The University of Texas at Austin
Master of Science in Information Security and Privacy
School of Information and Center for Identity

ISP 383 BUSINESS GOVERNANCE AND CONTROLS FOR INFORMATION SECURITY AND PRIVACY
UNIQUE NUMBER: 28515
Fall 2023

INSTRUCTIONAL MODE: Hybrid

CLASS MEETS: 1pm-5pm on F/S in Thompson Conference Center (TCC) Room 3.102 & on Zoom

Instructor: Dr. Hüseyin Tanriverdi
Office: CBA 5.208
Office hours: by appointment
Email: Huseyin.Tanriverdi@mccombs.utexas.edu
Phone: (512) 232-9164

Teaching Assistant: Dylan Beldon
E-mail: dylan.beldon@beldon.com

COURSE DESCRIPTION
This course makes an introduction to digital risks and risk mitigation mechanisms of organizations. Digital technologies have become a critical enabler and transformer of business innovation, growth, and profitability across almost all sectors of the economy. Digital technologies have also heightened cybersecurity, privacy, and ethical dilemma risks that impact the confidentiality, integrity, availability, and ethical, responsible use of information assets. If not governed and controlled effectively, the realization of these risks can lead to operational disruptions, financial loss, reputational damage, lawsuits, compliance problems, and destroy value for shareholder. The course will cover established governance and control frameworks for mitigating risks and achieving returns of digital technologies. It will also explore risks and mitigation mechanisms of emerging digital technologies such as Artificial Intelligence (AI), Robotic Process Automation (RPA), Process Mining, Blockchain, Internet of Things (IoT), etc. It is important for business leaders to understand how they can institute governance and control mechanisms to minimize such risks, maximize returns of digital technologies, and obtain favorable risk-return outcomes. This course aims to equip students with such skills and knowledge.

LEARNING OUTOMES (LO)
In this course, you will make an introduction to and master the following concepts and skills:
* LO1: How to apply NACD framework on board oversight of cybersecurity risks
* LO2: How to apply COSO framework for enterprise risk management
* LO3: How to apply NIST Cybersecurity framework for enterprise cyber risk management
* LO4: How to apply COBIT framework for enterprise IT risk management
* LO5: How to apply AICPA generally accepted privacy principles for enterprise privacy risk management
* LO6: How to apply IT general controls and IT application controls concepts in IT audits, and compliance with relevant laws, regulations, and industry standards
* LO7: How to use system and organization control (SOC) audit reports to manage third-party risks
* LO8: How to make sense of emerging security, privacy, and ethical dilemma risks of emerging digital technologies (e.g., AI, RPA, process mining, blockchain, IoT, etc.)
* LO9: How to apply ethical decision making frameworks in making sense of ethical dilemmas around digital technologies
* LO10: How to apply NIST's AI Risk Management framework and develop additional governance and controls for mitigating emerging risks in AI algorithms (e.g., bias, IT/model failure, privacy breach, cybersecurity breach, adversarial attacks, deepfakes, fake news, etc.)

The University of Texas at Austin
Master of Science in Information Security and Privacy
School of Information and Center for Identity

HOW WILL I LEARN?

- Analyze, write-up, and discuss case studies
- Share control and responsibility for learning by discussing readings, cases, and projects in a participant-centered, active learning format

HOW TO SUCCEED IN THIS COURSE?

- Doing the assigned readings in advance of class discussions
- Writing up the assigned case studies in a timely manner
- Consistently attending classes and actively participating in class discussions
- Being responsive to feedback on case write-ups and in-class contributions

COURSE REQUIREMENTS

REQUIRED MATERIALS

Course website	Hosted on Canvas: http://canvas.utexas.edu/. Updates to this syllabus and other course materials will be posted on this website. Please log on to the site before each class to view the announcements.
Course packet	A digital course packet, which contains electronic versions of some of the cases and articles can be purchased from Harvard Business School Publishing (HBSP) at https://hbsp.harvard.edu/import/1070832 If you face any difficulty with HBSP website in purchasing the course packet, please contact the customer service of HBSP. Reading assignments that are not available through HBSP are posted on Canvas.

REQUIRED DEVICES

- Come to in-person classes with a laptop or a mobile device that allows you to use full features of Zoom.
- This course will use Zoom for taking attendance, running poll questions, and receiving chat responses to some reflection questions.

