ITT Technical Institute

CJ2670

Computer Forensics

Onsite Course

SYLLABUS

Credit hours: 4.5

Contact/Instructional hours: 56 (34 Theory Hours, 22 Lab Hours)

Prerequisite(s) and/or Corequisite(s):

Prerequisites: CJ1110 Introduction to Criminal Justice or equivalent

Course Description:

This course introduces fundamentals of securing a crime scene and gathering evidence from computers used in a crime.

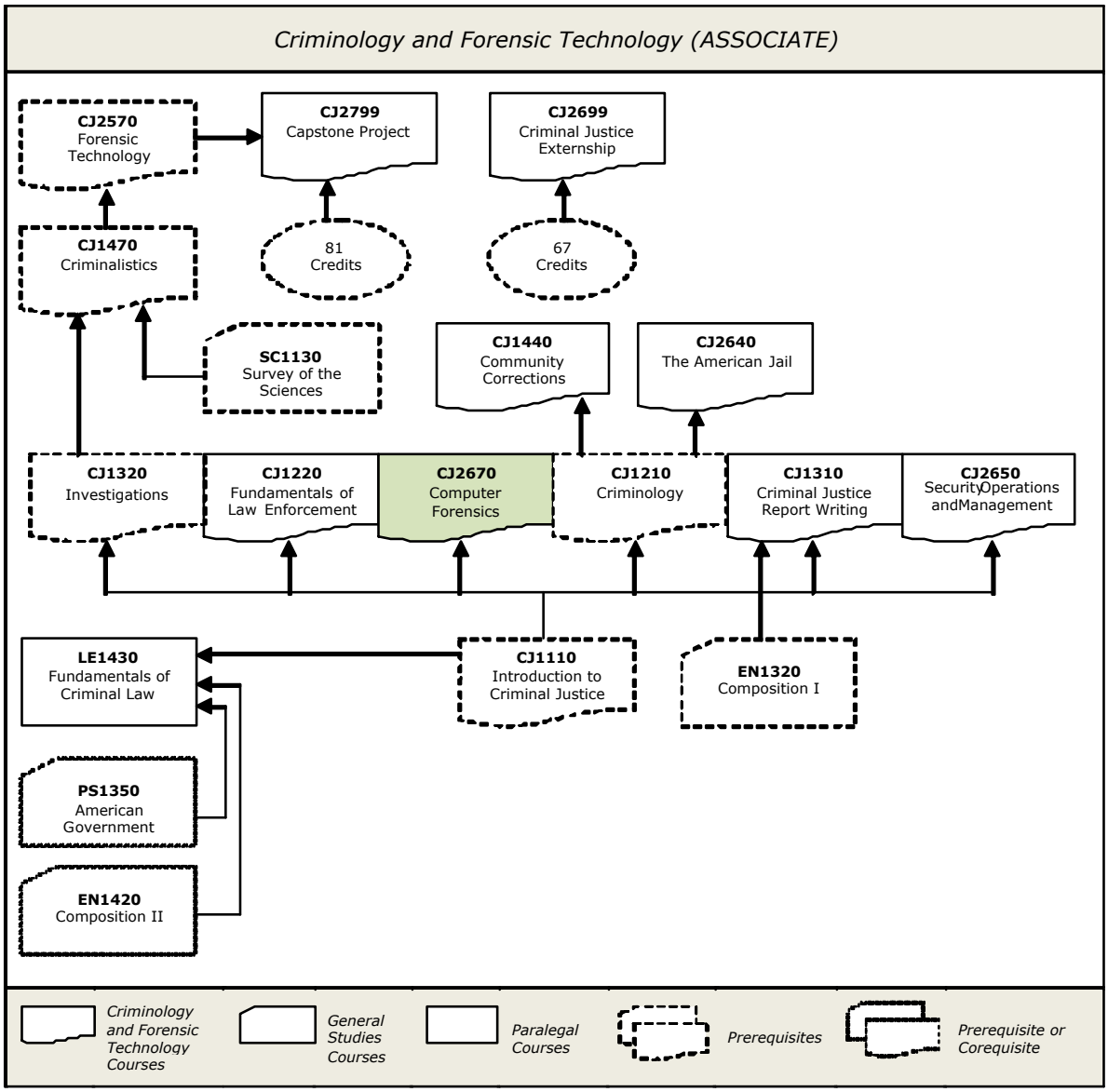
Where Does This Course Belong?

