**MSISP 385**

**Information Risk and Benefit Analysis, Fall 2022**

**Thompson Conference Center (TCC) Room 3.110**

**Instructional Mode: Hybrid**

# Instructors:

Hüseyin Tanriverdi (email: [Huseyin.Tanriverdi@mccombs.utexas.edu](mailto:Huseyin.Tanriverdi@mccombs.utexas.edu); phone: 512-232-9164)

Ashley Hunter (email: [Ashley@ahunterco.com](mailto:Ashley@ahunterco.com); phone: 512-827-9896)

Bruce Kellison (email: [bkellison@ic2.utexas.edu](mailto:bkellison@ic2.utexas.edu); phone: 512-475-7813), Lead Instructor

**Office Hours:**

Hüseyin Tanriverdi (By appointment)

Ashley Hunter (By appointment)

Bruce Kellison (T, W 4:00 – 5:30 pm or by appointment) Lead Instructor

**Office Location:**

Hüseyin Tanriverdi (CBA 5.208)

Ashley Hunter (IC2 Institute, 2815 San Gabriel, Rm 1.114)

Bruce Kellison (IC2 Institute, 2815 San Gabriel, Rm 1.114) Lead Instructor

# Teaching Assistant: TBD

Office Hours:

Office Location:

# Course Reading:

Required

Session 1 (August 26): Making the “business value” case for identity, privacy, and information-related investments

* **(Canvas)**. CyberArk Software. (2019). “The risk initiative: Cyber metrics for better decisions.”
* **(Canvas)**. Damodaran, A. (2020). Net Present Value (NPV) Analysis. “A Primer on the Time Value of Money.”
* **(Canvas)**. “Total cost of ownership (TCO) versus Return on investment (ROI): Which is Best for Making Investment Decisions?”
* **Assignment preview**: This session will preview the *HappyPay Case Assignment* which will be due in session 3 (9/23). Please read the PDF file and the Excel workbook for HappyPay case and do the prep work requested. HappyPay case assignment aims to give students hands-on experience with the quantification of business value of an identity, privacy, and information-related investment. The assignment has two parts. Part I is a non-graded intermediate deliverable, which is due by the first class session on August 26th. It is designed to familiarize you with the graded assignment and help you get started with it early on. Part I asks you to do some prep work on the assignment. The prep will help you absorb the concepts covered in the first class session and feel comfortable in doing the graded part of the assignment, i.e., Part II due on 9/23. Doing Part I without worrying about grade will also help you decide, by the first class session, whether you would prefer to do the graded part of the assignment on your own or with a group of 2-3 students. We will ask you to finalize this decision by the first class session (8/26) so we can know who wants to be on a group. We will also administer a survey on the first class day to assess skills of students and try to form groups whose members have complementary skills, to the extent feasible, with the number of students enrolled. Part II is the graded part of the assignment and it will be due by the third class session on September 23rd.

Session 2 (August 27) **Making the “public value” case for identity, privacy, and information security-related investments**

* **(Canvas).** Moore, M.H., and Khagram, S. (2004). “On creating public value: what business might learn from government about strategic management,” Corporate Social Responsibility Initiative Working Paper #3, Cambridge, MA: John F. Kennedy School of Government, Harvard University.
* **(Canvas)**. ISACA. (2010). "The Business case guide: using Val IT™ 2.0." (ISBN 978-1-60420-105-5)
* **(Canvas)**. ISACA (2007). “Val IT Case Study: Value Governance—Police Case Study”
* **Assignment preview:** This session will preview the *ShotSpotter Case Assignment* which will be due in session 4. Please read the details of this assignment and raise any questions in this session. Students who decide to do the HappyPay assignment with a group will also do the ShotSpotter case assignment with the same group.

Session 3 (September 23) **Application of business value justification concepts:**

* Students present their *HappyPay Case Assignment* solutions: the business value case for the IAM investment of HappyPay.
* Background materials for the *HappyPay Case Assignment*:
  + - **(Canvas)**. HappyPay Case - Part II (see both PDF file and Excel workbook)
    - **(Canvas)**. SailPoint (2016). How to Create a Business Case for Identity and Access Management.
* Discussion of presentations
* Discussion of strengths, weaknesses, and limitations of NPV, ROI, and TOC frameworks.