GRADING FOR THIS COURSE

Assignments	Percent of Total Grade
1. Contribution to class discussions in 10 sessions	20%
2. Individual write-ups: 8 cases total, 10pts each	80%
TOTAL	100%

CONTRIBUTIONS TO CLASS DISCUSSIONS (20%)

We use a participant-centered, discussion-based, active learning format. I expect you to share control and responsibility for learning by:

a) Attendance is mandatory for all MSISP classes and it is a pre-requisite for earning contribution credits. We grade contributions to class discussions rather than attendance per se. Students must attend classes in-person or remotely via Zoom. While class lectures are recorded in support of students' studies, review of class recordings does not constitute attendance or contribution to class discussions. Only extraordinary, documented requests submitted at least 72 hours in advance of class time will be considered for make-up of lost contribution credits of missed sessions. Documented absences will be considered for make-up by the faculty instructor and the MSISP Program Director. There must be a compelling reason for any requests not submitted 72 hours in advance of class start.
b) Verbally engaging in and contributing to class discussions.
c) Thoughtfully responding to Zoom poll questions.
d) Writing reflective responses to Zoom chat prompts.
e) Working with peers in breakout groups and volunteering to report out group's findings to class.

The mode of instruction is hybrid. You can attend this class in person or via Zoom. Instructor will do the last

The University of Texas at Austin
Master of Science in Information Security and Privacy
School of Information and Center for Identity

class weekend via Zoom due to his role at an international conference (discussed and approved by MSISP Director in advance of the semester).

We will use Zoom records for taking attendance and assessing contributions. Thus, whether you attend in person or virtually, you are expected log on to your Zoom account and remain connected to Zoom throughout the session. We will run structured Zoom poll questions at certain points during class discussions. Please respond to them thoughtfully. Some poll questions will elicit opinions on open-ended questions for which there may not be any agreed upon perspective. Some poll questions will have a right/wrong answer based on facts in assigned readings and cases. We will selectively use the latter to distinguish if a student's responses to poll questions are thoughtful or random. We will discount random responses and reward thoughtful responses that increase the quality of class discussions. We will also ask reflective questions and expect you to type your responses in Zoom chat box. We will select some of the responses for further discussion.

20% of your grade for this class is based on your contributions to class discussions. Participating in class discussion does not necessarily mean talking a lot or showing everyone else that you know or have studied a lot. Good discussion participation involves people trying to build on, and synthesize, comments from others, and on showing appreciation for others' contributions. It also involves inviting others to say more about what they are thinking. Some of the most helpful things you can do are call for a quiet interlude, bring a new resource to the classroom, or post an observation in Zoom chat. So there are multiple ways quieter learners can participate. Below are some specific behavioral examples of good participation in discussion:

- Ask a question or make a comment that shows you are interested in what another person says
- Ask a question or make a comment that encourages another person to elaborate on something they have already said
- Bring in a resource (a reading, web link, video) not covered in the syllabus but adds new information/perspectives to our learning
- Make a comment that underscores the link between two people's contributions & make this link explicit in your comment
- Use body language (in only a slightly exaggerated way) to show interest in what different speakers are saying
- Post a comment on the Zoom chat box that summarizes our conversations so far and/or suggests new directions and questions to be explored in the future
- Make a comment (in chat box if this is appropriate) indicating that you found another person's ideas interesting or useful. Be specific as to why this was the case
- Contribute something that builds on, or springs from, what someone else has said. Be explicit about the way you are building on the other person's thoughts – this can be done online
- When you think it's appropriate, ask the group for a moment's silence to slow the pace of conversation to give you, and others, time to think
- Make a comment that at least partly paraphrases a point someone has already made
- Make a summary observation that takes into account several people's contributions & that touches on a recurring theme in the discussion (online if you like)
- Ask a cause and effect question - for example, "can you explain why you think it's true that if these things are in place such and such a thing will occur?"
- Find a way to express appreciation for the enlightenment you have gained from the discussion. Try to be specific about what it was that helped you understand something better. Again this can be done online if this suits you better.

Advanced preparation for class discussions is required to make substantive contributions to class discussions. You are expected to read, analyze, and think about the assigned reading articles, cases, and other lecture materials before coming to class.

INDIVIDUAL WRITE-UP ASSIGNMENTS (80%)

We will discuss a total of ten cases throughout the semester. You are required to submit 1-page case write-ups for all of them. You should analyze the cases yourself and develop your own unique answers to the write-up questions. Submissions that indicate that the author developed the answers in communication, cooperation, or collaboration with anyone else will be subject to the scholastic dishonesty policies of the University. You will have opportunities to collaboratively analyze and make sense of these cases during the class discussions. We

The University of Texas at Austin
Master of Science in Information Security and Privacy
School of Information and Center for Identity

will grade the individual case write-ups using the following criteria:

a) How well does the write-up utilize, apply and integrate relevant course concepts in analyzing the questions, developing and justifying answers, conclusions, and recommendations? 70% of case grading come from this criterion. Before writing up a case, please read the case, reflect on all course concepts covered to date, including the concepts covered in the reading assignments of the case write-up day, and decide which concepts would be most relevant to build on for developing your perspective on the case questions.

b) How well does the write-up utilize case facts and evidence in support of its decisions, conclusions, and recommendations? 30 % of case grading come from this criterion.

