| | |
|---|---|
| **COURSE TITLE**<br>**BLACKBOARD SITE** | MIS 7233 Network Security<br>Summer 2011 – http://my.ltu.edu and select CRN 5492 |
| **INSTRUCTOR** | Robert Montgomery<br>Adjunct Lecturer, Graduate College of Management<br><br>E-mail Rmontgome@ltu.edu Web www.ltu.edu/ltuonline<br>Work Phone 248.232.4806<br>Office Location Online<br>Office Hours: by appointment<br>Notes: Please contact me first via e-mail. |
| **SCHEDULE** | May 18, 2011 – July 28, 2011<br><br>Refer to http://www.ltu.edu/registrars_office/calendar_final_exam.index.asp for the last date to withdraw and other important registration related information. |
| **LEVEL/ HOURS**<br>**PREREQUISITE** | This course will satisfy general elective requirements for DMIT, MSIS, BSCS, MSECE, MSCE, and BSCE. Three (3) Graduate Level Credit Hours<br>Prerequisites: Graduate level MIS 6143 Minimum Grade of C- |
| **REQUIRED TEXT**<br><br>(See Blackboard for additional resources) | 1. Principles of Computer Security: CompTIA Security+ and Beyond, by W.A. Conklin et al. McGraw-Hill Osborne Media, 2009. ISBN 978-0071633758<br>2. Readings and Cases in the Management of Information Security, by M. Whitman & H. Mattord. Course Technology, 2005. ISBN 978-<br><br>Available for online purchase through LTU Bookstore at:<br>http://lawrence-tech1.bkstore.com/bkstore/TextbookSelection.do?st=489<br><br>Additional Resources<br>1. ISO/IEC 17799 – Information Technology – Code of practice for Information Security management<br>2. NSAI/IS 17799-2 – Information Security Management Systems – Part 2: Specification with Guidance for Use |
| **ADDITIONAL RESOURCES** | LTU Online student resources: http://www.ltu.edu/ltuonline/ |
| **TECHNICAL SUPPORT** | Technical support for using Blackboard is provided by the Helpdesk. Visit www.ltu.edu/ehelp or 248.204.2330 or helpdesk@ltu.edu. Send the Help Desk a form detailing any issues by clicking here http://tinyurl.com/3yqrvne. |

**COURSE SCHEDULE FOR TRADITIONAL & COLLEGE OF MANAGEMENT SEMESTER COURSES**

This fully online course begins with a partial week online course orientation period to familiarize yourself with the online learning environment and to meet online or via the phone with your instructor. Each subsequent week starts on a Monday and ends on a Sunday.

| Dates | Modules | Topics / Readings | Assignments Due |
|---|---|---|---|
| Prior to Semester Start and May 18 – May 22 | Module 0 | Online Learning Orientation<br>Course Familiarity<br>Student introductions<br>Chapters 1-4 | TMAY |
| Week of May 23 – May 29 | Module 1 | Chapter 5- Cryptography | Bb Forums<br>Assignment 1<br>Due : May 29 by 10 pm |
| Week of May 30 – June 5 | Module 2 | Chapter:<br>6 PKI,<br>8 Physical Security,<br>10 Infrastructure Security | Bb Forums<br>Assignment 2<br>Due: June 5 by 10pm. |
| Week of June 6 – June 12 | Module 3 | Chapter:<br>7 Standards/Protocols,<br>9 Network Fundamentals | Bb Forums |
| Week of June 13 – June 19 | Module 4 | Chapter:<br>11 Remote Access,<br>12 Wireless/IM | Bb Forums<br>Assignment 3<br>Due: June 19 by 10pm. |
| Week of June 20 – June 26 | Module 5 | Chapter:<br>13 Intrusion Detection Systems | Bb Forums<br>Mid-Term exam:<br>90 mins/100 questions<br>8am June 23-10pm June 26 |
| Week of June 27 – July 3 | Module 6 | Chapter:<br>15 Attacks & Malware,<br>18 Software Development | Bb Forums<br>Assignment 4<br>Due: July 3 by 10pm. |
| Week of July 4 – July 10 | Module 7 | Chapter:<br>16 Email,<br>17 Web Components | Bb Forums |
| Week of July 11 – July 17 | Module 8 | Chapter:<br>14 Baselines,<br>20 Risk Management | Bb Forums<br>Assignment 5<br>Due: July 17 by 10pm. |
| Week of July 18 – July 24 | Module 9 | Chapter:<br>21 Change Management,<br>22 Privilege Management | Bb Forums |
| Week of July 25 – Jul 28 | Module 10 | Chapter:<br>19 Disaster Recovery/ Business Continuity Planning,<br>23 Forensics | Bb Forums<br>Assignment 6<br>Due: July 28 by 10pm. |
| **THIS IS A 10 WEEK SEMESTER. THE SEMESTER WILL BE CONDENSED TO INCLUDE REMAINING COURSEWORK AND FINAL EXAMS.** | | | |

