10/4/2012

Submit original with signatures + 1 copy + electronic copy to Faculty Senate (Box 7500).
See http://www.uaf.edu/uafgov/faculty-senate/curriculum/course-degree-procedures-/ for a
complete description of the rules governing curriculum & course changes.

## TRIAL COURSE OR NEW COURSE PROPOSAL

**SUBMITTED BY:**

| | | | |
|---|---|---|---|
| Department | CITS | College/School | CRCD |
| Prepared by | Keith Swarner | Phone | 455-2820 |
| Email Contact | keith.swarner@alaska.edu | Faculty Contact | Keith Swarner |

**1. ACTION DESIRED (CHECK ONE):** Trial Course [ ]  New Course [X]

**2. COURSE IDENTIFICATION:** Dept CITS  Course # F262  No. of Credits 3

Justify upper/lower division status & number of credits:

This course will build upon the skills and knowledge developed in CITS F261 and will develop the student's knowledge and ability to implement defensive security measures within a network environment. This course is appropriate for students who are entering their second or third semester of the IT Specialist associate degree program.

**3. PROPOSED COURSE TITLE:** Cybersecurity Defense and Countermeasures

**4. To be 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 additional required signatures.)

**5. To be STACKED? YES/NO** No  If yes, Dept. NA  Course # NA

Stacked course applications are reviewed by the (Undergraduate) Curricular Review Committee and by the Graduate Academic and Advising Committee. Creating two different syllabi—undergraduate and graduate versions—will help emphasize the different qualities of what are supposed to be two different courses. The committees will determine: 1) whether the two versions are sufficiently different (i.e. is there undergraduate and graduate level content being offered); 2) are undergraduates being overtaxed?; 3) are graduate students being undertaxed? In this context, the committees are looking out for the interests of the students taking the course. Typically, if either committee has qualms, they both do. More info online - see URL at top of this page.

**6. FREQUENCY OF OFFERING:** As Demand Warrants

Fall, Spring, Summer (Every, or Even-numbered Years, or Odd-numbered Years) — or As Demand Warrants

**7. SEMESTER & YEAR OF FIRST OFFERING**
(AY2013-14 if approved by 3/1/2013; otherwise AY2014-15)

Fall 2013

**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.

| COURSE FORMAT: (check all that apply) | 1 | 2 | 3 | 4 | 5 | X 6 weeks to full semester |
|---|---|---|---|---|---|---|

| OTHER FORMAT (specify) | NA |
|---|---|
| Mode of delivery (specify lecture, field trips, labs, etc) | Lecture |

| 9. **CONTACT HOURS PER WEEK:** | 3 | LECTURE hours/weeks | 0 | LAB hours /week | 0 | PRACTICUM hours /week |
|---|---|---|---|---|---|---|

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-senate/curriculum/course-degree-procedures-/guidelines-for-computing-/ for more information on number of credits.

| OTHER HOURS (specify type) | NA |
|---|---|

10. **COMPLETE CATALOG DESCRIPTION** including dept., number, title, credits, credit distribution, cross-listings and/or stacking (50 words or less if possible):

Example of a <u>complete</u> description:

FISH F487 W, O          Fisheries Management
  3 Credits          Offered Spring
  Theory and practice of fisheries management, with an emphasis on strategies utilized for the management of freshwater and marine fisheries. Prerequisites: COMM F131X or COMM F141X; ENGL F111X; ENGL F211X or ENGL F213X; ENGL F414; FISH F425; or permission of instructor. Cross-listed with NRM F487. (3+0)

> **CITS F262      Cybersecurity Defense and Countermeasures**
> 3 Credits      Offered As Demand Warrants
> This course focuses on network and information systems security from a defensive point of view. Students will learn how to analyze internal and external security threats, develop security policies, and implement security measures to protect information within an enterprise. Topics include risk assessment, security policies and procedures, incident response, cryptographic services, network and host-based security. *Prerequisite: CITS F261 or equivalent skills.* (3+0)

11. **COURSE CLASSIFICATIONS:** Undergraduate courses only. Consult with CLA Curriculum Council to apply S or H classification appropriately; otherwise leave fields blank.