Format, submission, and grading guidelines are posted on Files\Case write-up guidelines section of Canvas. Case write-ups are due on Canvas by 1:00pm on the day of the case discussion. Canvas submission link will close at 1:00pm sharp. Submissions after the deadline will not be considered as the case will be discussed in class.

GRADE DROP POLICY: At the conclusion of the semester, we will automatically drop the lowest contribution score out of the contribution scores of the attended sessions. Likewise, we will drop the lowest case write-up score out of the submitted case write-ups. Zeros received for sessions missed without officially accepted excuses will not be eligible for drops. The purpose of the grade drop policy is to give students an opportunity to recover from poor performance in a required grade component due to something unexpected not covered by other course policies. Please plan to attend all sessions and submit all case write-ups to be eligible for the grade drop policy.

REGRADE REQUESTS: Request for regrading an assignment must be made in writing within one week of the graded assignment being made available to students in the class.

FINAL LETTER GRADES: Weighted average of the grade components will be used to assign final letter grades. The following table will be used to convert weighted grade averages to final letter grades. No rounding will be applied. The instructor reserves the right to adjust numeric ranges, provided all adjustments are made fairly and uniformly for the entire class and to the benefit of the students. For example, if the class average turns out to be lower than anticipated, instructor can choose to shift down the numeric ranges of letter grades to the benefit of the students.

Weighted Average of Grade Components	Letter Grade
95-100	A
90-94.99	A-
87-89.99	B+
84-86.99	B
80-83.99	B-
77-79.99	C+
74-76.99	C
70-73.99	C-
67-69.99	D+
64-66.99	D
60-63.99	D-
00-59.99	F

This course must be taken on a letter grade basis. Candidates for the master's degree must have a cumulative GPA of at least 3.00 in core courses. Per University policy, any graduate student whose cumulative grade point average falls below 3.00 at the end of any semester will be placed on scholastic warning status, and must bring their cumulative GPA to at least 3.00 during the next semester, or be subject to dismissal from the program. Official grade point averages are calculated by the UT Registrar and appear on the student's academic record maintained by the Registrar.

Learning and Growth: Your learning and growth in theory and practice of the information security and privacy profession and your success in this class are important to me. We will all need accommodations because we all learn differently. If there are aspects of this course that prevent you from learning or exclude you, please let me know as soon as possible. Together we'll develop strategies to meet both your needs and the requirements of the course. I also encourage you to reach out to the resources available through UT and MSISP program. Many are listed on this syllabus, but I am happy to connect you with a person or Center if you would like.

The University of Texas at Austin
Master of Science in Information Security and Privacy
School of Information and Center for Identity

COURSE OUTLINE

- **(HP):** Harvard Package (HP) contains electronic versions of Harvard Business School Articles and Cases that will be used in the course. You can purchase the HP at: https://hbsp.harvard.edu/import/1070832
- **(Canvas):** Article to be posted on Canvas
- **(S/D):** Session/Date
- **(LO):** Learning objective (see page 1 for details)

