# Wayland Logo

Virtual Campus

School of Business

# 2. 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.

# 3. COURSE NUMBER & NAME:

MISM 4337-VC01, Incident Response and Forensics

# **4. TERM**:

Summer 2020

# **5. INSTRUCTOR**:

Jimmy Fikes

# **6. CONTACT INFORMATION**:

Cell phone: 806-831-3918

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

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

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

# **8. COURSE MEETING TIME & LOCATION**:

This class will be conducted entirely online on Blackboard.

# **9. 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.

# 10. PREREQUISITE:

MISM 4306

# **11. REQUIRED TEXTBOOK AND RESOURCE MATERIAL**:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **BOOK** | **AUTHOR** | **ED** | **YEAR** | **PUBLISHER** | **ISBN#** | **UPDATED** |
| Incident Repose and Computer Forensics | Pepe | 3rd | 2014 | McGraw-Hill | 9780-07179-8686 | 5/26/15 |

**IMPORTANT**: This eTextbook was included at registration. If you want to buy a hard copy that is fine, but you must OPT-OUT of the eTextbook in the classroom link prior to June 9 or be charged.

# 12. OPTIONAL MATERIALS

None

# **13. 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

# 14. 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.

# **15. 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.

# **16. 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.

# **17. COURSE REQUIREMENTS and GRADING CRITERIA**:

**Weekly Quizzes**

* **18 chapter quizzes (each chapter is quiz must be taken in the week it is assigned).**
* **The average of all chapter quiz grades will make up 33% 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 the Peer 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 two discussion forums make up 33% of the total term grade.**
* **Exams**
	+ **Two exams (in weeks 5 and 11)**
	+ **The average of the two exam scores will make up 34% of the total term grade.**

**17.1 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.”

# 18. TENTATIVE 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 | Exam 1 |
| 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 | Exam 2 |