This course is offered in the Criminology and Forensic Technology associate's degree program in the School of Criminal Justice. The Criminology Forensic Technology degree from ITT Technical Institute helps to prepare students for meaningful careers as a private investigator, detention officer, corrections officer, crime scene technician, crime scene investigator, loss prevention specialist, and other areas of the criminal justice system primarily in five main areas: (1) law enforcement, (2) adjudication, (3) corrections, (4) forensics, and (5) security. Depending on each agency and organization's special requirements and selection process, careers in criminal justice may be pursued at four levels: local, state, federal, and private.

The Criminology and Forensic Technology program exposes students to the knowledge and skills used in a variety of entry-level criminal justice positions, including but not necessarily limited to private investigator, detention officer, corrections officer, loss prevention specialist, crime scene investigator, and crime scene technician. The program introduces the fundamentals of criminal law and law enforcement, community corrections, criminal justice report writing, criminalistics, forensic technology, investigations, and many other key components of the criminal justice system. Students are exposed to teamwork concepts, technology, and multiple approaches to problem solving.
This course is required for the Criminology and Forensic Technology program. This program covers the following core areas:

- Law enforcement
- Adjudication
- Corrections
- Forensics
- Security

The following diagram demonstrates how this course fits in the program:



Course Summary

Course Description

This course introduces fundamentals of securing a crime scene and gathering evidence from computers used in a crime.

Major Instructional Areas

1. Maximizing effective evidence collection using computer and forensic tools
2. Maintaining evidence in its purest form to ensure it will be admissible in legal action
3. Investigating cybercrime attacks such as identity theft, fraud, phishing, extortion, and malware infections
4. Maintaining the rule of law in adhering to the U.S. Constitution and related state and federal policies and procedural standards

Course Objectives

1. Define computer crime.
2. Examine the categories of computer crimes.
3. Identify the basic components of a computer system in relationship to the computer forensic tools that interact with those components.
4. Summarize the criminology of computer crime using the five theories that explain computer crime.
5. Describe the evolution of computer crime by examining the category Computers as Means.
6. Examine the types of crimes associated with the category of Computers as Targets.
7. Examine the crime of identity theft focusing on investigation, prosecution, and preventative issues.
8. Summarize the various social engineering techniques employed by criminals.
9. Describe the statutory issues related to cybercrime investigations.
10. Describe the relationship between the 1st Amendment and computer crime by examining the issues of decency, child pornography, and associated case law.
11. Explain the relationship between the 4th Amendment and computer crime by examining important case law and the unique search and seizure issues related to technology.
12. Discuss the emerging issues of computer crime and the relevant investigative issues.
13. Utilize the resources, tools, and knowledge of the course to conduct an electronic crime scene investigation.

14. Describe the technological trends that investigators must be aware of when conducting an investigation.
15. Research topics related to computer forensics using the ITT Tech Virtual Library.

Learning Materials and References

Required Resources

Textbook Package	New to this Course	Carried over from Previous Course(s)	Required for Subsequent Course(s)
Volonino, L., Anzaldua, R., & Godwin, J. (2007). *Computer forensics: Principles and practices (1st ed)*. Upper Saddle River, NJ: Prentice Hall.	■		■
Forensic XP Virtual Machine Student DVDs. (2012)	■		
Other Items	**New to this Course**	**Carried over from Previous Course(s)**	**Required for Subsequent Course(s)**
Fighting Back against Identity Theft (Federal Trade Commission) http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (accessed 2/20/2012)	■		

Recommended Resources

ITT Tech Virtual Library (http://library.itt-tech.edu)

Log on to the ITT Tech Virtual Library to access online books, journals, and other reference resources selected to support ITT Tech curricula.

Books

You may click “Books” or use the “Search” function on the home page to find the following books:

Books> Ebrary:

- Greenfield, R. S., & Marcella, A. J. (2002). (Ed.). *Cyber forensics: A field manual for collecting, examining and preserving evidence of computer crimes*. Philadelphia, PA: Auerbach Publishers, Incorporated.
- Computer Forensics Jump Start
- Privacy Protection and Computer Forensics, 2nd Ed
- The Copyright Book: A Practical Guide

Periodicals

You may click "Periodicals" or use the "Search" function on the home page to find the following periodicals.