**STUDENT EVALUATION**

The course has six assignments, discussion board activities, and a mid-term exam totaling 100 points (left column). Letter grades are awarded based on the total number of points achieved. Points are deducted for late assignments.

EXAMPLES:

| Assignments | Points |
|---|---|
| Individual Assignment 1<br>CNSS, US-CERT Research Report | 50 |
| Individual Assignment 2<br>CISSP, Security+, SSCP, CISM, CCSP, Other Exams | 100 |
| Individual Assignment 3<br>Activity – Security Situation – Select any TWO of the 4 activities | 100 |
| Individual Assignment 4<br>Infrastructure Security Case - Proposal | 100 |
| Individual Assignment 5<br>Intrusion Detection System | 100 |
| Individual Assignment 6<br>Risk Management | 100 |
| Midterm Exam<br>Chapters covered to date | 250 |
| Online Participation<br>Online Forum Discussions on Bb | 200 |
| Total | 1000 |

| Class Points | Letter Grade |
|---|---|
| 96 and above | A |
| 90 – 95.9 | A- |
| 87 – 89.9 | B+ |
| 83 – 86.9 | B |
| 80 – 82.9 | B- |
| 77 – 79.9 | C+ |
| 73 – 76.9 | C |
| 70 – 72.9 | C- |
| 61 – 70 | D (Undergrad Only) |
| 60 and below | E |

*Note: Grades lower than a "B" fall below the LTU graduate standard*

**EDUCATIONAL GOALS**

This course offers an in-depth exploration of security issues and related challenges for any organization. It is highly technical, and focuses on Information and Computer Security technologies, tools, techniques and approaches. This course addresses emerging technologies and best practices that are state-of-the-art. It can yield significant value to the student during the implementation phase of an enterprise information security plan.

The course is designed to take a deep dive in today's technologies of computer security. It will discuss the following topics in depth:

- Cryptography
- Security Standards and Protocols
- Infrastructure Security
- Internet and Web Security
- Intrusion Detection and Prevention
- Wireless security and remote access
- Disaster Recovery and Business Continuity
- Computer Forensics
- Risk Management
- Patch Management
- Privilege Management
- Auditing
- And more

Students who attend this course should have had some background knowledge in computer networks, enterprise computer security policy, and an overall understanding for the need to implement an information security plan.

**STUDENT LEARNING OBJECTIVES / OUTCOMES**

This course is designed for students working toward a degree in MSIS, MSECE, MSCE, and other disciplines with focus on Information and Computer Security. This course may be considered as one of several courses required to satisfy that emphasis. Students can gain a greater advantage if they come into this course having had:

- An enterprise information security type course
- A data telecommunication course, or
- A networking / infrastructure course

This course is NOT intended to be an introduction to information security and assumes that the students already understand the importance of developing an enterprise information security plan and policy.

The objective of this course is to equip the students with the knowledge necessary to address tactical and strategic business issues by selecting and recommending the appropriate technologies and tools necessary to solve a business problem related to the security of information and computers.

Ideally, the student will be prepared to provide an optimal solution to a real-life information security business problem upon successful completion of this course. Understanding the pros and cons of the various technologies and techniques that are available for use in order to secure and protect intellectual property and the infrastructures that contain it, the student should be able to apply the appropriate tools, techniques, and technologies to the situation at hand effectively.