Session 4 (September 24): **Application of public value justification concepts:**

* Students present their solutions to the *ShotSpotter Case Assignment*: i.e., public value case for the ShotSpotter investment of Austin Police Department.
* Background materials for the *ShotSpotter Case Assignment*:
* **(Harvard)**. Weiss, M.B., and McAra, S. (2016). ShotSpotter. Harvard Business School Product #: 817034-PDF-ENG (purchase the case at: https://hbsp.harvard.edu/import/737681).
* **(Canvas)**. La Vigne, N.G., Thompson, P.S., Lawrence, D.S., Goff. M. (2019). “Implementing Gunshot Detection Technology Recommendations for Law Enforcement and Municipal Partners.”
* **Re-read from session-2: (Canvas)**. ISACA. (2010). "The Business case guide: using Val IT™ 2.0." (ISBN 978-1-60420-105-5)
* **Re-read from session-2: (Canvas)**. ISACA (2007). “Val IT Case Study: Value Governance—Police Case Study”
* Discussion of presentations
* Discussion of strengths, weaknesses, and limitations of the public value framework

Session 5 (October 21)

* 2022 Ponemon Institute: Keeper Report

Session 6 (October 22)

* 2022 Verizon: Data Breach Investigations Report

Session 7 (November 18)

* *The Steps CIOs Must Take To Deal With Ransomware Attacks Like The One That Hit Garmin* (2020, Forbes)

Session 8 (November 19)

* *What Is the Real Cost of a Data Breach? New Report Indicates It’s About $4 Million to $9 Million for SMEs* (2020, CPO Magazine)

Session 9 (December 9)

Selected chapters from L. Camp and M. Johnson (2012). *The Economics of Financial and Medical Identity Theft*

Session 10 (December 10)

Wehbé, “OPM Data Breach Case Study: Mitigating Personnel Security Risk” (2017)

Seeley, “Once More Unto the Breach: The Constitutional Right to Informational Privacy and the Privacy Act” (2016)

# Course Meeting Dates and Times:

|  |  |  |  |
| --- | --- | --- | --- |
| Weekend | Dates | Times | Zoom link |
| 1 | August 26-27 | 8am-12noon | To be posted on Canvas/Zoom folder |
| 2 | September 23-24 | 8am-12noon | To be posted on Canvas/Zoom folder |
| 3 | October 21-22 | 8am-12noon | To be posted on Canvas/Zoom folder |
| 4 | November 18-19 | 8am-12noon | To be posted on Canvas/Zoom folder |
| 5 | December 9-10 | 8am-12noon | To be posted on Canvas/Zoom folder |

# Course Overview:

Individuals, organizations, and societies invest in digital technologies, big data, and machine learning (ML) and artificial intelligence (AI) algorithms to obtain returns such as efficiency gains, innovations, growth, and profitability. Along with the returns, these technologies can also increase risks of organizations such as privacy risks, information security risks, and risks of unethical, irresponsible use of big data. The objective of this course is to equip students with skills and knowledge for estimating and managing the risks and benefits of these technologies. The course addresses risk/return issues at different levels of analysis such as individuals, organizations, society, and economy.

# Course Learning Goals:

By the end of sessions 1-4, students will learn how to make the business value and public value case for identity, privacy, and information security investments:

* How to make the “business value case” for privacy and information security investments of for-profit organizations
* How to make the “public value case” for privacy and information security investments of non-profit organizations
* How to establish an accountability framework for evaluating and justifying privacy and information security investments
* How to recognize and address the limitations of the existing business value and public value frameworks

By the end of sessions 5-8, students will:

* Have a working knowledge of liability forms available to emerging industries
* Understand the differences between traditional risk transfer and alternative risk models and how to apply those models based on the organization’s exposures
* Use reinsurance and financial models to determine underwriting premiums and rates

By the end of sessions 9 and 10, students will:

