework: Homework Assignment 6
Chapter Quiz: Chapter 6 Quiz on Blackboard

Week 7 – Class 7
Midterm Exam: The midterm exam will provide an assessment of the students use and retention of course material covered in weeks 1-6.

Week 8 – Class 8
Reading Assignment: Chapter 7 Protecting Advanced Communications
Topics: Securing advanced communications; Hardening File Transfer Protocol (FTP); Securing remote access; Protecting directory services; Securing digital cellular telephony; Hardening wireless local area networks (WLAN)
Chapter Homework: Homework Assignment 7
Chapter Quiz: Chapter 7 Quiz on Blackboard

Week 9 – Class 9
Reading Assignment: Chapter 8 Scrambling Through Cryptography
Topics: Encryption overview; How encryption protects data; Basics of cryptography and common terminology; Securing data with cryptography hashing algorithms; Protecting data with symmetric encryption algorithms; hardening data with asymmetric encryption algorithms; how to use cryptography
Chapter Homework: Homework Assignment 8
Chapter Quiz: Chapter 8 Quiz on Blackboard

Week 10 – Class 10
Reading Assignment: Chapter 9 Using and Managing Keys
Topics: Cryptography strengths and vulnerabilities; Overview of Public Key Encryption (PKI); Managing digital certificates; Key management
Chapter Homework: Homework Assignment 9
Chapter Quiz: Chapter 9 Quiz on Blackboard

Week 11 – Class 11
Reading Assignment: Chapter 10 Operational Security
Topics: Establishing physical security perimeters; Securing the physical environment; Minimizing social engineering, Using access controls; Establishing business continuity plans; Planning for disaster recovery from attackers and natural disasters.
Chapter Homework: Homework Assignment 10
Chapter Quiz: Chapter 10 Quiz on Blackboard
Week 12 – Class 12
Reading Assignment: Chapter 11 Policies and Procedures
Topics: Information security policies and procedures; Security policy cycle; Asset and risk identity; Security policy development; Monitoring compliance with established policies; Strategies for continuously evaluating established policies
Chapter Homework: Homework Assignment 11
Chapter Quiz: Chapter 11 Quiz on Blackboard

Week 13 – Class 13
Reading Assignment: Chapter 12 Security Management
Topics: Overview of identity management; Hardening systems through privilege management; Change management; Digital rights management; Training and education
Chapter Homework: Homework Assignment 12
Chapter Quiz: Chapter 12 Quiz on Blackboard

Week 14 – Class 14
Reading Assignment: Chapter 13 Advanced Security and Beyond
Topics: Overview of computer forensics; Responding to computer forensic incidents; New technology solutions available to harden security; Security careers and required job skills
Chapter Homework: Homework Assignment 13
Chapter Quiz: Chapter 13 Quiz on Blackboard

Week 15 – Class 15
Final Exam: The Final Exam is a comprehensive assessment of the student’s use and retention of course material covered in weeks 1-15. Exam will consist of both short answer and scenario-based multiple choice questions designed to measure student competency in the student learning outcomes defined for this class.