Periodicals> ProQuest Criminal Justice Periodicals:

- Slade, R. M. (2005, Winter). Introduction to software forensics. *Computer Security Journal*, 21(1), 21.
- Blackwell, G. (2005, July). Computer forensics: the new, must-have skill. *Canadian Lawyer*, 29(7), 10.
- Bell, C. (2004, July). Cross-examining the computer forensics expert. *Trial*, 40(7), 78.
- Dees, T. (2004, June). New computer forensics tools. *Law & Order*, 52(6), 24-26.
- Mercer, L.D. (2004, March). Computer forensics: Characteristics and preservation of digital evidence. *FBI Law Enforcement Bulletin*, 73(3), 28-32.
- Anonymous. (2003, Sept.). Digital evidence standards. *Law & Order*, 51(9), 6.
- Piazza, P. (2003, Feb.). Digital tools from NIST. *Security Management*, 47(2) 30-31.
- Kiriakova, M. (2002, April 30). Computer forensics: Incident response essentials. *Law Enforcement News*, 28(576), S4.
- Piazza, P. (2001, Aug.). Hurdles to cyberjustice. *Security Management*, 45(8), 45-46.

Professional Associations

- American Bar Association: www.abanet.org
- The International Society of Forensic Computer Examiners (ISFCE): http://www.isfce.com/
- The International Association of Computer Investigative Specialists (IACIS): https://www.iacis.com/

Other References

The following resources can be found **outside** of the ITT Tech Virtual Library, whether online or in hard copy:

- Department of Justice: Computer Crime and Intellectual Property: http://www.cybercrime.gov/ (accessed February 20, 2012)

This web site presents insights into topics such as intellectual property, computer crimes, and electronic evidence.

- Computer Security Institute: http://www.gocsi.com/ (accessed February 20, 2012)

The Computer Security Institute (CSI) serves the needs of information security professionals through membership, educational events, security surveys and awareness tools.

- Fred Cohen & Associates: http://all.net/ (accessed February 20, 2012)

This web site provides information on the latest advancements on information protection.

- Books and Information for Private Investigators: http://crimetime.com/ (accessed February 20, 2012)

This site provides important information for private investigators.

- Computer Underground Digest: http://cu-digest.org/ (accessed February 20, 2012)

The website offers journals, newsletters, and digest of debates, news, research, and discussions of legal, social, and other issues related to computer culture.

- Search Security: http://searchsecurity.techtarget.com/ (accessed February 20, 2012)

This web site presents current issues, tips, and news on information security.

- Computer Forensics World: http://www.computerforensicsworld.com/ (accessed February 20, 2012)

This free resource for digital forensics professionals encourages information sharing and peer-to-peer assistance.

- Regional Computer Forensics Laboratory: http://www.rcfl.gov/ (accessed February 20, 2012)

This site of the Regional Computer Forensics Laboratory offers access to the premier digital forensics laboratory network in the country.

- Phrack Magazine: http://artofhacking.com/files/phrack/index.htm (accessed February 20, 2012)

An online hacker magazine that presents latest related articles

Web sites

- Center for Intellectual Property and Copyright in the Digital Environment
  http://www.umuc.edu/distance/odell/cip/cip.html (accessed February 20, 2012)
  Provides resources and workshops for the higher education community on IP and copyright in the digital environment, with an emphasis on law and policy relating to distance education.
- Learning Cyber Law in Cyberspace

http://www.cyberspacelaw.org/dogan/ (accessed February 20, 2012)

An introduction to copyright in cyberspace

- Crash Course in Copyright

http://www.lib.utsystem.edu/copyright/ (accessed February 20, 2012)

The basics of copyright law

- InfoWebLinks: Ethics in Computing: http://www.infoweblinks.com/content/ethicsincomputing.htm (accessed February 20, 2012)

An online reference to ethical guidelines for information technology.