| H = Humanities | | S = Social Sciences | |
|---|---|---|---|

| Will this course be used to fulfill a requirement for the baccalaureate core? **If YES, attach form.** | **YES:** | | **NO:** | X |
|---|---|---|---|---|

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

| O = Oral Intensive, **Format 6** | | W = Writing Intensive, **Format 7** | | Natural Science, **Format 8** | |
|---|---|---|---|---|---|

11.A **Is course content related to northern, arctic or circumpolar studies? If yes, a "snowflake" symbol will be added in the printed Catalog, and flagged in Banner.**

| YES | | NO | X |
|---|---|---|---|

12. **COURSE REPEATABILITY:**

| Is this course repeatable for credit? | **YES** | | **NO** | X |
|---|---|---|---|---|

| 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 for credit, what is the maximum number of credit hours that may be earned for this course? | NA | **CREDITS** |
| If the course can be repeated with <u>variable</u> credit, what is the maximum number of credit hours that may be earned for this course? | NA | **CREDITS** |

13. **GRADING SYSTEM:** Specify only one. Note: Later changing the grading system for a course constitutes a Major Course Change.

| **LETTER:** | X | **PASS/FAIL:** | |
|---|---|---|---|

## RESTRICTIONS ON ENROLLMENT (if any)

| 14. PREREQUISITES | CITS F261 or equivalent skills |
|---|---|

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

Reference the registration implications below due to Banner coding of these terms:
Prerequisite: Course completed and grade of "C" (2.0) or higher prior to registering for the course that requires it.
Concurrent: Course may be taken simultaneously (and allows for a course to have been previously completed).
Co-requisite: Courses MUST be taken simultaneously and does NOT allow for fact that a course was previously completed!

| 15. SPECIAL RESTRICTIONS, CONDITIONS | None |
|---|---|

| 16. PROPOSED COURSE FEES | None |
|---|---|
| Has a memo been submitted through your dean to the Provost for fee approval?  **Yes/No** | NA |

## 17. PREVIOUS HISTORY

| Has the course been offered as special topics or trial course previously?  **Yes/No** | No |
|---|---|
| If yes, give semester, year, course #, etc.: | NA |

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

The IT Specialist program currently has sufficient resources (budget, facilities/space and faculty) to teach this proposed course and incorporate it into the IT Specialist program.

## 19. LIBRARY COLLECTIONS
*Have you contacted the library collection development officer (kljensen@alaska.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.*

| No | | Yes | X | | Karen Jensen, the collection development officer for the library, was contacted by email on 9/17/2012. We don't anticipate the need for any library acquisitions. |
|---|---|---|---|---|---|

## 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)

The IT Specialist program is the only program that will be affected by this proposed action.

## 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 Cybersecurity concentration of the IT Specialist A.A.S. degree program. The content of this course enables students to build on the skills and knowledge developed in CITS F261 Computer and Network Security. In CITS F261 students are introduced to fundamental concepts of computer and network security. In this course, CITS F262, students will develop the knowledge and skills necessary to implement advanced defensive security measures to protect network and information systems within an enterprise. The offering of this course will result in a workforce that is better prepared to secure the digital assets that exist within the environments in which they work.

**Negative Impacts:** No negative impacts are foreseen.

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.

Cybersecurity has been identified as one of the most serious economic and national security challenges we face as a nation. The National Initiative for Cybersecurity Education (NICE) was established to help face this challenge head on with a strategy to build a cyber savvy nation through training, awareness, K through post-graduate educational programs, and professional development for federal security professionals. (http://www.nist.gov/itl/csd/nice.cfm. Retrieved September 14, 2012.)

NICE's Strategic Plan, which is currently in a draft format, states within the Executive Summary that: "Our nation is at risk. The cybersecurity vulnerabilities in our government and critical infrastructure are a risk to national security, public safety, and economic prosperity. Now is the time to begin a coordinated national initiative focused on cybersecurity awareness, education, training, and professional development. The United States must encourage cybersecurity competence across the nation and build an agile, highly skilled workforce capable of responding to a dynamic and rapidly developing array of threats."
(http://csrc.nist.gov/nice/documents/nicestratplan/Draft_NICE-Strategic-Plan_Aug2011.pdf. Retrieved September 14, 2012).