S/D	LO	Topic	Readings/Assignments
Session1 (8/25)	LO1, LO2.	**Board-level Oversight of Enterprise Cyber Risks** • NACD Framework: Board oversight of cyber risk • COSO Framework: Enterprise risk management	• (Canvas) Course syllabus • (Canvas) Cybersecurity disclosure benchmarking. E&Y 2018 • (Canvas). Uku, O. (2023). From Regulation To Resilience: The Role of Cybersecurity Experts On Public Company Boards. Forbes Technology Council. • (Canvas) Galligan, M.E. and Rau, K. (2016). "COSO in the Cyber Age" pp. 1-18.
		• Case write-up-1: Equifax	• (HP) Case: Srinivasan, S., Pitcher, Q., and Goldberg, J.S. (2019). "Data Breach at Equifax." Harvard Business School, pp. 1-28.
Session2 (8/26)	LO2, LO3.	**Enterprise Cyber Risk Management** • NIST Cybersecurity Framework	• (Canvas) A board's guide to the NIST Cybersecurity Framework (CSF) for better risk oversight. PwC. 2019. (Read this note for a brief introduction to NIST CSF). • (Canvas) NIST Cybersecurity Framework (This is the full version of the NIST CSF. Skim Section 2.1 and Appendix A for detailed controls).
		• Case write-up-2: PharmaCo	• (HP) Parent, M., Murray, G., Sandhu, S. (2020). PharmaCo. Ivey Publishing, W20218-PDF-ENG.
Session3 (9/22)	LO2, LO4.	**Enterprise IT Risk Management** • COBIT Framework • Disaster recovery and business continuity	• (Canvas) COBIT 4.1 (Read pp. 9-23 to learn about COBIT; Use this book as a reference book to look up specific IT controls). • (Canvas) Kozina, M. (2009). "COBIT - ITIL mapping for Business Process Continuity Management," Proceedings of the 20th Central European Conference on Information and Intelligent Systems, pp. 113-119. • (Canvas) Brunau, C. (2016). "Business Continuity Planning Essentials," pp. 1-8.
		• Case write-up-3: CareGroup	• (HP) McFarlan, F.W., and Austin, R.D. (2005). "CareGroup," Harvard Business School Case #: 9-303-097, Boston, MA.
Session4 (9/23)	LO2, LO5.	**Enterprise Privacy Risk Management** • AICPA GAPP Framework	• (Canvas) AICPA Generally Accepted Privacy Principles (GAPP) Framework, 2009. (Please see p.14 of the framework for a list of the 10 privacy principles. If you need more details on any principle, please look up the relevant section of the framework; also use this framework as a reference book on privacy governance and controls).
		• Case write-up-4: Sidewalk Labs	• (HP) John, L.K., Weiss, M.B., Kelley, J. (2018). "Sidewalk Labs: Privacy in a City Built from the Internet Up." 819024-PDF-ENG.

The University of Texas at Austin
Master of Science in Information Security and Privacy
School of Information and Center for Identity

S/D	LO	Topic	Readings/Assignments
Session5 (10/13)	LO2, LO6, LO7.	**IT Controls, IT Audits, and Compliance with Regulations** • IT General Control (ITGC) Audits • IT Application control Audits • System and Organization Control (SOC) audits	• (Canvas) GAIT for IT General Control Deficiency Assessment - An approach for evaluating ITGC deficiencies in Sarbanes-Oxley Section 404 assessments of internal controls over financial reporting. • (Canvas) GTAG-8: Auditing Application Controls. • Review the different types of "System and Organization Control (SOC)" audit reports and certifications at: https://tinyurl.com/c5dt3hae
		• Case write-up-5: Target	• (HP) Case: Srinivasan, S., Paine, L.S., Goyal, N. "Cyber Breach at Target." Harvard Business School, 117027-PDF-ENG. • (Canvas) Radichel, T. (2014). "Critical Controls that Could Have Prevented Target Breach," SANS Institute, pp.1-32.
Session6 (10/14)	LO8-LO10.	**Taming Illicit Activity and Trust Problems in Supply Chains** • Blockchain	• (Canvas). IBM. "What is blockchain technology?" https://www.ibm.com/topics/blockchain • Reuters. 2022. "Can blockchain offer solutions for cross-border trade and supply chain disruptions?"
		• Case write-up-6: Conflict Minerals	• (HP) Fagan, M., and Cushing, T. "Conflict Minerals: Influencing the Supply Chain for Public Purpose."
Session7 (11/10)	LO8-LO10.	**Robotic Process Automation, Process Mining, Artificial Intelligence (AI): Benefits, Risks, and Controls** • Robotic process automation (RPA) • Process mining • Artificial intelligence (AI)	• (HP) Li, X. and Liu, R. (2020). "Artificial Intelligence in Accounting." The University of Hong Kong case product #: HK1306-PDF-ENG. • (Canvas) Trevor-Wilson, C. and Tanriverdi, H. (2022). "Organizational mitigations for adversarial attacks on machine learning systems."
		• Case write-up-7: FireEye	• (HP) Miller, S.M., and Bhattacharya, L. (2021). "Cybesecurity at FireEye: Human+AI." SMU916-PDF-ENG.
Session8 (11/11)	LO8-LO10.	**Emerging privacy and ethical risks in AI** • Privacy breaches in AI • Bias in AI • Ethical development and use of AI	• (HP) Blackman, R. (2023). How to Avoid the Ethical Nightmares of Emerging Technology. • (Canvas) Ethical decision making frameworks https://tinyurl.com/2sjha85u • (Canvas) NIST Special Publication 1270, "Towards a Standard for Identifying and Managing Bias in Artificial Intelligence."
		• Case write-up-8: Ubiquitous Surveillance	• (HP) Gentile, M., Danks, D., and Harrell, M. (2022). Ubiquitous Surveillance (A). UV8530-PDF-ENG
Session9 (12/1)	LO1-LO10.	**IT failure risks in IT ecosystem of AI**	• (Canvas). Nolan, R., and McFarlan, W. (2005). "Building an IT Governance Committee."
		• Case write-up-9: Boeing 737 MAX	• (HP) Roberto, M.A. (2020). "Boeing 737 MAX: Company Culture and Product Failure." W82C83-PDF-ENG.

