IS-380-OME1&2 – Information Security for the Organization

**Class Schedule:** OME1: Tuesday 5:00-7:50 pm OME2: Thursday 5-7:50PM

**Class Location:** SBL 105 (Tues OME1 section) SBL102 (Thurs OME2 section)

**Class Dates:** Aug 29 – Dec 18

|  |  |
| --- | --- |
| Cary Barker  Instructor | Email: cbarker@stevenson.edu  Tel: 410-812-6368 (Cell)  Website: <http://carybarker.com>  Blackboard: <https://blackboard.stevenson.edu> |

**Instructor:**

**Course Description:**

      This course addresses the top security issues to be recognized by any business and surveys the tools to detect threats and protect valuable organization resources. Key topics including threat and risk assessment, viruses, worms, Trojan horses, port scans spyware, and denial of service attacks will be covered along with discussion of free security tools available to help uncover vulnerabilities. Students will learn to write a security policy for their organization.

**Course Materials**:

Course texts include:

Harris, Shon *All-In-One CISSP Exam Guide,* 5th Edition. McGraw-Hill Osborne Media.

2010. ISBN-10: 0071602178 ISBN-13: 978-0071602174

**Other Requirements:**

Microsoft Visio 2010

Note: Students must have a computer login and password, Blackboard login and password and be able to access their storage space on the M drive.

**Course Goals:**

* To explore the range of technology issues in managing information security.
* To become aware of the leading vendors and their information security products.
* To understand the process of creating an information security framework.
* To understand the issues in risk analysis and vulnerability assessment
* To understand the technologies in the area of cryptography
* To explore the key issues in computer security
* To offer a method for the evaluation of technology solutions.

# Learning Outcomes:

Students will be able to:

* Identify, evaluate, and select the most cost effective security solutions for a given organization
* Write effective security communications and assessments
* Complete the risk assessment process for a given problem.
* Evaluate security threats from a business perspective
* Perform research, write a technical analysis, and deliver a professional presentation detailing a site security plan.
* Apply the concept of Defense in Depth.
* Identify the tasks of operations security
* Explain Confidentiality, Integrity, and Availability
* Identify the strengths, limitations, and appropriate use of network and physical security tools
* Explain the legal and ethical issues surrounding information security

# Learning Strategies

Learning outcomes will be achieved through the following strategies:

* Guided tutorials – in and out of class
* Quizzes
* PowerPoint lectures
* Class discussion (face to face)
* Application Activities
* Simulation exercises
* Independent study

Table of Contents

[Learning Outcomes: 2](#_Toc112606446)

[Learning Strategies 2](#_Toc112606447)

[Course Grading Policy 4](#_Toc112606448)

[Course Grading Policy: 4](#_Toc112606449)

[Late work and make up exam policy: 5](#_Toc112606450)

[Attendance Policy: 5](#_Toc112606451)

[Course Assignments 9](#_Toc112606452)

[Deliverable Schedule 10](#_Toc112606453)

[Course Readings 11](#_Toc112606454)

[Quizzes 12](#_Toc112606455)

[Exams 15](#_Toc112606457)

[Blackboard WEB Access 21](#_Toc112606459)

[Stevenson College Policies 22](#_Toc112606460)

[Network Security Agreement 22](#_Toc112606461)

[Email Policy: 22](#_Toc112606462)

[Classroom PC Acceptable Use Policy 22](#_Toc112606463)

[Academic Honesty Penalty 22](#_Toc112606464)

[Writing Policy 23](#_Toc112606465)

[Students with Disabilities 23](#_Toc112606466)

**Course Grading Policy**

# 

The final course grade will be allocated according to the following formula:

|  |  |
| --- | --- |
| Component | Points (approx.) |
| Professionalism | 20 |
| Quizzes (about 8 total) | 200 |
| Article Presentation | 20 |
| Midterm exam | 150 |
| Final exam | 200 |
| Assignments | 20 |
| Final Project | 100 |
| Final Presentation | 100 |
| Total | 790 |