The addition of this course to the IT Specialist program curriculum is an effort to begin addressing the need identified by NICE to increase the skills and knowledge within the cybersecurity workforce. Also, as mentioned above under item 21, this course will serve as a required course for the Network and Cybersecurity concentration of the IT Specialist A.A.S. degree program and the topics delivered through this course will serve as an essential for the cybersecurity courses used within this concentration. Without this course, graduates from this concentration area will not possess the in-depth knowledge of how to implement the defensive measures used to secure network and information systems within an enterprise. The addition of this course will enable the IT Specialist degree program to better prepare students to meet employer expectations of today's IT worker.

CITS 262

**APPROVALS:** Add additional signature lines as needed.

| *Keith Swarner* | Date | 09/27/2012 |
|---|---|---|
| Signature, Chair, Program/Department of: | Computer and Information Technology Systems | |

| *[signature]* | Date | 10/4 12 |
|---|---|---|
| Signature, Chair, College/School Curriculum Council for: | College of Rural and Community Development | |

| *Peter Pinney* | Date | 10/5/12 |
|---|---|---|
| Signature, Dean, College/School of: | College of Rural and Community Development | |

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

| | Date | |
|---|---|---|
| Signature of Provost (if above level of approved programs) | | |

**ALL SIGNATURES MUST BE OBTAINED PRIOR TO SUBMISSION TO THE GOVERNANCE OFFICE**

| | Date | |
|---|---|---|
| Signature, Chair Faculty Senate Review Committee: | ___Curriculum Review | ___GAAC |
| | ___Core Review | ___SADAC |

**ADDITIONAL SIGNATURES:** (As needed for cross-listing and/or stacking)

| | Date | |
|---|---|---|
| Signature, Chair, Program/Department of: | | |

| | Date | |
|---|---|---|
| Signature, Chair, College/School Curriculum Council for: | | |

| | Date | |
|---|---|---|
| Signature, Dean, College/School of: | | |

**ATTACH COMPLETE SYLLABUS (as part of this application).** The guidelines are online:
http://www.uaf.edu/uafgov/faculty-senate/curriculum/course-degree-procedures-/uaf-syllabus-requirements/
The Faculty Senate 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 (or changes to it) may 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, ❑prerequisites, ❑ 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 (see #6)**

6. ❑ **Student Learning Outcomes (more specific)**

7. **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.).

8. **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.

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

10. **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.) ❑ Publicize UAF regulations with regard to the grades of "C" and below as applicable to this course. (Not required in the syllabus, but may be a convenient way to publicize this.) Faculty Senate Meeting #171:
    http://www.uaf.edu/uafgov/faculty-senate/meetings/2010-2011-meetings/#171

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

12. **Disabilities Services:** Note that the phone# and location have been **updated.**
    The Office of Disability Services implements the Americans with Disabilities Act (ADA), and ensures that UAF students have equal access to the campus and course materials.
    ❑ State that you will work with the Office of Disabilities Services (208 WHITAKER BLDG, 474-5655)to provide reasonable accommodation to students with disabilities.

CITS F262 Cybersecurity Defense and Countermeasures
University of Alaska Fairbanks

## Course Information
*Course Number-Section, Title:* CITS F262 Cybersecurity Defense and Countermeasures

*Number of Credits:* 3.0

*Prerequisite:* CITS 261 or permission of the instructor.

*Class Location:* CTC 604B, Room 316 (604 Barnette Street, Fairbanks AK)

*Meeting Days & Time:* Tuesday and Thursday, 3:40-5:10 PM, 8/30 – 12/14.

This course will consist of two 90 minute class lectures delivered to students twice a week for 14 weeks. Students can expected to spend an additional six to nine hours per week, outside of scheduled classroom lecture, studying lecture materials and completing reading assignments and homework. A final exam will be given during the 15th week.