* Understand factors that affect national economic efficiency
* Be able to describe assumptions about private economics in a public economy
* Be able to outline national productivity gains from a functioning digital economy that depends on information security and privacy guardrails
* Understand national security implications of investments in information security related to:

1. Office of Personnel Management
2. Transnational/state-sponsored threats: terrorism, cyber war (N. Korea, China, Russia)
3. International gangs and organized crime syndicates (human trafficking, cyber attacks, Big Data)

* Be familiar with “internet of things” (algorithmic trading that depends on information security and privacy considerations; Second Machine Age and automation of cognitive tasks)

# Beyond this Course:

The MSISP curriculum prepares students to mitigate information security and privacy risks that threaten the achievement of an organization’s business value / public value objectives. Cybersecurity and privacy professionals compete for scarce investment resources of organizations to institute and operate mitigations for cybersecurity and privacy risks. Among the many investment proposals of different business units promising to improve profitability, growth, productivity, etc., why should decision makers fund an information security / privacy investment proposal? This course aims to equip students with skills to estimate risks and benefits of information security / privacy investments so that decision makers can clearly see the business value / public value of the investment and fund the proposal.

# Grading policy:

## Course Evaluations

**Sessions 1-4,** Making the business value and public value cases for privacy and information security investments

Assignment for Session-3 (September 23):

HappyPay Case Assignment, Part II (posted on Canvas). Due on Canvas by 12noon on September 23th.

Assignments for Section 4 (September 24):

ShotSpotter Case Assignment (posted on Canvas). Due on Canvas by 12noon on September 24th.

Assignments total value: 40%

Late-submission policy:There is no make-up for missing the assignments. A late submission is better than no submission at all. If you miss the submission deadline, a late submission within 7 days after the submission deadline will be accepted with a penalty. Since we will have discussed the assignments in class on the due dates, late submissions will have the benefit of that discussion, and hence, they will be subject to a late submission penalty of 20% reduction.

**Sessions 5-8**, “Financial Implications of Insuring Information Security Risk”

Using the information you have gained from our discussions and readings, each student will prepare an RFP (Request for Proposal) on behalf of your corporation (real or fictitious) for cyber insurance coverage. As the CIO, your RFP should include sufficient background information on the company to avoid potential gaps in cover from the insurance underwriter.

Assignment total value: 40%

Assignment Due Date: Nov. 21, 2022, 5:00 pm CST

Late assignment penalty: There is no make-up for missing the assignments. A late submission is better than no submission at all. If you miss the submission deadline, a late submission within 7 days after the submission deadline will be accepted with a penalty. Since we will have discussed the assignments in class on the due dates, late submissions will have the benefit of that discussion, and hence, they will be subject to a late submission penalty of 20% reduction.

**Sessions 9 and 10**, “Societal Impacts of Identity Assets”

Individual assignment: Create a hypothetical public organization, national in scope, and describe its role and function. Create identity assets for your organization. Describe how you value them, and why they should be protected. Describe your organization’s position vis-à-vis other federal agencies. Does it share information with other agencies? What identity protection investments should your organization make in the short, medium, and long term?

Assignment total value: 20%

Assignment Due Date: Dec. 13, 5:00 pm CST

Late assignment penalty: There is no make-up for missing the assignments. A late submission is better than no submission at all. If you miss the submission deadline, a late submission within 7 days after the submission deadline will be accepted with a penalty. Since we will have discussed the assignments in class on the due dates, late submissions will have the benefit of that discussion, and hence, they will be subject to a late submission penalty of 20% reduction.

**Final letter grades:** The weighted average of the grade components will be used to assign final letter grades. The following tables are 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, the instructor can choose to shift down the numeric ranges of letter grades.

|  |  |
| --- | --- |
| **Weighted average of grade components** | **Letter grade category** |
| 90-100 | A |
| 80-89.99 | B |
| 70-79.99 | C |
| 60-69.99 | D |
| 00-59.99 | F |

The instructor also reserves the right to use the +/- assignment of letter grades:

|  |  |
| --- | --- |
|  |  |
| 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 |

Attendance and participation in class are an important part of the success of our course and will be considered part of the course grade at the instructors’ discretion. Please understand the hybrid nature of the course means that we will make video recordings of our class sessions available on Canvas, watching video recordings are not a replacement for attendance.