**Note: Improper, distracting, disrespectful or disruptive behavior in the classroom or anything less than professional and respectful email communication will result a severe grading penalty beyond the breakdown noted above at the discretion of the instructor. Any violation of the Academic Honesty Policy or the policies detailed in this syllabus may result in an ‘F’ for the assignment or an ‘F’ for the course at the discretion of the instructor. The penalty for a violation of the Academic Honesty Policy could be changed to dismissal from the college by higher authorities.**

**Grading Ranges**

|  |  |
| --- | --- |
| Grade | Numeric Standard |
| A | 93 - 100 |
| A- | 90 – 92 |
| B+ | 87 – 89 |
| B | 83 – 86 |
| B- | 80 – 82 |
| C+ | 77 – 79 |
| C | 73 – 76 |
| C- | 70 – 72 |
| D+ | 67 – 69 |
| D | 60 – 66 |
| F | 0 – 59 |

## Course Grading Policy:

In compliance with the Stevenson College grading policy, a student’s performance in a course will be measured in accordance with the following grading system:

|  |  |
| --- | --- |
| Grade | Quality Points Awarded |
| A | 4.0 |
| A- | 3.7 |
| B+ | 3.3 |
| B | 3.0 |
| B- | 2.7 |
| C+ | 2.3 |
| C | 2.0 |
| C- | 1.7 |
| D+ | 1.3 |
| D | 1.0 |
| F | 0.00 |

The grade of 'C' is the lowest acceptable grade for Information Systems courses. Required IS courses in the major must be repeated for a grade of C minus or better in order to graduate.

## Late work and make up exam policy:

**Students will not receive credit for assignments submitted late or missed exams without prior approval of the instructor**. Only in the most extreme circumstances may students petition the instructor for exemption. The instructor will consider all petitions, deny those deemed other than extreme, and grant those were evidence is clear. At the discretion of the instructor, the student may be required to petition the Division Director Information Systems for exemption. The process requires an in person interview with the Division Director Information Systems and a detailed formal letter of explanation which shall cite, among other items, the personal contact information for verification of required references. Further details of the process and the documentation required can be obtained from the instructor.

## Attendance Policy:

Students are responsible for all information covered in class and the timely delivery of out of class assignments regardless of attendance. If a class is missed for any reason it is the student’s responsibility to obtain from a classmate all information covered in class including but not limited to instructors lecture, class instructions, class notes, assignments, or any other relevant materials. All information provided in Information Systems courses is to be considered “essential content”. Failure to attend class does not exempt the student from assignment deadlines nor does it exempt the student from the responsibility of understanding testable concepts as well as concepts and skills required as a prerequisite to other courses in the curriculum.

**INFORMATION SYSTEMS DIVISION**

**STUDENT & FACULTY COMMUNICATION GUIDELINES**

Effective communication between students and faculty is essential for student success and faculty expectations. The process below is designed to help everyone feel comfortable that their message is successfully delivered and acknowledged. Students and faculty should use the steps below to close the loop in contacting each other. Note that for questions requiring a more immediate response, students should contact faculty by telephone on their office extension.

1. Student emails faculty with question or deliverable.
2. Within one business day or as soon as the faculty sees the message, the faculty sends an email message in response that acknowledges receipt and review of message from the student. (not necessarily an answer)
3. If the student does not get a response acknowledging the receipt within one business day, the student should send the message again. If no acknowledgement is received, the student should call the faculty member on their office extension or the phone number listed in the course syllabus.
4. If the student is still unable to reach the faculty member, they should then contact Ken Snyder by email on ksnyder@mail.Stevenson.edu
5. Within 96 hours or sooner if project deadlines are involved, the faculty will respond with a feedback message on questions or assignments.
6. Students will respond with an acknowledgment of the feedback message from the faculty.

**Student Responsibilities:**

Students are responsible for communication with their instructor. There should be no delay in asking questions, expressing concern about the clarity of concepts or requesting feedback on assignments.

IMPORTANT:

* In all email communications with the instructor, students must identify themselves in the subject line of the message to include: **Last Name, First Name, Course Number, and Section Number.**
* All college email communication will be exchanged **only over Stevenson email accounts**. Students are responsible for the information sent to their Stevenson email account and must monitor their Stevenson accounts each day for important college and course related information. Students are required to view their Stevenson email accounts directly or set up their Stevenson email account to forward to an account they view regularly during the day.