The University of Texas at Austin
Master of Science in Information Security and Privacy
School of Information and Center for Identity

S/D	LO	Topic	Readings/Assignments
Session10 (12/2)	LO8-LO10.	**Emerging cybersecurity risks in AI** • Cybersecurity breach risk in AI/ML • Adversarial attacks on AI/ML	• (Canvas) "Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It." Harvard Kennedy School, Belfer Center. (Skim this report and use it a reference book). • (Canvas) ENISA. (2021). "Securing Machine Learning Algorithms." • (Canvas) Trevor-Wilson, C. and Tanriverdi, H. (2022). "Organizational mitigations for adversarial attacks on machine learning systems."
		• Case write-up-10: Alexa	• (HP) Schulman, K.A., Wood, S. (2019). "Amazon Alexa and Patient Engagement." SM328-PDF-ENG.

COURSE POLICIES AND DISCLOSURES

ACADEMIC INTEGRITY EXPECTATIONS

Students who violate University rules on academic dishonesty are subject to disciplinary penalties, including the possibility of failure in the course and/or dismissal from the University. Since such dishonesty harms the individual, all students, and the integrity of the University, policies on academic dishonesty will be strictly enforced. For further information, please visit the Student Conduct and Academic Integrity website at: http://deanofstudents.utexas.edu/conduct.

CONFIDENTIALITY OF CLASS RECORDINGS

Class recordings are reserved only for students in this class for educational purposes and are protected under FERPA. The recordings should not be shared outside the class in any form. Violation of this restriction by a student could lead to Student Misconduct proceedings.

Getting Help with technology

Students needing help with technology in this course should contact the ITS Service Desk.

Content warning

Our classroom provides an open space for the critical and civil exchange of ideas. Some readings and other content in this course will include topics that some students may find offensive and/or traumatizing. I'll aim to forewarn students about potentially disturbing content and I ask all students to help to create an atmosphere of mutual respect and sensitivity.

Sharing of Course Materials is Prohibited

No materials used in this class, including, but not limited to, lecture hand-outs, videos, assessments (quizzes, exams, papers, projects, homework assignments), in-class materials, review sheets, and additional problem sets, may be shared online or with anyone outside of the class without explicit, written permission of the instructor. Unauthorized sharing of materials promotes cheating. The University is well aware of the sites used for sharing materials, and any materials found online that are associated with you, or any suspected unauthorized sharing of materials, will be reported to Student Conduct and Academic Integrity in the Office of the Dean of Students. These reports can result in sanctions, including failure of the course.

Religious Holy Days

By UT Austin policy, you must notify me of your pending absence as far in advance as possible of the date of observance of a religious holy day. If you must miss a class, an examination, a work assignment, or a project in order to observe a religious holy day, you will be given an opportunity to complete the missed work within a reasonable time after the absence.

The University of Texas at Austin
Master of Science in Information Security and Privacy
School of Information and Center for Identity

Absence for Military Service

In accordance with section 51.9111 of the Texas Education code and University policies on class attendance, a student is excused from attending classes or engaging in other required activities, including exams, if he or she is called to active military service of a reasonably brief duration. The maximum time for which the student may be excused has been defined by the Texas Higher Education Coordinating Board as ``no more than 25 percent of the total number of class meetings or the contact hour equivalent (not including the final examination period) for the specific course or courses in which the student is currently enrolled at the beginning of the period of active military service." The student will be allowed a reasonable time after the absence to complete assignments and take exams.

Land acknowledgment

I would like to acknowledge that we are meeting on the Indigenous lands of Turtle Island, the ancestral name for what now is called North America. Moreover, I would like to acknowledge the Alabama-Coushatta, Caddo, Carrizo/Comecrudo, Coahuiltecan, Comanche, Kickapoo, Lipan Apache, Tonkawa and Ysleta Del Sur Pueblo, and all the American Indian and Indigenous Peoples and communities who have been or have become a part of these lands and territories in Texas.