## Excused Absences

Attendance is mandatory for all MSISP classes. 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. Only extraordinary, documented requests submitted at least 72 hours in advance of class time will be considered for absences. There must be a compelling reason for any requests not submitted 72 hours in advance of class start. Acceptance of excused absences will be considered by the faculty instructor in consultation with the MSISP Program Director.

# Schedule

|  |  |  |
| --- | --- | --- |
| Session # | Main Topic(s) | Instructor or Guest Lecturer |
| 1 (August 26) | **Making the “business value” case for identity, privacy, and cybersecurity related investments:**   * **(Canvas)**. CyberArk Software. (2019). “The risk initiative: Cyber metrics for better decisions.” * **(Canvas)**. Damodaran, A. (2020). Net Present Value (NPV) Analysis. “A Primer on the Time Value of Money.” * **(Canvas)**. “Total cost of ownership (TCO) versus Return on investment (ROI): Which is Best for Making Investment Decisions?” * **Assignment preview**: This session will preview the *HappyPay Case Assignment* which will be due in session 3. Please read the PDF file and the Excel workbook for HappyPay case and raise any questions about them in this session. | Hüseyin Tanriverdi |
| 2 (August 27) | **Making the “public value” case for identity, privacy, and security related investments**   * **(Canvas).** Moore, M.H., and Khagram, S. (2004). “On creating public value: what business might learn from government about strategic management,” Corporate Social Responsibility Initiative Working Paper #3, Cambridge, MA: John F. Kennedy School of Government, Harvard University. * **(Canvas)**. ISACA. (2010). "The Business case guide: using Val IT™ 2.0." (ISBN 978-1-60420-105-5) * **(Canvas)**. ISACA (2007). “Val IT Case Study: Value Governance—Police Case Study” * **Assignment preview:** This session will preview the *ShotSpotter Case Assignment* which will be due in session 4. Please read the details of this assignment and raise any questions in this session. | Hüseyin Tanriverdi |
| 3 (September 23) | **Application of business value justification concepts:**   * Students present their *HappyPay Case Assignment* solutions: the business value case for the IAM investment of HappyPay. * Background materials for the *HappyPay Case Assignment*:   + - **(Canvas)**. HappyPay Case - Part II (see both PDF file and Excel workbook).     - **(Canvas)**. SailPoint (2016). How to Create a Business Case for Identity and Access Management. * Discussion of presentations * Discussion of strengths, weaknesses, and limitations of NPV, ROI, and TOC frameworks. | Hüseyin Tanriverdi |
| 4 (September 24) | **Application of public value justification concepts:**   * Student teams present their solutions to the *ShotSpotter Case Assignment*: i.e., public value case for the ShotSpotter investment of Austin Police Department. * Background materials for the *ShotSpotter Case Assignment*: * **(Harvard)**. Weiss, M.B., and McAra, S. (2016). ShotSpotter. Harvard Business School Product #: 817034-PDF-ENG (purchase the case at: <https://hbsp.harvard.edu/import/737681>). * **(Canvas)**. La Vigne, N.G., Thompson, P.S., Lawrence, D.S., Goff. M. (2019). “Implementing Gunshot Detection Technology Recommendations for Law Enforcement and Municipal Partners.” * **Re-read from session-2: (Canvas).** Moore, M.H., and Khagram, S. (2004). “On creating public value: what business might learn from government about strategic management,” Corporate Social Responsibility Initiative Working Paper #3, Cambridge, MA: John F. Kennedy School of Government, Harvard University. * **Re-read from session-2: (Canvas)**. ISACA. (2010). "The Business case guide: using Val IT™ 2.0." (ISBN 978-1-60420-105-5). * **Re-read from session-2: (Canvas)**. ISACA (2007). “Val IT Case Study: Value Governance—Police Case Study”. * Discussion of presentations * Discussion of strengths, weaknesses, and limitations of the public value framework | Hüseyin Tanriverdi |
| 5 (Oct. 21) | **Fundamentals of Professional and General Liability Insurance**  **Professional Liability (Cyber and Technology Risk) Overview** | Ashley M. Hunter |
| 6 (Oct. 22) | **Financial Analysis**  **Professional Liability Reinsurance**  **Alternative Risk Markets**  **Privacy and Data Security Liability** | Ashley M. Hunter |
| 7 (Nov. 18) | **Privacy and Data Security Liability *(cont.)***  **Reinsurance**  **Insurer Financial Statements** | Ashley M. Hunter |
| 8 (Nov. 19) | **Interpreting Insurer Financial Statements**  **Insurer Financial Management**  **Insurer Strategic Management and Global Operations** | Ashley M. Hunter |
| 9 (Dec. 9) | **Elements of national macroeconomic efficiency**  **Assumptions about private economics in a public economy**  **National productivity gains and the digital economy**  Read before class: (Canvas) Camp & Johnson, Chs. 5 and 6; Ch. 10 | Bruce Kellison |
| 10 (Dec. 10) | **Issues of national security: IRS, OPM breaches**  **Issues of national security: State-sponsored threats**  **Issues of national security: international organized crime**  Read before class: (Canvas) Camp & Johnson, Ch. 11 and Closing; Wehbé, “OPM Data Breach Case Study: Mitigating Personnel Security Risk” (2017)  Seeley, “Once More Unto the Breach: The Constitutional Right to Informational Privacy and the Privacy Act” (2016) | Bruce Kellison |