Upon successful completion of this course, each student should have a deep understanding of both business and technical issues related to:

1. Adopting/developing and implementing information security Best Practices
2. Managing risk and protecting against network attacks and malware (DoS, spoofing, hijacking, viruses, worms, Trojan horses, zombies, logic bombs, etc)
3. Understanding various types of devices that construct the infrastructure, the variety of media that carry network signal, the diversity of storage devices, and how the use of security zones and other topologies provide network/web-based security.
4. Defending the infrastructure with techniques, technologies and approaches such as authentication, digital signatures, digital watermarking, digital certificates, public and private keys, intrusion detection, intrusion prevention, standards and protocols (PKIX/PKCS, X.509, SSL/TLS, ISAKMP, CMP, S/MIME, PGP, HTTPS, IPSec, FIPS, WTLS, WEP, ISO 17799) and cryptography
5. Understanding the vulnerabilities of Wireless LAN's, WAN's, Protocols and Instant Messaging, and how Remote Access methods can be effectively applied to maximize security and privacy (WAP, WTLS, WEP, AAA, VPN, SSH, Telnet, Tunneling L2TP, PPTP, IEEE 802.11, 802.1X, RADIUS, etc)
6. Hardening various operating systems, network devices, and applications (with special emphasis on e-mail transmissions), and establishing the system's security state (baselining process)
7. Understanding hacking threats & the importance of trustworthy code
8. Securing and protecting Web Components (SSL/TLS suite, LDAP, FTP, Web Services, plug-ins, directory services, dynamic content, applets, servlets, malicious cookies, etc)
9. Incorporating security best practices into the software development process in order to prevent/minimize future/production attacks.
10. Understanding the importance of auditing, what should be audited, and how to conduct an effective and timely audit.
11. Understanding Disaster Recovery and the different strategies and alternatives that can maintain Business Continuity (of course, the subject of Disaster Recovery is so broad and diverse, and deserves to have a course on its own).
12. Applying Privilege Management using the advantages of single sign-on and other techniques
13. Understanding the rules of Computer Forensics and how various types of evidence can be used to prevent future computer crime
14. Legal and ethical aspects of network security

To pursue the course objectives effectively, students will engage in the following activities:

- Read assigned material prior to the online sessions
- Complete individual assignments and submit them on time
- Participate in online class discussions (via BB Discussion Board)
- Complete a midterm examination

Unless specifically authorized by the professor, all work assignments should be solely the student's own individual work.

**PREREQUISITE SKILLS**
Students who attend this course will have had some background knowledge in computer networks, enterprise computer security policy, and an overall understanding for the need to implement an information security plan.

**INSTRUCTIONAL METHODS AND COURSE ORGANIZATION**

**Blackboard Learning Environment** – Blackboard at my.ltu.edu contains the syllabus, all assignments, reading materials, streaming videos, narrated PowerPoint mini-lectures, podcasts, written lecture notes, chapter quizzes, links to Web resources, and discussion forums. You will submit all assignments via

Blackboard, and are expected to participate regularly in discussion topics. Please take time to familiarize yourself with the organization of the Blackboard site. You will want to check the site frequently for announcements reminding you of new resources and upcoming assignments.
**Student/Instructor Conversations** – Students keep in touch with the instructor via e-mail messages, telephone conference calls, and IM conversations.
**Self-Assessments** – Pre- and post- self-assessment tools will help students measure their entering skills and progress during the course.
**Required Reading** – Textbook chapters should be read according to the schedule outlined in the syllabus. Chapters will be discussed online.
**Assignments** – See the assignment details at the end of the syllabus.

**CLASS POLICIES AND EXPECTATIONS**

*I plan to offer you a valuable learning experience, and expect us to work together to achieve this goal. Here are some general expectations regarding this course:*

Each student has a LTU email account. If you wish to use a different email address for this course, please **change your email address in Blackboard under "Blackboard Tools", then "Personal Information"** and send an email to me so I can store your address in my email directory.

Readings, discussion forum participation, and written assignments must be completed according to the class schedule. It is important to contact the instructor as needed to discuss personal needs regarding course requirements and assignments.

It is essential that all students actively contribute to the course objectives through their experiences and working knowledge.

All assignments must be submitted on schedule, via Blackboard, and using Microsoft Office compatible software. If you need to submit an assignment via email, contact the instructor in advance.

Assignments must be completed to an adequate standard to obtain a passing grade. Requirements for each assignment are detailed in this syllabus.

Be prepared to log into Blackboard at least once each day. Please focus your online correspondence within the appropriate Blackboard discussion forums so that your colleagues can learn from you.

At midterm and at the end of the course, you will be invited to participate in a University evaluation of this course. Your feedback is important to the University, to LTU Online, and to me as an instructor, and I encourage you to participate in the evaluation process.