- Ethics in Computing PowerPoint presentation: www.cs.fredonia.edu/~zubairi/s2k6/csit120/**ethics**1.ppt

A presentation on ethics from SUNY Fredonia

- The Ten Commandments of Computer Ethics: http://computerethicsinstitute.org/ (accessed February 20, 2012)

Guidelines for computer ethics from the Computer Ethics Institute

- Patent and Trademark Resources: http://www.uspto.gov/ (accessed February 20, 2012)

The website for the United States patent and trademark office

- Computer Forensics from US-CERT: http://www.us-cert.gov/reading_room/forensics.pdf (accessed February 20, 2012)

A discussion paper on the need for computer forensics to be practiced in an effective and legal way; outlines basic technical issues and points to references for further reading

NOTE: All links to Web references are subject to change without prior notice.

Information Search

Use the following keywords to search for additional online resources that may be used for supporting your work on the course assignments:

- Computer forensics
- Computer forensic tools
- Slack space
- Data carving
- Forensic image
- Hashing
- Cyber law

Course Plan

Suggested Learning Approach

In this course, you will be studying individually and within a group of your peers. As you work on the course deliverables, you are encouraged to share ideas with your peers and instructor, work collaboratively on projects and team assignments, raise critical questions, and provide constructive feedback.

Use the following advice to receive maximum learning benefits from your participation in this course:

DO	DON'T
▪ Do take a proactive learning approach. ▪ Do share your thoughts on critical issues and potential problem solutions. ▪ Do plan your course work in advance. ▪ Do explore a variety of learning resources in addition to the textbook. ▪ Do offer relevant examples from your experience. ▪ Do make an effort to understand different points of view. ▪ Do connect concepts explored in this course to real-life professional situations and your own experiences.	▪ Don't assume there is only one correct answer to a question. ▪ Don't be afraid to share your perspective on the issues analyzed in the course. ▪ Don't be negative about the points of view that are different from yours. ▪ Don't underestimate the impact of collaboration on your learning. ▪ Don't limit your course experience to reading the textbook. ▪ Don't postpone your work on the course deliverables – work on small assignment components every day.

Course Outline

Unit 1: ADMISSIBILITY OF ELECTRONIC EVIDENCE

Out-of-class work: *11 Hours*

Upon completion of this unit, students are expected to:

- Identify different types of evidence.
- Explain how electronic evidence differs from physical evidence.
- Explain the process of discovery and electronic discovery.
- Describe the basic steps in a computer forensics investigation.

READING ASSIGNMENT	GRADED ACTIVITIES / DELIVERABLES		
	Grading Category	**Activity/Deliverable Title**	**Grade Allocation** (% of all graded work)
• Volonino, Anzaldua, & Godwin, Chapters 1 & 2	Assignment	Unit 1 Assignment 1: Test Your Skills	1.0%
		Unit 1 Assignment 2: Storage Devices	1.0%
	Lab	Unit 1 Lab 1: Structure of the Microsoft Windows Operating System	3.25%

Unit 2: PREPARING FOR E-EVIDENCE COLLECTION AND PRESERVATION

Out-of-class work: *11 Hours*

Upon completion of this unit, students are expected to:

- Explain the management of e-evidence throughout the life-cycle of a case.
- Identify requirements for acquiring and authenticating evidence.
- Recognize the various certification programs available for a computer forensics investigator.
- Explain the reasons for policies and procedures.
- Formulate policies and procedures.
- Identify the steps in a forensic examination.
- Conduct an investigation yielding a written report.
- Examine file compression.

READING ASSIGNMENT	GRADED ACTIVITIES / DELIVERABLES		
	Grading Category	**Activity/Deliverable Title**	**Grade Allocation** (% of all graded work)
• Volonino, Anzaldua, & Godwin, Chapters 3 & 4 • Fighting Back against Identity Theft (Federal Trade Commission) http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (accessed 2/20/2012)	Assignment	Unit 2 Assignment 1: Test your Skills	1.0%
		Unit 2 Assignment 2: Fighting Back Against Identity Theft	1.0%
	Lab	Unit 2 Lab 1: Identity on the	3.25%

		Internet	

Unit 3: FORENSIC EXAMINATION OF COMPUTERS AND DIGITAL MEDIA

Out-of-class work: *11 Hours*

Upon completion of this unit, students are expected to:

- Identify types of drives and media storage devices.
- Explain techniques for acquiring and analyzing various hard drives.
- Describe PDA and cellular phone technology.
- List the various tools used to analyze PDA's and cell phone data.
- Define and recognize an operating system.
- Identify the different types of operating system interfaces and file systems.
- Understand the basic data transmission on networks.
- Describe legal methods for obtaining electronically stored evidence.