Students should expect to receive a great deal of information over their Stevenson email account. If you are not receiving regular information over a forwarded email address you should immediately investigate the problem before missing important instructions or announcements.**Course Schedule**

|  |  |  |  |
| --- | --- | --- | --- |
| Class | Topic | Assignments Prior to class | Class Activities |
| 1 (Aug-30) | *Class Introduction and overview of 10 Domains* |  | * Lecture and Discussion * Article presentation sign-up * Introduction to Microsoft Visio * Marshmallow challenge |
| 2 (Sept 6) | *Information Security and Risk Management* | Read Chapter 3 | Lecture and Discussion  Risk Analysis Exercise Intro. |
| 3 (Sept 13) | *Access Control* | Read Chapter 4 | Article presentations  **Quiz on Chapter 3**  Lecture and Discussion  RA continued |
| 4 (Sept 20) | *Security Architecture and Design* | Read Chapter 5  Risk Assessment due | Article presentations  **Quiz on Chapter 4**  Lecture and Discussion |
| 5 (Sept 27) | *Physical and Environmental Security* | Read Chapter 6 | Article presentations  **Quiz on Chapter 5**  Lecture and Discussion  Lab: Lockpicking  Lab: Physical security diagramming in Visio |
| 6 (Oct 4) | *Telecommunications and network security* | Read Chapter 7  Physical Security Layout in MS Visio due | Article presentations  **Quiz on Chapter 6**  Lecture and Discussion  In class assignments |
| 7 (Oct 11) | *Midterm Exam* | Study for Exam | Midterm Exam |
| 8 (Oct 18) | *Networking lab* | Complete Chapter 7 | Article presentations  Discuss final project  Lab: Network security diagramming in Visio  Lab: Network captures |
| 9 (Oct 25) | *Cryptography* | Read Chapter 8  Network Diagram in MS Visio due  Work on final project | Lab: Frequency Analysis |
| 10 (Nov 1) | *Business Continuity and Disaster Recovery* | Read Chapter 9  Work on final project  RA draft due  Phy. diagram draft due  Budget Request due  Network Diagram due | Article presentations  **Quiz on Chapter 8**  Lecture and Discussion  Lab: Business Continuity plan |
| 11 (Nov 8) | *Law, Investigation, and ethics* | Read Chapter 10  Work on final project | Article presentations  **Quiz on Chapter 9**  Lecture and Discussion |
| 12 (Nov 15) | Project Presentations | Presentations Due | Article presentations  **Quiz Chapter 10**  Project Presentations |
| 13 (Nov 29) | *Application Security* | Read Chapter 11 | Article presentations  Lecture and Discussion |
| 14 (Dec 6) | *Operations Security* | Read Chapter 12 | **Quiz on Chapter 11** |
| 15 (Dec 13) | *Final Exam* |  |  |

# Course Assignments

The following deliverables are required. The schedule for delivery and detailed requirements can be found on the pages to follow.

* Course Readings
* Professionalism
* Quizzes
* Exams
* Article Presentations
* Final Project

## Deliverable Schedule

|  |  |
| --- | --- |
| **DELIVERABLE** | **DUE** |
| Readings | Weekly |
| Quizzes | Weekly |
| Assignments | Weekly |
| Midterm Exam | Week 7 |
| Final Exam | Week 15 |
| Final Project presentations | Week 12 |
| Article Presentations | 1 per semester, scheduled individually |

**Course Readings**

*Outcomes:*

* Define information security and information assurance.
* Complete the risk assessment process given applicable data.
* Explain the process of security management.
* Implement Audits and the Auditing process.
* Explain the process of incident detection and incident response.
* Create a site security plan.
* Classify the daily tasks of a business analyst and identify the kinds of jobs that might employ this profession.

*Description/Requirements:*

It is expected that students complete readings for each prior to class. For example, readings for session 2 should be read before attending the second class session. Please see the course schedule for additional detail on the readings due before each class session.