UT Zoom account

All students <u>must</u> use a UT Zoom account in order to participate in classes, office hours, and any UT affiliated events. For detailed instructions on how to sign up for a UT Zoom account, see Getting Started with Zoom. You will be denied access to Zoom sessions if you attempt to access without a valid UT account.

Joining a class or office hours in Zoom

The preferred method of joining a class or office hours is through Canvas. Students must log into their Canvas course site and click on Zoom on the left menu bar to locate links to join the class in Zoom in the calendar on Canvas. Zoom links for a class or office hours may also be emailed by the instructor. Regardless, students must use their UT Zoom account to participate. For more information, see How to Join Class or Office Hours.

Zoom professionalism and etiquette

Following are some best practices for making sure we are working together to create an efficient, effective, respectful, and ultimately enjoyable classroom when accessing remotely:

- Keep your video on at all times.
- Be mindful of your surroundings when on camera to minimize distractions.
- Avoid display of inappropriate materials or expressions, either visual, textual, or otherwise. Such displays may be subject to disciplinary action.
- Turn your camera off when leaving the meeting temporarily and use the away feedback icon.
- Include a professional photo of yourself for your Zoom profile picture. This photo will be visible during class sessions if you keep your video off.
- Mute yourself unless you are speaking. This will reduce background or feedback noise and limit distractions.
- Pose questions or comments using the "raise" your hand feature or typing in the chat window. Try to keep questions and comments brief, especially in large classes.
- Turn off your video if the video or audio is choppy. After the class or meeting, try these Internet Connection Tips.
- Use the most reliable WIFI you can access. If you are experiencing problems with your internet connection, here are some Internet Connection Tips.

For more information, please see Zoom Etiquette.

Classroom professionalism policy

The highest professional standards are expected of all members of the UT community. The collective class reputation and the value of the UT experience hinges on this. You should treat the UT classroom as you would a professional corporate environment. Faculty are expected to be professional and prepared to deliver value for every class session. Students are expected to be professional in all respects. The UT classroom experience is enhanced when:

- Students arrive on time. On-time arrival ensures that classes are able to start and finish at the scheduled

time. On-time arrival shows respect for both fellow students and faculty and it enhances learning by reducing avoidable distractions.

- Students display their name cards. This permits fellow students and faculty to learn names, enhancing opportunities for community building and evaluation of in-class contributions.
- Students are fully prepared for each class. Much of the learning in the UT program takes place during classroom discussions. When students are not prepared, they cannot contribute to the overall learning process. This affects not only the individual but their peers who count on them, as well.
- Students respect the views and opinions of their colleagues. Disagreement and debate are encouraged. Intolerance for the views of others is unacceptable.
- Students attend the class section to which they are registered. Learning is enhanced when class sizes are optimized. Limits are set to ensure a quality experience and safety.
- Technology is used to enhance the class experience. When students are surfing the web, responding to e-mail, instant messaging each other, and otherwise not devoting their full attention to the topic at hand, they are doing themselves and their peers a major disservice. Those around them face additional distractions. Fellow students cannot benefit from the insights of the students who are not engaged. Faculty office hours are spent going over class material with students who chose not to pay attention, rather than truly adding value by helping students who want a better understanding of the material or want to explore the issues in more depth. Students with real needs may not be able to obtain adequate help if faculty time is spent repeating what was said in class. There are often cases where learning is enhanced by the use of technology in class. Faculty will let you know when it is appropriate.
- Phones and wireless devices are turned off. We've all heard the annoying ringing in the middle of a meeting. Not only is it not professional, but it also cuts off the flow of discussion when the search for the offender begins. When a true need to communicate with someone outside of class exists (e.g., for some medical need) please inform the professor prior to class.

Diversity and inclusion

It is my intent that students from all diverse backgrounds and perspectives be well served by this course, that students' learning needs be addressed, and that the diversity that students bring to this class can be comfortably expressed and be viewed as a resource, strength and benefit to all students. Please come to me at any time with any concerns.

Names and pronouns

Professional courtesy and sensitivity are especially important with respect to individuals and topics dealing with differences of race, culture, religion, politics, sexual orientation, gender, gender variance, and nationalities. I will gladly honor your request to address you by your chosen name and by the gender pronouns you use. Class rosters are provided to the instructor with the student's chosen (not legal) name, if you have provided one. If you wish to provide or update a chosen name, that can be done easily at this page, and you can add your pronouns to Canvas.