READING ASSIGNMENT	GRADED ACTIVITIES / DELIVERABLES		
	Grading Category	**Activity/Deliverable Title**	**Grade Allocation** (% of all graded work)
• Volonino, Anzaldua, & Godwin, Chapters 5 & 6	Assignment	Unit 3 Assignment 1: Test Your Skills	1.0%
		Unit 3 Assignment 2: Persistent and Volatile Memory	1.0%
	Lab	Unit 3 Lab 1: Installing a Virtual Machine	3.25%
	Quiz	Unit 3 Quiz 1: Chapters 1-4	3.75%

Unit 4: INVESTIGATING WINDOWS, LINUX, AND GRAPHICS FILES

Out-of-class work: *11 Hours*

Upon completion of this unit, students are expected to:

- Conduct an effective investigation of the windows system and find user data files and profiles in Windows folders.
- Identify proper computer forensic graphic tools and what they can reveal and recover.
- Examine the contents of Linux folders.

READING ASSIGNMENT	GRADED ACTIVITIES / DELIVERABLES		
	Grading Category	**Activity/Deliverable Title**	**Grade Allocation** (% of all graded work)
• Volonino, Anzaldua, & Godwin, Chapter 7	Assignment	Unit 4 Assignment 1; Test Your Skills	1.0%
		Unit 4 Assignment 2: Live and Alternate Data Streams	1.0%
	Lab	Unit 4 Lab 1: Examining an Image for Hidden Information	3.25%

Unit 5: E-MAIL AND WEBMAIL FORENSICS

Out-of-class work: *11 Hours*

Upon completion of this unit, students are expected to:

- Describe how email flows across a network.
- Distinguish resident e-mail client programs and webmail-based programs.
- Compare desktop data storage and server data storage.

• Examine how instant messaging works and moves across the network.			
READING ASSIGNMENT	**GRADED ACTIVITIES / DELIVERABLES**		
	Grading Category	**Activity/Deliverable Title**	**Grade Allocation** (% of all graded work)
• Volonino, Anzaldua, & Godwin, Chapter 8	Assignment	Unit 5 Assignment 1; Test Your Skills	1.0%
		Unit 5 Assignment 2: E-mail Headers and IP Address	1.0%
	Lab	Unit 5 Lab 1: Examining E-mail for Evidence	3.25%
	Quiz	Unit 5 Quiz 2: Chapters 5-7	3.75%

Unit 6: INTERNET AND NETWORK FORENSICS – INTRUSION DETECTION

Out-of-class work: *11 Hours*

Upon completion of this unit, students are expected to:

- Describe the operations of intrusion detection systems (IDS).
- Understand the use of network forensic analysis toolkits (NFAT).
- List the different areas where data can be extracted.
- Identify the most common NFAT systems.

READING ASSIGNMENT	GRADED ACTIVITIES / DELIVERABLES		
	Grading Category	**Activity/Deliverable Title**	**Grade Allocation** (% of all graded work)
• Volonino, Anzaldua, & Godwin, Chapter 9	Assignment	Unit 6 Assignment 1: Test Your Skills	1.0%
		Unit 6 Assignment 2: Online Crimes Against Children	1.0%
	Lab	Unit 6 Lab 1: Using the FTK Imaging Software and Using FTK to Recover Deleted Files	3.25%

Unit 7: TRACKING THE "BAD GUYS"

Out-of-class work: *11 Hours*

Upon completion of this unit, students are expected to:

- Identify tactics used in large-scale attacks and their "cybertrails."
- Understand the use of the Internet in terrorism and virtual warfare.
- Understand hacker objectives and the economy of cybercriminals.
- Explain the process of collecting e-evidence in criminal cases.