## Instructor Information
*Name:* Keith Swarner

*Office Location:* CTC 604B, Room 326 (604 Barnette Street, Fairbanks AK)

*Student Office Hours:* 2:00 pm – 4:30 pm Monday, Tuesday and Thursday or by appointment

*Telephone:* 455-2820

*Email:* keith.swarner@alaska.edu

## Course Readings/Materials
Required textbook/materials:
    *Title:*     CASP: CompTIA Advanced Security Practitioner Study Guide
    *Author(s):* Michael and Billy Haines
    *Publisher:* John Wiley & Sons, Inc.
    *ISBN13:*    978-1-118-08319-2

Recommended textbook/materials: None

## Course Description
This course focuses on network and information systems security from a defensive point of view. Students will learn how to analyze internal and external security threats, develop security policies, and implement security measures to protect information within an enterprise. Topics include risk assessment, security policies and procedures, incident response, cryptographic services, network and host-based security.

## Course Goals
Upon successful completion of this course, the student will be able to define, explain, or perform tasks related to the following:

1.0   Cryptographic Tools and Techniques
2.0   Implementing and Integrating Security Solutions throughout an Enterprise
3.0   Securing Virtualized, Distributed, and Shared Computing
4.0   Host Security
5.0   Application Security
6.0   Risk Management
7.0   Policies, Procedures and Incident Response
8.0   Security Research and Analysis
9.0   Security Controls for Communication and Collaboration

**Student Learning Outcomes**
Upon successful completion of this course, the student will be able to:

1.1 Distinguish which cryptographic tools and techniques are appropriate for a given situation.
1.2 Describe the basic operation of PKI and advanced PKI concepts.
1.3 Explain terms such as wildcard when applied to PKI.
1.4 Describe transport encryption.
1.5 Describe a digital signature.
1.6 Describe code signing.
1.7 Explain how non-repudiation works.
1.8 Define and explain the concept of psudorandom number generation.
1.9 Explain how perfect forward secret relates to the compromise of a single key.
1.10 Define the terms confusion and diffusion as it relates to plaintext and ciphertext.
2.1 Describe advanced network design concepts.
2.2 Describe the process of remote access as it relates to controlling access to network systems.
2.3 Describe SCADA systems and why security considerations for these systems are so important.
2.4 Explain the importance of securing DNS zone transfers and methods to secure these transfers.
2.5 Explain how DNSSEC works.
2.6 Explain the characteristics of Transaction Signature (TSIG).
2.7 Explain how Lightweight Directory Application Protocol (LDAP) works.
2.8 Describe the importance of transport security.
2.9 Describe the security concerns of interconnecting multiple industries.
2.10 Explain how the integration of products and services can be implemented securely.
3.1 Describe the advantages and disadvantages of virtualizing servers.
3.2 Describe VM escape and the problems associated with it.
3.3 Describe virtual desktop infrastructure (VDI).
3.4 Describe the purpose and benefits of VLANs.
3.5 Explain the characteristics of cloud computing.
3.6 Explain how to secure enterprise storage.
4.1 Describe and implement host-based firewalls.
4.2 Describe what is meant by a "trusted OS".
4.3 Explain the importance of endpoint security.
4.4 Describe multiple approaches that can be used to implement anti-virus, anti-spyware and spam filtering within an enterprise.
4.5 Describe steps and process that should be taken to harden host operating systems.
4.6 Describe what is meant by a standard operating environment.
4.7 Recognize the characteristics of command shell restrictions.
4.8 Describe the purpose of warning banners and how to they are implemented.
4.9 Describe what a restricted interface is and how they are implemented.
4.10 Describe data exfiltration and methods that can be implemented to defend against it.
4.11 Describe intrusion detection systems (IDS) and intrusion prevention systems (IPS) and how these systems are implemented.
5.1 Describe how software exploitation occurs.
5.2 Describe common application issues; such as, XSS, CSRF, clickjacking, SQL injection, and poor input validation.
5.3 Describe approaches to secure development.
5.4 Explain the difference between vulnerability scanning and penetration testing.
5.5 Describe the processes and methods used to crack passwords.
5.6 Describe when code review or black box testing should be used.
5.7 Describe why social engineering attacks are hard to prevent.

6.1 Describe various business models, including: partnerships, outsourcing, and mergers and acquisitions.

6.2 Describe the internal and external factors that influence a business.

6.3 Explain how the changing of network boundaries (i.e. cloud computing) is affecting businesses.

6.4 Describe the risks associated with allowing personally manageable devices to connect to the corporate environment.

6.5 Classify information based on an aggregate score of confidentiality, integrity, and availability (CIA).

6.7 Describe and compare the two basic techniques (qualitative and quantitative) that can be used to perform risk analysis.