Student rights & responsibilities

- You have a right to a learning environment that supports mental and physical wellness.
- You have a right to respect.
- You have a right to be assessed and graded fairly.
- You have a right to freedom of opinion and expression.
- You have a right to privacy and confidentiality.
- You have a right to meaningful and equal participation, to self-organize groups to improve your learning environment.
- You have a right to learn in an environment that is welcoming to all people. No student shall be isolated, excluded or diminished in any way.

With these rights come responsibilities:

- You are responsible for taking care of yourself, managing your time, and communicating with the teaching team and with others if things start to feel out of control or overwhelming.
- You are responsible for acting in a way that is worthy of respect and always respectful of others. • Your experience with this course is directly related to the quality of the energy that you bring to it, and your

The University of Texas at Austin
Master of Science in Information Security and Privacy
School of Information and Center for Identity

energy shapes the quality of your peers' experiences.
- You are responsible for creating an inclusive environment and for speaking up when someone is excluded.
- You are responsible for holding yourself accountable to these standards, holding each other to these standards, and holding the teaching team accountable as well.

UNIVERSITY RESOURCES FOR STUDENTS

SERVICES FOR STUDENTS WITH DISABILITIES (SSD)
The university is committed to creating an accessible and inclusive learning environment consistent with university policy and federal and state law. Please let me know if you experience any barriers to learning so I can work with you to ensure you have equal opportunity to participate fully in this course. If you are a student with a disability, or think you may have a disability, and need accommodations please contact Services for Students with Disabilities (SSD). Please refer to SSD's website for contact and more information: http://diversity.utexas.edu/disability/. If you are already registered with SSD, please deliver your Accommodation Letter to me as early as possible in the semester so we can discuss your approved accommodations and needs in this course.

COUNSELING AND MENTAL HEALTH CENTER (CMHC)
All of us benefit from support during times of struggle. Know you are not alone. If you or anyone you know is experiencing symptoms of stress, anxiety, depression, academic concerns, loneliness, difficulty sleeping, or any other concern impacting your wellbeing – you are strongly encouraged to connect with CMHC. The Counseling and Mental Health Center provides a wide variety of mental health services to all UT students including crisis services, counseling services with immediate support and well-being resources. Additionally, CARE Counselors are located within the academic schools and colleges. These counselors get to know the concerns that are unique to their college's students. For more information on CMHC, visit https://cmhc.utexas.edu or call 512-471-3515.

UNIVERSITY HEALTH SERVICES (UHS)
Your physical health and wellness are a priority. University Health Services is an on-campus high-quality medical facility providing care to all UT students. Services offered by UHS include general medicine, urgent care, a 24/7 nurse advice line, women's health, sports medicine, physical therapy, lab and radiology services, COVID-19 testing and vaccinations and much more. For additional information, visit https://healthyhorns.utexas.edu or call 512-471-4955.

SANGER LEARNING CENTER
Did you know that more than one-third of UT undergraduate students use the Sanger Learning Center each year to improve their academic performance? All students are welcome to take advantage of Sanger Center's classes and workshops, private learning specialist appointments, peer academic coaching, and tutoring for more than 70 courses in 15 different subject areas. For more information, please visit https://ugs.utexas.edu/slc or call 512-471-3614 (JES A332)."

STUDENT EMERGENCY SERVICES (SES)
Student Emergency Services in the Office of the Dean of Students helps students and their families during difficult or emergency situations. Assistance includes outreach, advocacy, intervention, support, and referrals to relevant campus and community resources. If you need to be absent from class due to a family emergency, medical or mental health concern, or academic difficulty due to crisis or an emergency situation, you can work with Student Emergency Services. SES will document your situation and notify your professors. Additional information is available at https://deanofstudents.utexas.edu/emergency/ or by calling 512-471-5017.

IMPORTANT SAFETY INFORMATION
If you have concerns about the safety or behavior of fellow students, TAs or professors, contact BCCAL (the Behavior Concerns and COVID-19 Advice Line) at https://safety.utexas.edu/behavior-concerns-advice-line or by calling 512-232-5050. Confidentiality will be maintained as much as possible, however the university may be required to release some information to appropriate parties.

CLASSROOM SAFETY AND COVID-19
To help preserve our in-person learning environment, the university recommends the following.