Read the assigned text sections identified in the reading assignment topic before the class indicated, take notes on class discussions, and ask for clarification on those points that are unclear. Attempt to answer the questions and perform the exercises in the text sections. These questions may very well be a source for exam questions. Begin work on the tutorial assignments earlier than the night before the assignment is due! Plan ahead and pay attention to details—it may make the difference between an A and a B for your final grade. The schedule on the following page indicates the assignments and other work due on particular dates.

*Grading/Points Possible:*

This assignment will not be assessed formally. However content from readings will be assessed indirectly through all course assignments.**Professionalism**

*Outcomes:*

* Write effective security communications and assessments
* Evaluate security threats from a business perspective
* Identify the tasks of operations security
* Explain Confidentiality, Integrity, and Availability
* Explain the legal and ethical issues surrounding information security

*Description/Requirements:*

Professionalism is a graded assessment in all Information Systems courses. The Professionalism assignment is based on two key themes found in all Information Systems courses:

1. “The classroom is the workplace.”
2. “Students are professionals in the workplace.”

As in the workplace, students in information systems courses receive performance appraisals. These weekly performance appraisals are a measure of the students “Professionalism”. Professionalism is evaluated based on these criteria:

1. Respectful
2. Responsible
3. Readiness to Learn
4. Timeliness

The “Professionalism Assessment Grading” table that follows provides a model for those behaviors employers seek out and those they disdain in prospective employees. Employers contributed many of these behavior examples. While employers are certainly interested in a prospective employee’s technical knowledge, employers are only interested in hiring those with a professional attitude. A professional attitude is essential for success in the workplace and it is essential for success in the IT classroom. This should be an easy component of the grade to attain for everyone. Just review those positive behaviors in the chart, emulate them in the classroom and emulate them in all communication with fellow students and the faculty member.

Contributing to class discussions is a vital component of the course and the professionalism grade. It’s a measure of the student’s interest and level of familiarity with the information being discussed. Most importantly, participation in the group discussions elevates the group’s knowledge as a whole and makes the course more meaningful to all. Each student is expected to contribute by way of offering supporting information or posing questions about the topic during the evening’s discussions. Each student should join in the group discussions at least once per class. No one should feel that they have nothing to contribute. Everyone’s opinion and need for clarification is valid. Please share your thoughts, comments, and questions with us.

*Grading/Points Possible:*

This assignment is worth 20 points. This grade will be assessed at the end of the semester according to the behaviors detailed in the Professionalism Assessment Grading table that follows.

# Professionalism Assessment Grading

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Students will be evaluated based on in class and email communications using the professionalism criteria below. Review the behaviors below carefully. Your score for each section will be calculated by multiplying the potential points by the percentage rounded up to the nearest integer. It is the student’s responsibility to explicitly and consistently demonstrate these attributes to the faculty member who will be making a subjective value judgment regarding the student’s professionalism.** | | | | | | |
| **Behavior** | **Potential Points** | **0%** | **25%** | **75%** | **100%** | **Total** |
| **Responsible**  **(Contributor)** | **20** | The participant consistently failed or refused to participate in discussions Participant is unreliable, shows no initiative.  OR  Participant is not prepared for class discussions. | Participant shows some responsibility and initiative, respects the standards though may not always adhere to them.  Seldom participates in discussion. | Occasionally, contributes ideas and thoughts on discussion topics  Comes to class prepared and occasionally makes an effort to contribute. | Participant always comes to class prepared and is ready to discuss topics armed with ideas and questions.  Participant assesses concepts being discussed, contributes ideas, views, and comments frequently. |  |
| **Respectful** | **30** | Participant was rude or abusive to other course participants or the instructor.  OR  Participant persists in talking or creating a distraction while the instructor or another student is speaking. | Confrontational attitude towards instructor or other students while participating in discussions or posing questions. | Participant is passive and is not engaged in the class activities. | Participant is always polite and respectful. Does not interrupt others or talk privately while someone is speaking. |  |
| **Ready to Learn**  **(Listener)** | **20** | Participant tends to play a passive or disruptive role in the class, persists in talking while the instructor or another student is speaking  OR  Participant is not seated and logged on to the Stevenson network or other required software prior to the start of the class session. | Participant is preoccupied and not focused on the speaker and is occasionally a distraction. | Participant listens. | Participate is an attentive listener, visibly engaged, and comprehends the subject.  Participant seated and logged on to the Stevenson network or other required software prior to the start of the class session. |  |
| **Timely** | **30** | Missed a class with out providing the instructor advanced notice and a valid excuse.  Fails to turn in assignments or obtain notes from other students. | Periodically shows up late to class which creates a distraction for other students.  OR  Fails to meet deadlines. | Participant is punctual, gets work done one time, | Participant is always on time for class and consistently meets assignment deadlines. |  |
|  |  |  |  |  | **Total points:** |  |