READING ASSIGNMENT	GRADED ACTIVITIES / DELIVERABLES		
	Grading Category	**Activity/Deliverable Title**	**Grade Allocation** (% of all graded work)
• Volonino, Anzaldua, & Godwin, Chapter 10	Assignment	Unit 7 Assignment 1: Test Your Skills	1.0%
		Unit 7 Assignment 2: Search Warrant Exceptions	1.0%
	Lab	Unit 7 Lab 1: Creating Additional Storage on a Virtual Forensic Machine	3.25%
	Quiz	Unit 7 Quiz 3: Chapters 8-9	3.75%

Unit 8: FRAUD AND FORENSIC ACCOUNTING INVESTIGATION

Out-of-class work: *11 Hours*

Upon completion of this unit, students are expected to:

- Understand the challenges of fraud investigations.
- Describe the characteristics and symptoms of the more common types of computer fraud.
- Identify the role of computer forensics in fraud detection, investigation, and deterrence.

READING ASSIGNMENT	GRADED ACTIVITIES / DELIVERABLES

	Grading Category	Activity/Deliverable Title	Grade Allocation (% of all graded work)
• Volonino, Anzaldua, & Godwin, Chapter 11	Assignment	Unit 8 Assignment 1: Test Your Skills	1.0%
		Unit 8 Assignment 2: Affidavit in Support of a Search Warrant	1.0%
	Lab	Unit 8 Lab 1: Computer Forensic Analysis of a Given Image	3.25%

Unit 9: FEDERAL RULES AND CRIMINAL CODES

Out-of-class work: *11 Hours*

Upon completion of this unit, students are expected to:

- Identify federal rules of evidence and other principles of the due process.
- Explain the legal foundations and reasons for pretrial motions on evidence.
- Identify a "reasonable expectation of privacy" and its limitations.
- Discuss the major anticrime laws and amendments impacting e-discovery and the use of e-evidence.

READING ASSIGNMENT	GRADED ACTIVITIES / DELIVERABLES		
	Grading Category	Activity/Deliverable Title	Grade Allocation (% of all graded work)
• Volonino, Anzaldua, & Godwin, Chapter 12	Assignment	Unit 9 Assignment 1: Test Your Skills	1.0%
		Unit 9 Assignment 2: Limitation of Constitutional Rights and the Expectation of Privacy	1.0%
	Quiz	Unit 9 Quiz 4: Chapters 10-12	3.75%
	Project	Unit 9 Project Part 1: Computer Forensic Analysis of the Project Image	10%

Unit 10: PROFESSIONAL RESPONSIBILITY IN TESTIMONY

Out-of-class work: *11 Hours*

Upon completion of this unit, students are expected to:

- Understand the ethical duty of a computer forensic examiner both in and out of court.
- Identify the responsibilities of an expert witness in the legal system.
- Describe the challenges of testifying in a case involving computer forensics.

READING ASSIGNMENT	GRADED ACTIVITIES / DELIVERABLES		
	Grading Category	Activity/Deliverable Title	Grade Allocation (% of all graded work)
• Volonino, Anzaldua, & Godwin, Chapter 13	Assignment	Unit 10 Assignment 1: Test Your Skills	1.0%
	Project	Unit 10 Project Part 2: Deliver a Computer Forensic Report of the Image Analysis Findings for Testimony in Court - Porfolio	10%

Unit 11: COURSE REVIEW AND FINAL EXAMINATION

Out-of-class

• All learning objectives for course			***work:*** *4 Hours*
READING ASSIGNMENT	**GRADED ACTIVITIES / DELIVERABLES**		
	Grading Category	**Activity/Deliverable Title**	**Grade Allocation** (% of all graded work)
• None	Exam	Final Exam	20%

Note: Your instructor may add a few learning activities that will change the grade allocation for each assignment in a category. The overall category percentages will not change.

Evaluation and Grading

Evaluation Criteria

The graded assignments will be evaluated using the following weighted categories:

Category	Weight
Assignment	19%
Lab	26%
Project	20%
Quiz	15%
Exam	20%
TOTAL	**100%**

Grade Conversion

The final grades will be calculated from the percentages earned in the course, as follows:

Grade	Percentage	Credit
A	90–100%	4.0
B+	85–89%	3.5
B	80–84%	3.0
C+	75–79%	2.5
C	70–74%	2.0
D+	65–69%	1.5
D	60–64%	1.0
F	<60%	0.0

Academic Integrity

All students must comply with the policies that regulate all forms of academic dishonesty, or academic misconduct, including plagiarism, self-plagiarism, fabrication, deception, cheating, and sabotage. For

more information on the academic honesty policies, refer to the Student Handbook and the Course Catalog.

(End of Syllabus)