# Wayland Baptist University logo

Virtual Campus

School of Business

# UNIVERSITY MISSION STATEMENT

Wayland Baptist University exists to educate students in an academically challenging, learning-focused and distinctively Christian environment for professional success, and service to God and humankind.

# COURSE NUMBER & NAME:

MISM 4337-VC01, Incident Response and Forensics

# **TERM**:

Spring 2018

# **INSTRUCTOR**:

Jimmy Fikes

# **CONTACT INFORMATION**:

Cell phone: 806-831-3918

WBU Email: jimmy.fikes@wayland.wbu.edu

# **OFFICE HOURS, BUILDING & LOCATION**:

Students may request personal conferences with the instructor on any day, and at any time.

# **COURSE MEETING TIME & LOCATION**:

This class will be conducted entirely online on Blackboard.

# **CATALOG DESCRIPTION**:

Analysis of data breach incidents, affected systems, preservation of hardware, software, log files and other computer and network related information that could be needed for litigation. Attention is given both to internal organization policies and procedures that were intended to prevent an intrusion, as well as the methods that were used to circumvent these security policies.

# PREREQUISITE:

MISM 4306

# **REQUIRED TEXTBOOK AND RESOURCE MATERIAL**:

Required book: Incident Response and Computer Forensics

Author: Luttgens, J., Pepe, M., & Mandia, K.

Edition: 3rd

Year: 2014

Publisher: McGraw-Hill

ISBN: 978-0071798686

Updated: 5/26/2015

# OPTIONAL MATERIALS

Students will use a free Dropbox account for sharing documents with the instructor.

# **COURSE OUTCOMES AND COMPETENCIES**:

* Explain the types of computer security incidents that threaten information assets
* Analyze vectors of attack and compromised systems
* Explain the purpose and composition of an Incident Response Team (IRT)
* Explain the steps required to prove chain-of-custody

# ATTENDANCE REQUIREMENTS:

As stated in the Wayland Catalog, students enrolled at one of the University’s external campuses should make every effort to attend all class meetings. All absences must be explained to the instructor, who will then determine whether the omitted work may be made up. When a student reaches that number of absences considered by the instructor to be excessive, the instructor will so advise the student and file an unsatisfactory progress report with the campus executive director. Any student who misses 25 percent or more of the regularly scheduled class meetings may receive a grade of F in the course. Additional attendance policies for each course, as defined by the instructor in the course syllabus, are considered a part of the University’s attendance policy.

**Instructor’s Attendance Statement:** Students who miss more than 25% of class sessions will receive a grade of F for the term. Participation in a "class session" is defined (for this class) as failing to participate in all activities for a given week. This includes required assignments, discussion forums, and projects.

# **STATEMENT ON PLAGIARISM & ACADEMIC DISHONESTY**:

Wayland Baptist University observes a zero-tolerance policy regarding academic dishonesty. Per university policy as described in the academic catalog, all cases of academic dishonesty will be reported and second offenses will result in suspension from the university.

#  **DISABILITY STATEMENT**:

In compliance with the Americans with Disabilities Act of 1990 (ADA), it is the policy of Wayland Baptist University that no otherwise qualified person with a disability be excluded from participation in, be denied the benefits of, or be subject to discrimination under any educational program or activity in the university. The Coordinator of Counseling Services serves as the coordinator of students with a disability and should be contacted concerning accommodation requests at (806) 291-3765. Documentation of a disability must accompany any request for accommodations.

# **COURSE REQUIREMENTS and GRADING CRITERIA**:

**Weekly Quizzes**

* **For each chapter covered, students will complete a 20-question quiz (18 chapters x 20 questions – 360 questions).**
* **The average of all quiz grades will make up 30% of the total term grade.**

**Research Paper**

* **Students will select one chapter (or topic) that deals a topic that interests them in the field of Incident Response and Computer Forensics.**
* **Students will write a 10-15-page research paper (APA style) that covers this topic. This paper is due by the end of week 11.**
* **Research papers will be graded according to the grading rubric (found in the Course Info / Syllabus location in Blackboard).**
* **The grade received for the research paper will make up 30% of the total term grade.**

**Discussion Board**

* **There are two discussion forums in this class**
	+ **Peer-to-Peer Support Forum (called the Peer Forum)**
		- **Students must post at least one message per week in this forum**
		- **Students use this forum to support one another on anything related to this class (assignments, solutions, research materials, etc.)**
	+ **Case Study Forum**
		- **Students must post two messages per week in this forum**
		- **In this forum, students are specifically addressing the case studies given in the chapters of the textbook**
* **The average of all grades in the discussion forums make up 30% of the total term grade.**

**Participation**

* **This class requires that all students be working together on the same material at the same time in each week of the term.**
* **The final 10% of the total term grade will come from how timely students are in being on time with written assignments and in the discussion forums.**
1. **Grade Appeal Statement:**

“Students shall have protection through orderly procedures against prejudices or capricious academic evaluation. A student who believes that he or she has not been held to realistic academic standards, just evaluation procedures, or appropriate grading, may appeal the final grade given in the course by using the student grade appeal process described in the Academic Catalog. Appeals may not be made for advanced placement examinations or course bypass examinations. Appeals are limited to the final course grade, which may be upheld, raised, or lowered at any stage of the appeal process. Any recommendation to lower a course grade must be submitted through the Vice President of Academic Affairs/Faculty Assembly Grade Appeals Committee for review and approval. The Faculty Assembly Grade Appeals Committee may instruct that the course grade be upheld, raised, or lowered to a more proper evaluation.”

# SCHEDULE

|  |  |
| --- | --- |
| **Week** | **Chapters Covered** |
| 1 | 1. Real-World Incidents
2. IR Management Handbook
 |
| 2 | 1. Pre-Incident Preparation
2. Getting the Investigation Started on the Right Food
 |
| 3 | 1. Initial Development of Leads
2. Discovering the Scope of the Incident
 |
| 4 | 1. Live Data Collection
2. Forensic Duplication
 |
| 5 | Review |
| 6 | 1. Network Evidence
2. Enterprise Services
 |
| 7 | 1. Analysis Methodology
2. Investigating Windows Systems
 |
| 8 | 1. Investigating Mac OS X Systems
2. Investigating Applications
 |
| 9 | 1. Malware Triage
2. Report Writing
 |
| 10 | 1. Remediation Introduction
2. Remediation Case Study
 |
| 11 | Research Paper Due |