# University of Texas and MSISP grading policies

## Examinations and Grades

The faculty instructors for each course will determine if exams are necessary as well as exam schedules and grading criteria if exams are included.

## Grading

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

Throughout the course, your learning and growth in theory and practice of the information security and privacy profession are important. We all need accommodations because we all learn differently, and the current pandemic makes accommodations all the more important. If there are aspects of this course that prevent you from learning or exclude you, please let Professor Kellison, as Lead Instructor, know as soon as possible. Together we will develop strategies to meet your needs and the course requirements. We also encourage you to reach out to the resources available through UT and the MSISP program. Many are included on this syllabus.

# Academic Integrity

Each student is expected to abide by the UT Honor Code: “As a student of The University of Texas at Austin, I shall abide by the core values of the University and uphold academic integrity.'' If you use words or ideas that are not your own (or that you have used in a previous class), you must cite your sources. Otherwise, you might be in violation of the university's academic integrity policies. Please see [Student Conduct and Academic Integrity](https://deanofstudents.utexas.edu/conduct/).

# Use of Electronics

To help you connect the pieces of the class together, please focus the use of electronics on the content in lecture and laboratory.

# Video Recordings

Video recording of class activities are reserved for students and TAs in this class only for educational purposes and are protected by [FERPA](https://registrar.utexas.edu/staff/ferpa) laws if any students are identifiable in the video. Video recordings should not be shared outside the class in any form. Students violating this university policy could face misconduct proceedings.

# Students with Disabilities

The university is committed to creating an accessible and inclusive learning environment consistent with university policy and federal and state law. Please let Professor Kellison 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](https://diversity.utexas.edu/disability/) (SSD). Here are some [examples](https://diversity.utexas.edu/disability/about-disabilities/) of the types of diagnoses and conditions that can be considered disabilities: [Attention-Deficit/Hyperactivity Disorders (ADHD)](https://diversity.utexas.edu/disability/adhd), [Autism](https://diversity.utexas.edu/disability/students-with-austism-spectrum-disorders/), [Blind & Visually Impaired](https://diversity.utexas.edu/disability/visual-impairments/), [Brain Injuries](https://diversity.utexas.edu/disability/traumatic-brain-injuries/), [Deaf & Hard of Hearing](https://diversity.utexas.edu/disability/deaf-and-hard-of-hearing/), [Learning Disabilities](https://diversity.utexas.edu/disability/learning-disabilities/), [Medical Disabilities](https://diversity.utexas.edu/disability/medical-disabilities/), [Physical Disabilities](https://diversity.utexas.edu/disability/physical-disabilities/), [Psychological Disabilities](https://diversity.utexas.edu/disability/psychological-disabilities-2/) and [Temporary Disabilities](https://diversity.utexas.edu/disability/temporary-disabilities/). Please refer to SSD's [website](https://diversity.utexas.edu/disability/) for contact and more information. If you are already registered with SSD, please deliver your Accommodation Letter to Professor Kellison as early as possible in the semester so we can discuss your approved accommodations and needs in this course.