Participant’s Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Assignments/Quizzes**

*Outcomes:*

* Apply the concept of Defense in Depth.
* Identify the tasks of operations security
* Explain Confidentiality, Integrity, and Availability
* Identify the strengths, limitations, and appropriate use of network and physical security tools
* Explain the legal and ethical issues surrounding information security

*Description/Requirements:*

This quiz will cover the readings and class discussion from the prior week with an emphasis on course concepts and vocabulary as opposed to application scenarios. Please see the learning units posted under the assignments section of Blackboard for specific details about this assignment.

**I do expect that each student do his or her own quizzes. Having someone else submit the quiz or give you the answers is considered cheating. If detected, both students will receive a “0” for that quiz.**

*Grading/Points Possible:*

Assignments will be worth approximately 10 points per assignment. Quizzes will be worth approximately 25 points each. Quizzes will consist of multiple choice questions; however, make-up quizzes will be essay. Please see the course grading policy for additional details on the grading of late assignments.

**Article Presentations**

*Objectives:*

* Write effective security communications and assessments
* Evaluate security threats from a business perspective
* Identify the tasks of operations security
* Explain Confidentiality, Integrity, and Availability
* Identify the strengths, limitations, and appropriate use of network and physical security tools
* Explain the legal and ethical issues surrounding information security

*Description/Requirements:*

Each student will give one article presentation per semester. A sign-up sheet will be provided. Each presentation should be 5-10 minutes and should discuss a recent information security/information assurance issue. Identify how the article is relevant to security and business professionals- what lessons can be learned.

*Grading/Points possible:*

Article presentations are worth 20 points.

**Exams**

*Objectives:*

* Identify, evaluate, and select the most cost effective security solutions for a given organization
* Write effective security communications and assessments
* Complete the risk assessment process for a given problem.
* Evaluate security threats from a business perspective
* Apply the concept of Defense in Depth.
* Identify the tasks of operations security
* Explain Confidentiality, Integrity, and Availability
* Identify the strengths, limitations, and appropriate use of network and physical security tools
* Explain the legal and ethical issues surrounding information security

*Description/Requirements:*

A midterm and a final exam will be given. Exams will be given in class and will contain a combination of objective questions as well as exercises covering the assigned readings to that point. Please see course schedule for exam dates.

*Grading/Points possible:*

The Mid-term exam is worth 150 points and the Final exam is worth 200 points.

**Final Project**

*Outcomes:*

* Identify, evaluate, and select the most cost effective security solutions for a given organization
* Write effective security communications and assessments
* Complete the risk assessment process for a given problem.
* Evaluate security threats from a business perspective
* Perform research, write a technical analysis, and deliver a professional presentation detailing a site security plan.
* Apply the concept of Defense in Depth.
* Identify the tasks of operations security
* Explain Confidentiality, Integrity, and Availability
* Identify the strengths, limitations, and appropriate use of network and physical security tools
* Explain the legal and ethical issues surrounding information security

*Description:*

For this project, students will assume the role of outside security contractors. Students will be given a company profile, and will bre responsible for determining the risks facing that company, and designing a site security plan to address that company’s needs.