6.8 Explain how to perform risk determination analysis.

6.9 Explain how and when security controls should be applied.

6.10 Describe and compare the various approaches that can be used to address risk (accept, avoid, mitigate, or transfer).

7.1 Use common business documents (policies, procedures, guidelines, and baselines) to support security.

7.2 Explain the importance of privacy principles used to protect sensitive information.

7.3 Explain how basic controls, such as separation of duties, job rotation, least privilege, and mandatory vacation, are used to govern employees.

7.4 Describe the components of an incident response plan.

7.5 Describe how to perform basic forensic tasks; such as, identification, preservation, collection, examination, analysis, and presentation of findings.

7.6 Describe policy development in light of new business, technology, and environmental changes.

7.7 Explain the importance of ongoing security training and awareness programs.

8.1 Describe the process of performing ongoing research as it relates to securing information systems within enterprise.

8.2 Describe situation awareness as it relates to securing information systems within an enterprise.

8.3 Explain how to research the security implications of new business tools.

8.4 Describe the global information assurance (IA) industry and community.

8.5 Research security requirements for contracts such as, request for proposals (RFP), request for quotes (RFQ), request for information (RFI), and agreements.

8.6 Carry out relevant analysis for the purpose of securing an enterprise.

8.7 Analyze security solutions to ensure they meet business needs.

8.8 Conduct network traffic analysis.

9.1 Describe unified communication security.

9.2 Describe the importance of VoIP security.

9.3 Explain the concerns and best practices related to remote access.

9.4 Describe the best practices in securing mobile devices.

9.5 Describe prioritization and QoS.

9.6 Explain advanced authentication tools, techniques, and concepts; such as, federated identity management, XACML, and SOAP.

9.7 Describe advantages, disadvantages and methods related to single sign-on (SSO).

9.8 Describe how to carry out security activities across the technology life cycle.

9.9 Explain how system designs are validated using standards such as common criteria (CC).

**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.

*Assignment Due Dates:* Check the Course Schedule at the end of the class syllabus for assignment due dates. Assignments are due at 3:30 PM on the due date specified for the assignment.

*Late Assignments:* Assignments submitted after 3:30 PM on the assignment due date will be considered late. Late assignments will receive a 10% deduction for every day (24-hour period) past the assignment due date. Students must also notify the course instructor through email that the late assignment has been submitted or it will not be graded.

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

*Other Important Dates:* Check the UAF Academic Calendar for important dates related to fee payment and the last day to drop or withdraw from 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 courses. The standards in this class will follow the *Student Code of Conduct* policy stated in the current UAF Catalog.

*Email:* Students are expected to be able to receive email sent to their UAF email address and are expected to check email sent to this email address regularly. This expectation can be met by students either regularly checking their UAF email account or by forwarding their UAF email to an email address that they do regularly check. Information about email and email forwarding can be found online at www.uaf.edu/google/faqs/general/#mail. Further assistance can be obtained by contacting the Help Desk at 450-8300.

## Support Services

The UAF Community and Technical College Student Assistance and Advising Center provides registration, placement assessments and financial aid services. Services are available on a walk-in basis at the, 604 Barnette Street, room 110. Appointments can be scheduled by calling 455-2800.

## 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 documented through the UAF Office of Disability Services. Information is available online at www.uaf.edu/disability/. Their office can be reached by phone at 474-5655.

**Evaluation:**

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

**Assignments** ...................................................................................................225 pts

Assignments are intended to provide an opportunity to complete and receive instructor feedback on tasks and questions that will be tested on the mid-term and final exams.

**Quizzes** ..........................................................................................................225 pts

Quizzes will be available on the class Blackboard site and will be completed outside of class. See the class schedule for quiz due dates.

**Midterm Exam** ...............................................................................................200 pts

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

**Final Exam**.....................................................................................................350 pts

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.

| | | |
|---|---|---|
| A+ .............. 1000–970 pts | A .................. 969–930 pts | A- .................. 929–900 pts |
| B+ ................ 899–870 pts | B................... 869–830 pts | B- ................ 829–800 pts |
| C+ ................ 799–770 pts | C................... 769–730 pts | C- ................ 729–700 pts |
| D+ ................ 699–670 pts | D .................. 669–630 pts | D- ................ 629–600 pts |
| | F ............ less than 600 pts | |

**Grade Required to Satisfy Degree Requirements** – To use this course to satisfy requirements in the IT Specialist certificate or associate degree program, students must earn a course grade of C or better. A grade of "C-" is not sufficient to meet degree requirements.