The University of Texas at Austin
Master of Science in Information Security and Privacy
School of Information and Center for Identity

- Adhere to university [mask guidance](). Masks are strongly recommended, but optional, inside university buildings for vaccinated and unvaccinated individuals, except when alone in a private office or single-occupant cubicle.
- [Vaccinations are widely available](), free and not billed to health insurance. The vaccine will help protect against the transmission of the virus to others and reduce serious symptoms in those who are vaccinated.
- [Proactive Community Testing]() remains an important part of the university's efforts to protect our community. Tests are fast and free.
- We encourage the use of the [Protect Texas App]() each day prior to coming to campus.
- If you develop COVID-19 symptoms or feel sick, stay home and contact the [University Health Services]()' Nurse Advice Line at 512-475-6877. If you need to be absent from class, contact [Student Emergency Services]() and they will notify your professors. In addition, to help understand what to do if you have been had close contact with someone who tested positive for COVID-19, see this [University Health Services link]().
- [Behavior Concerns and COVID-19 Advice Line]() (BCCAL) remains available as the primary tool to address questions or concerns from the university community about COVID-19.
- Students who test positive should contact [BCCAL]() or self-report (if tested off campus) to [University Health Services]().
- Visit [Protect Texas Together]() for more information.

CARRYING OF HANDGUNS ON CAMPUS

Texas' Open Carry law expressly prohibits a licensed to carry (LTC) holder from carrying a handgun openly on the campus of an institution of higher education such as UT Austin. Students in this class should be aware of the following university policies:

- Students in this class who hold a license to carry are asked to [review the university policy regarding campus carry]().
- Individuals who hold a license to carry are eligible to carry a concealed handgun on campus, including in most outdoor areas, buildings and spaces that are accessible to the public, and in classrooms.
- It is the responsibility of concealed-carry license holders to carry their handguns on or about their person at all times while on campus. Open carry is NOT permitted, meaning that a license holder may not carry a partially or wholly visible handgun on campus premises or on any university driveway, street, sidewalk or walkway, parking lot, parking garage, or other parking area.
- Per my right, I prohibit carrying of handguns in my personal office. Note that this information will also be conveyed to all students verbally during the first week of class. This written notice is intended to reinforce the verbal notification, and is not a "legally effective" means of notification in its own right.

TITLE IX DISCLOSURE

Beginning January 1, 2020, Texas Senate Bill 212 requires all employees of Texas universities, including faculty, to report any information to the Title IX Office regarding sexual harassment, sexual assault, dating violence and stalking that is disclosed to them. Texas law requires that all employees who witness or receive any information of this type (including, but not limited to, writing assignments, class discussions, or one-on-one conversations) must be report it. If you would like to speak with someone who can provide support or remedies without making an official report to the university, please email [advocate@austin.utexas.edu](). For more information about reporting options and resources, visit [http://www.titleix.utexas.edu/](), contact the Title IX Office via email at titleix@austin.utexas.edu, or call 512-471-0419. Although graduate teaching and research assistants are not subject to Texas Senate Bill 212, they are still mandatory reporters under Federal Title IX laws and are required to report a wide range of behaviors we refer to as sexual misconduct, including the types of sexual misconduct covered under Texas Senate Bill 212.The Title IX office has developed supportive ways to respond to a survivor and compiled campus resources to support survivors.

Faculty members and certain staff members are considered "Responsible Employees" or "Mandatory Reporters," which means that they are required to report violations of Title IX to the Title IX Coordinator. **I am a Responsible Employee and must report any Title IX-related incidents** that are disclosed in writing, discussion, or one-on-one. Before talking with me or with any faculty or staff member about a Title IX-related incident, be sure to ask whether they are a responsible employee. If you want to speak with someone for support or remedies without making an official report to the university, email [advocate@austin.utexas.edu]() For more information about reporting options and resources, visit the [Title IX Office]() or email [titleix@austin.utexas.edu]().

The University of Texas at Austin
Master of Science in Information Security and Privacy
School of Information and Center for Identity

CAMPUS SAFETY

The following are recommendations regarding emergency evacuation from the [Office of Campus Safety and Security](#), 512-471-5767,

- Students should sign up for Campus Emergency Text Alerts at the page linked above.
- Occupants of buildings on The University of Texas at Austin campus must evacuate buildings when a fire alarm is activated. Alarm activation or announcement requires exiting and assembling outside.
- Familiarize yourself with all exit doors of each classroom and building you may occupy. Remember that the nearest exit door may not be the one you used when entering the building.
- Students requiring assistance in evacuation shall inform their instructor in writing during the first week of class.
- In the event of an evacuation, follow the instruction of faculty or class instructors. Do not re-enter a building unless given instructions by the following: Austin Fire Department, The University of Texas at Austin Police Department, or Fire Prevention Services office.
- For more information, please visit [emergency preparedness](#).