*Requirements:*

1. Create a **Risk Assessment.** This should be approximately 20 pages identifying security risks you are addressing and scenarios where this could impact the company. It should also include the impact if the security risks are not addressed. The audience is the management of the company.
2. Create a **Physical Security diagram.** Using MS Visio, identify how physical threats identified in the Risk Assessment should be mitigated. The plan should be appropriate to the risks faced and the assets being protected.
3. Create a **Network Diagram.** Using MS Visio, identify how network based attacks identified in the Risk Assessment will be mitigated. The plan should be appropriate to the risks faced and the assets being protected. The diagram should show how the technologies being used will be deployed.
4. Create a **Budget Request.** This document will show the products selected to secure the company and how they will be deployed. The products should correspond to the network and physical security diagrams and implimenting the mitigations identified in the Risk Assessment. Product strengths and weaknesses should be discussed, and compared to products that were not selected. A cost benefit analysis should be included. While the discussion of the merits of selected products is encouraged, an excel spreadsheet of detailed costs (including profit) is to be included.
5. **Printed project proposal and Power Point Presentation.** All the items above will be presented to the class in a sales pitch format. Presentation skill and preparation as well as content will be graded. **A formal, printed and bound presentation document is given to the instuctor at the date and time the presentation class is to begin. Anything handed in after this time is considered late.**

*Grading/Points possible:*

This project will be worth 200 points. Of that 200 points, half will be based on your written work and half on your presentation. **Spelling, grammar, binding, use of color and overall professional appearance count**. This project will be assessed using the rubric on the pages that follow:

**Final Project Rubric NAME:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

| **Grade:** | **Element** | 20 | 13 | 8 | 0 |
| --- | --- | --- | --- | --- | --- |
|  | Risk Assessment | Includes all relevant information as outlined in the assignment description. Professional presentation. | Missing important information outlined in the assignment. | Missing important information outlined in the assignment. Unprofessional presentation (Spelling mistakes, formatting errors.) | Assignment not handed in. |
|  | Physical Security Diagram | Clear and easy to understand at a glance. Includes appropriate protections for the company profiled. Professional presentation. | Missing critical defense elements or has inappropriate protections included. | Confusing and/or incomplete diagram.  Missing critical defense elements or has inappropriate protections included. | Assignment not handed in. |
|  | Network Security Diagram | Clear and easy to understand at a glance. Includes appropriate protections for the company profiled. Professional presentation. | Missing critical defense elements or has inappropriate protections included. | Confusing and/or incomplete diagram.  Missing critical defense elements or has inappropriate protections included. | Assignment not handed in. |
|  | Budget Request | Fully explains technologies and that were selected. Provides cost/benefit analysis. Shows why alternate products were no selected. | Poor explanation of why products were used. Some technologies may not be appropriate for the company profiled. | Poor explanation of why products were used. Plan is inappropriate for the company profiled. Cost benefit analysis is unclear. | Assignment not handed in. |
|  | Printed proposal | Proposal is professional looking and easy to read. | Some information missing, a few errors in grammar. | Proposal is messy with numerous errors and missing important information | Not handed in |
|  | **:TOTAL** |  |  |  |  |
| **Presentation:** | **Element** | 100 | 75 | 50 | 0 |
|  | Power Point Presentations | Presentation is smooth. Presenter is understands content, is able to answer questions. Does not read from slides, but uses them for visual aid. | Presenter understands content. Delivery is choppy, and slides are read to audience verbatim. | Presenter does not grasp content, or is unable to convey grasp of content. | Assignment not handed in. |

**Additionally: On all written work, 2 points will be deducted for each typo/spelling/grammar error. 2 Points will be deducted for each instance of redundancy. 5 Points will be deducted for each instance of factually innacurate or misleading information.**