**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.

The deadline for student- or faculty-initiated withdrawals is Friday, October 26th.

**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 a grade of incomplete is assigned, it must be made up within one year or it will automatically be changed to a grade of "F".

**Course Calendar:**

The following course calendar provides a schedule of major course topics, reading assignments, homework assignments, and quizzes and exams.

| Wk No. | Class No. | Topic | Textbook Chapters | Assignment and Quiz Due Dates |
|---|---|---|---|---|
| 1 | 1 | • Cryptographic Services<br>• Symmetric, Asymmetric, and Hybrid Encryption<br>• Hashing and Digital Signatures | Chapter 1 | |
| 2 | 2 | • Public Key Infrastructure<br>• Cryptographic Solutions and Attack | | |
| | 3 | • Advanced Network Design<br>• TCP/IP | Chapter 2 | |
| 3 | 4 | • Secure Communication Solutions | Chapter 2 | • Quiz 1 due<br>• Assignment 1 due |
| | 5 | • Secure Facilities Solutions<br>• Secure Network Infrastructure Design | Chapter 2 | |
| 4 | 6 | • Cloud Computing Security<br>• Virtualization Security | Chapter 3 | |
| | 7 | • Virtual LANs (VLANs)<br>• Enterprise Storage | Chapter 3 | • Quiz 2 due<br>• Assignment 2 due |
| 5 | 8 | • Firewalls and Access Control Lists<br>• Host-Based Firewalls | Chapter 4 | |
| | 9 | • Endpoint Security Software<br>• Anti-malware | Chapter 4 | • Quiz 3 due<br>• Assignment 3 due |
| 6 | 10 | • Host Hardening | Chapter 4 | |
| | 11 | • Asset Management<br>• Data Exfiltration | Chapter 4 | |
| 7 | 12 | • Intrusion Detection and Prevention | Chapter 4 | |
| | 13 | • Midterm Exam | | • Quiz 4 due<br>• Assignment 4 due |
| 8 | 14 | • Application Security | Chapter 5 | |
| | 15 | • Privilege Escalation, Improper Storage, Cookies, and Process Handling Issues | Chapter 5 | |
| 9 | 16 | • Security Assessment and Penetration Testing | Chapter 5 | |
| | 17 | • Identifying Vulnerabilities<br>• Operational Risks | Chapter 6 | • Quiz 5 due<br>• Assignment 5 due |
| 10 | 18 | • Risk Assessment Process<br>• Risk Assessment Best Practices | Chapter 6 | |
| | 19 | • Business Documents Used to Support Security<br>• Documents and Controls for Sensitive Information | Chapter 7 | |

| Wk No. | Class No. | Topic | Textbook Chapters | Assignment and Quiz Due Dates |
|---|---|---|---|---|
| 11 | 20 | • Auditing Requirements and Frequency<br>• Incident Response Framework | Chapter 7 | • Quiz 6 due<br>• Assignment 6 due |
| | 21 | • Digital Forensics<br>• Training and Employee Awareness | Chapter 7 | |
| 12 | 22 | • Industry Trends and Potential Impact | Chapter 8 | |
| | 23 | • Relevant Analysis to Secure an Enterprise | Chapter 8 | • Quiz 7 due<br>• Assignment 7 due |
| 13 | 24 | • Integrating Business Disciplines to Achieve Secure Solutions | Chapter 9 | |
| | 25 | • Security Impact of Interorganizational Change | Chapter 9 | • Quiz 8 due<br>• Assignment 8 due |
| 14 | 26 | • Selecting and Distinguishing Appropriate Security Controls<br>• Advanced Authentication Tools, Techniques, and Concepts | Chapter 10 | |
| | 27 | • Carrying Out Security Activities across the Technology Life Cycle | Chapter 10 | • Quiz 9 due<br>• Assignment 9 due |
| 15 | 28 | • Final Exam | | |