The topics listed in the syllabus are only an estimate of the material, which can be covered during the semester. Some topics might be deleted and some others might be added at the discretion of the instructor. Teamwork and collegiality are encouraged but everyone must understand and be responsible for their work, actions and work products; observations of the Honor Code Policy are mandatory. http://www.ltu.edu/currentstudents/honor_code.asp All other University policies regarding incomplete grades, etc. apply.

It is important for you as students to know what to expect from me as your instructor:

- I will be available to you via e-mail and phone, and will promptly reply to your messages.
- I will maintain the Blackboard web site with current materials, and will resolve any content-related problems promptly as they are reported to me.
- I will send out a weekly e-mail update to all class members to guide upcoming work and remind you of assignment due dates.

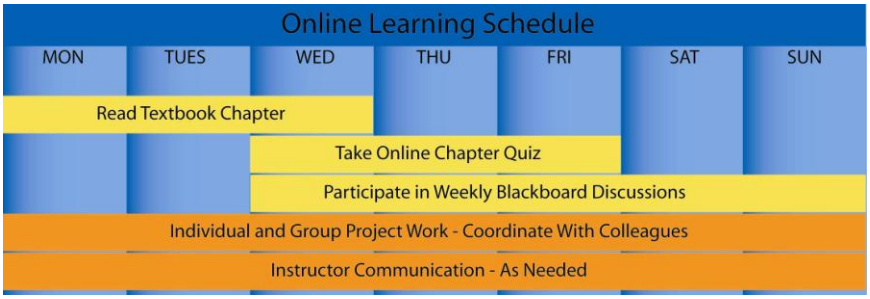
- I will return all assignments to you promptly, and will include individualized comments and suggestions with each assignment.
- I will hold our personal written or verbal communications in confidence. I will not post any of your assignments for viewing by the class without requesting your approval in advance.
- I will treat all members of the class fairly, and will do my best to accommodate individual learning styles and special needs.
- If any of these points need clarification, or when special circumstances arise that require my assistance, please contact me so that we can discuss the matter personally.

**PRACTICAL GUIDELINES FOR CLASS LOAD EXPECTATIONS**

A three-credit course generally requires at least nine hours per week of time commitment. Here are some practical guidelines to help schedule your time commitments for this online course:

- A 14-week semester (the Summer semester is compressed into 10 weeks) would require at least 126 hours of time commitment to successfully complete all readings, activities, assignments, and texts as described in this syllabus.
- You should reserve at least 6 hours per week to read the required textbook chapters and resources, participate in online discussions, review presentation materials, and work through online quizzes. This effort will total at least 84 hours over the course of the semester.
- You should organize your remaining time to roughly correspond with the point value of each major assignment. This means that you should plan to spend at least:
  - 8-9 hours preparing your case study review;
  - 24-40 hours working with your group on the three parts of your semester-long project;
  - 8-9 hours working on the various components of your reflective consolidation (final exam).

These guidelines may not reflect the actual amount of outside time that you – as a unique individual with your own learning style – will need to complete the course requirements. The number of hours each week will vary based on assignment due dates, so please plan ahead to insure that you schedule your academic, work, and personal time effectively. The following graphic can be used to guide you in planning your weekly course work to remain on schedule:




**ASSIGNMENT DETAILS**

Course assignments and evaluation criteria are detailed below. Please review these requirements carefully. See the section Academic Resources / Assessment Guidelines for information about assessment of written and oral presentations.

Details for all assignments are shown below. Please note that you should not submit any assignments to the Blackboard “Digital Drop Box.” All assignments are submitted using the Blackboard “Assignments” or “SafeAssign” function. Some assignments are also posted to the Blackboard Discussion Forum for student comments.

## Assignments

### Assignment # 1
### How prepared are we?

Students should visit the Center for National Security Studies (CNSS), US-CERT http://www.us-cert.gov/, and other cyber-terrorism and counter-terrorism websites including the Whitehouse and the Department of Homeland Security (DHS), and summarize their findings, assessments, and personal opinions regarding the US readiness in combating information threats and attacks, and the degree to which Information Technology is able to address national and global information security issues.

The length of the report should be a minimum of 1,200 words but should not exceed 2,000 words, using APA style format with references (both within and at the end) and a font of "Arial 12".