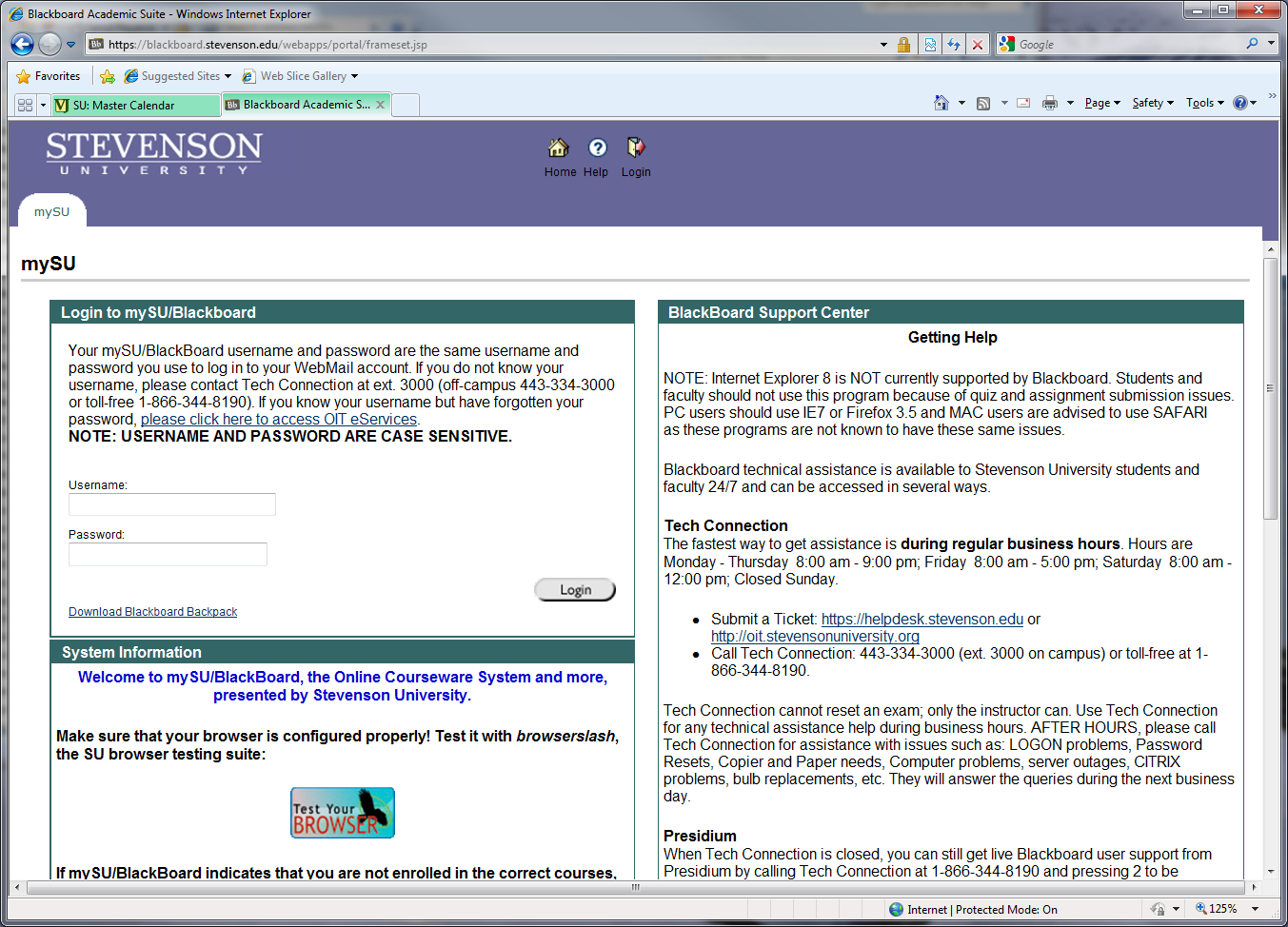
**Additional Resources**

Additional resources for the completion of course requirements are included in the pages that follow. These resources include:

* Blackboard
* Stevenson College Policies

**Blackboard Web access**

Each student taking a graduate accelerated course will have access to an Blackboard (Blackboard) website for their course. You will access Blackboard via URL <https://blackboard.stevenson.edu> (no www) as follows:



Click on and enter your Blackboard login.

Once you log in, you go to a viewing area that lists your classes and any announcements. Use the toolbars to navigate through Blackboard.

**Stevenson College Policies**

## Network Security Agreement

All components of the Stevenson College Network Security Agreement will be enforced in this class. Failure to abide by this agreement will result in the loss of your access to the college computer facilities. The loss of computer access will not excuse you from completing any of the course requirements. Class assignments, announcements, and other materials may be distributed via e-mail, the Stevenson network or the Stevenson Blackboard during the semester. It is the responsibility of the student to check their Stevenson e-mail account and Blackboard each school day, to check the class network directory, and to report to the instructor any problem with the campus telecommunications system.

## Email Policy:

All college email communication will be exchanged **only over Stevenson email accounts**. Students are responsible for the information sent to their Stevenson email account and must monitor their Stevenson accounts each day for important college and course related information. Students are required to view their Stevenson email accounts directly or set up their Stevenson email account to forward to an account they view regularly during the day. If you are not receiving regular information over a forwarded email address you should immediately investigate the problem before missing important instructions or announcements. Students should also note that email messages in their MAILBOX and personal mail folders are routinely purged on a regular schedule.

**A violation of this policy will result in a grading penalty to be determined at the discretion of the instructor.**

## Classroom PC Acceptable Use Policy

During class time, the classroom PC is to be used for class activities only as directed by the instructor. Any other use is in violation of the Classroom PC Acceptable Use Policy.

* The use of cell phones, PDAs or other electronic devices will not be allowed during class time. These devices are to be turned off before the start of each class.
* Monitors are to be turned off at the start of class unless otherwise directed by the instructor.
* The use of Instant Messaging (IM) or email is prohibited during class.

Penalty:

Failure of a student to follow the Classroom PC Acceptable Use Policy may result in the student being asked to leave the class and / or the subtraction of points from the student’s final average.

**The instructor is in charge of the classroom. Refusal of any request to turn off monitors, cell phones, or any other equipment detailed in this policy will result in a grading penalty the range of which is at the discretion of the instructor**.

## Academic Honesty Policy

Any attempt to commit cheating, plagiarism, unauthorized assistance, fabrication, multiple submissions, or other violations as defined in the Stevenson academic Honesty Policy constitutes academic dishonesty. A violation of academic honesty is considered a serious offense by the college administration. Penalties include loss of credit for the assignment or failure of the course at the discretion of the instructor. Violations may also lead to dismissal from the program or college at the discretion of the Associate Dean for Academic Support Services. Any attempt to commit the following offenses constitutes academic dishonesty.

**Cheating:** Using unauthorized material to complete a test, quiz, examination, or assignment. Cheating includes, but is not limited to, copying from other students, relying upon aids or notes during a test, or consulting outside sources without the instructor's permission. Giving unauthorized assistance to other students also constitutes cheating.

**Plagiarism:** Representing the words, ideas, research, or works of another as one’s own.  Plagiarism can involve submitting work prepared entirely or in part by another person or commercial service or borrowing material as direct quotation, partial quotation, or paraphrase from published or unpublished sources without proper acknowledgement.  Students must document all print, online, and oral sources they use to complete assignments.

**Unauthorized Assistance:** Preparing an assignment with the help of another student or allowing another person, such as a tutor, to alter or revise an assignment beyond the scope of collaboration the instructor has defined.

**Fabrication:** Presenting false data, sources, or research results for academic credit.

**Multiple Submission:** Presenting the same work, in whole or in part, for credit in more than one course without the explicit permission of all interested instructors.

**Other Violations:** Including, but not limited to, lying, forgery, bribery, damaging or stealing college or another’s property, physically abusing another person, or verbally threatening another.

(See www. <https://www.stevenson.edu/fas/policy-manual/default.asp> for the full Academic Honesty Policy.)

**Any violation of the Academic Honesty Policy may result in an ‘F’ for the assignment or an ‘F’ for the course at the discretion of the instructor. This penalty could be changed to dismissal from the college by higher authorities.**

## Writing Policy

Plagiarism is considered a serious offense by the college administration and can result in the student’s dismissal from the program. Plagiarism is the intentional or unintentional presentation of another person's idea or product as one's own. Plagiarism includes, but is not limited to, copying verbatim all or part of another's written work: using phrases, conclusions, charts, figures, illustrations etc. without citing sources. Penalties include a grade of zero or F for work, a grade of F for the course, or dismissal.

**A violation of this policy will result in a grading penalty to be determined at the discretion of the instructor.**

## Students with Disabilities

Consult the Stevenson Student handbook.