### Assignment # 2
### Security Certification Research
### "Some certifications are hot, some not"

Security Certification has increasingly become an important consideration among business managers and technical professionals alike. With the advent of 9/11 terrorism and the progressive threats and attacks on computer and data systems worldwide, governments and businesses have sharply increased their requirements for information security certified professionals.

Students should research information on the various types and classifications of Security Certifications from a variety of sources. At minimum students should contrast, compare, and report on the following certifications:

CISSP (from ISC2)
CompTIA Security+
SSCP
CISM
CCSP, and
Other relevant Certifications and Exams.
Your personal observations and conclusions on certification

**Assignment # 3**
**Security Scenario**

For the 2nd assignment, you may select ANY TWO of the 4 following activities – the choice is yours. Remember: you should answer ONLY TWO of the 4 activities:

Activity 1: E-mail memo to customer regarding Melissa virus incident
Situation:

Recently, a workstation in the Engineering Department was infected with a virus delivered through e-mail. You investigate and discover that the virus did not penetrate your normal security protections, which would have detected and cleaned the e-mail arriving through the company's mail servers. An engineer had, however, in addition to the normal company mail, established a Hotmail account and had downloaded an e-mail unaware of the virus that was attached. When the engineer opened the attachment, the virus installed itself. The Hotmail account was not being used for work purposes; however, everybody knows that employees access web mail for personal reasons on a regular basis.

You need to solve the problem, and then prepare an incident report (see template in Assignments section) that describes the incident and what you did to resolve the problem.

Write an informal cover (for the incident report) email to your supervisor.

In the memo, describe in your own words what happened, and the corrective action taken.

Criteria for Success:

At least two solutions to the problem including (1) user education and (2) the regular use of antivirus software. Your solutions will be read for reliability and effectiveness of the proposed solutions. For instance, how reliable will user education be in preventing users from using non-secure e-mail services at work? When you suggest installing and keeping antivirus software up-to–date, discuss the most reliable strategy for doing this.

Appropriate and correct language for the intended audience, in this case a technical audience. The language should be accurate, spell-checked, and grammatically correct.

Activity 2: Factory worker doing eBay business on company's computer
Situation:

Acme allows employees to use their computers for personal use such as checking bank statements and personal Web searches. An employee has requested that he be able to use his laptop at work and home for checking his eBay store during lunch breaks and at home for doing other eBay activities. Your boss has asked you to study the issue and recommend a company policy regarding eBay. Determine if there are any security issues associated with eBay. Choose a position and develop pros and cons in the policy. Draft the policy in a memo format.

Criteria for Success:

Display knowledge of security issues as relevant to the requirement.
Develop position developed logically and with general security policies in mind.
Use accurate and appropriate language that is spell-checked and grammatically correct.

Activity 3: Engineer is not allowing his workstation to be updated with the most recent patches
Situation:

An engineer is not allowing his workstation to be updated with the most recent patches because the updates cause problems. His workstation is used to run large computations and many computations may run for days. Updates, especially automated patches and virus fixes, often require reboots. These unplanned reboots interrupt the computation, which forces the engineer to restart the computation from the beginning. Unscheduled reboots have direct impact on his schedule to support his projects. The results of the computations and many graphics files created are used by other engineers. They are stored in JPG format on his workstation, so his system must be on the network that exposes it to virus infections. Company security policy requires virus updates and security patches to be kept up-to-date. Explain the importance of following the Company security policy and let him know that you will be providing him a solution. Then type a memo to your manager in which you suggest three solutions with their pros and cons, and recommend the best solution.

Criteria for Success:

Write a memo to engineer regarding the security policies and reasons for the need to comply with the security policies.
Write a memo to your supervisor describing alternative plans to solve the problem.
Spell-checked and grammatically correct language.

Activity 4: A company executive is concerned about company's confidential data being compromised
Situation:

Acme has recently begun work on a new product that requires the engineers to collaborate with another firm located in another state. In order to collaborate, the engineers are using shared design software on Acme's server. They also plan to co-develop technical documentation, which will be stored on Acme's server. An Acme executive is concerned that the company's confidential data will be compromised on the project, if outsiders are allowed to access proprietary information. You have been asked to give a presentation on the security aspects of remote access and how the security procedures such as VPN and cryptography will protect Acme's confidential information. A short PowerPoint presentation on how VPNs and cryptography will protect Acme's network should be appropriate for Acme's high level managers.

Criteria for Success:

Detailed information regarding VPN, how it works, and why it is more secure than a normal network.
Description of cryptographic techniques and the one, which is most secure.
A suggested solution with justifications for the solution being a best practice.
PowerPoint presentation with title page, table of contents, purpose, body, and conclusion charts.
Spell-checked and grammatically correct language.

**Assignment # 4**
**Infrastructure Security**

To complete this assignment, you need to read "Reading 2", which can be found on page #8 in the Readings and Cases in the Management of Information Security Textbook, AND, "Case A", which can be found on page A-1 of the same book.

Here, you are presented with a fictitious computer gaming company (CGT, Inc.) that has put out a Request for Proposal (RFP) relative to a variety of security needs and objectives that will align with and support the company's goals, if implemented effectively.

The proposal you prepare in response to the RFP has a well-structured format that you should follow. This case study will expose you to a number of security topics, but most importantly, I'd like you to focus the bulk of your efforts on the logical and physical security design, and implementation strategies which can be found under sections III and IV of the RFP on page A-9. These 2 sections will provide ample opportunity to leverage the Infrastructure Security knowledge you gained from chapters 6, 8, 9, 10, 17, and 18 of your main textbook – Principles of Computer Security.

Your job is to prepare and present a proposal in response to CGT's RFP which starts on page A-7. Again, please make sure you follow the proposal format with the following exceptions:

In section I, you may skip the following items:

Feasibility Study. We will assume that the project is feasible.
Estimate of costs
Feasibility analysis

In section II, you may skip the following:

Documentation of findings and updated feasibility analysis. **You should document your findings,** but ignore the updated feasibility analysis.

In section III, you may skip the following:

Feasibility

Recommendation for continuing and/or outsourcing the project

In section IV, you may skip the following:

Documentation of the system
Updated feasibility analysis

Section V maybe skipped all together.

Appendix A and B: may be skipped in its entirety.

**Assignment # 5**
**Intrusion Detection System**

This assignment is being re-designed and will be made available after the term begins.

**Assignment # 6**
**Risk Management**

To complete this assignment, you need to read "Reading 5", which can be found on page #45 in the Readings and Cases in the Management of Information Security Textbook, AND, "Case B", which can be found on page B-1 of the same book.
Here, you are presented with a fictitious government agency that is dealing a number of security issues. The case clearly identifies the risks and vulnerabilities, and discusses the recommendations for mitigating such risks.

Your job is review, assess, and debate each pair of risk/mitigation, and answer the following questions:
State the risk/vulnerability in your own words. If you had to tell the CIO about this risk during your elevator ride with him down to the cafeteria, what would you say?

In your opinion, what is the source(s) of these risks? For example, are they related to Policy or lack of it? User Education and Awareness? Technology? A combination of 2 or all of the above? Is there a single Root Cause? List as many sources/causes as you can.

State the mitigation technique for this risk in your own words, much like the same approach in the 1st question. Do you agree with the prescribed mitigation? Why/Why not? What would you suggest to improve the proposed mitigation? Can you come up with a better mitigation plan? What is you contingency plan to this mitigation plan?

Draft your report, which you will submit to your CIO, to the tune of 1,200 to 2,000 words, single space, using APA style format with references and a font of "Arial 12".

## Online Participation (20 points per Discussion)

Each student is expected to actively participate in online activities. **Class participation is evaluated to a maximum of 20 points** based on actively participating in Blackboard discussion forums, responding to questions posted by the instructor, and interacting positively with other students.

### SYLLABUS ADDENDA

Please see the LTU Online "Current Students" web site http://www.ltu.edu/ltuonline/ for comprehensive information about Lawrence Tech's academic services, library services, student services, and academic integrity standards. The content of this web site is explicitly included as syllabus requirements.

The LTU Online "Current Students" web site also includes grading rubrics used by your instructor to evaluate written assignments, discussion forum participation, and group assignments. Please note that the SafeAssign anti-plagiarism product will be used for written assignments submitted for this course. Please see the instructions included on the LTU Online web site regarding the use of the SafeAssign product.

Leadership Transcripts

The leadership transcript enables students to track co-curricular activities that are undertaken above and beyond the requirements of the LTU curriculum. The leadership transcript serves students by enhancing the leadership portfolio; providing the opportunity for a transcript of distinction; enhancing their resumes; and assisting in articulating leadership experience. It can be accessed by logging on to Banner Web and clicking the Student and Financial Aid tab. Leadership Activities is located at the bottom of the list.