# Mental Health Counseling

College can be stressful and sometimes we need a little help. Luckily, we have a wealth of resources and dedicated people ready to assist you, and treatment does work. The [Counseling and Mental Health Center](https://cmhc.utexas.edu/index.html) provides counseling, psychiatric, consultation, and prevention services that facilitate academic and life goals and enhance personal growth and well-being. Counselors are available Monday-Friday 8am-5pm by phone (512-471-3515) and Zoom.

If you are experiencing a mental health crisis (e.g. depression or anxiety), please call the Mental Health Center Crisis line at 512-471-CALL(2255). Call even if you aren't sure you're in a full-blown crisis, but sincerely need help. Staff are there to help you.

# Student Rights and 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 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 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.

# Official Correspondence

UT Austin [considers e-mail as an official mode of university correspondence](https://cio.utexas.edu/policies/university-electronic-mail-student-notification-policy). You are responsible for following course-related information on the course Canvas site.

# Religious Holy Days

In accordance with [section 51.911 of the Texas Education code](https://texas.public.law/statutes/tex._educ._code_section_51.911) and [University policies on class attendance](https://catalog.utexas.edu/general-information/academic-policies-and-procedures/attendance/), a student who misses classes or other required activities, including examinations, for the observance of a religious holy day should inform the instructor as far in advance of the absence as possible so that arrangements can be made to complete an assignment within a reasonable period after the absence. A reasonable accommodation does not include substantial modification to academic standards, or adjustments of requirements essential to any program of instruction. Students and instructors who have questions or concerns about academic accommodations for religious observance or religious beliefs may contact the [Office for Inclusion and Equity](https://equity.utexas.edu/). The University does not maintain a list of religious holy days.

# Absence for Military Service

In accordance with [section 51.9111 of the Texas Education code](https://texas.public.law/statutes/tex._educ._code_section_51.9111) and [University policies on class attendance](https://catalog.utexas.edu/general-information/academic-policies-and-procedures/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.

# COVID-19 Guidance

To help preserve our in-person learning environment, the university recommends the following.

* Adhere to university [mask guidance](https://healthyhorns.utexas.edu/images/pdf/ProtectiveFaceMaskGuidance_2020.pdf).

* [Vaccinations are widely available](https://healthyhorns.utexas.edu/coronavirus_vaccination.html), 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](https://healthyhorns.utexas.edu/coronavirus_proactive_testing.html) remains an important part of the university’s efforts to protect our community. Tests are fast and free.
* Visit [Protect Texas Together](http://protect.utexas.edu) for more information

# Safety Information (http://www.utexas.edu/safety)

If you have concerns about the safety or behavior of students, TAs, Professors, or others, call the Behavioral Concerns Advice Line at 512-232-5050. Your call can be anonymous. If something doesn't feel right, it probably isn't. Trust your instincts and share your concerns.

Occupants of buildings are required to 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. The nearest exit door may not be the one you used when entering the building.
* Students requiring assistance in evacuation shall inform the lead 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, UT Austin Police Department, or Fire Prevention Services.

* [Information regarding emergency evacuation routes and emergency procedures](http://www.utexas.edu/emergency).

# Sanger Learning Center

More students use the Sanger Learning Center each year to improve their academic performance. All students are welcome to join their classes and workshops and make appointments for their private learning specialists, peer academic coaches, and tutors. For more information, see the [Sanger Web site](http://www.utexas.edu/ugs/slc) or call 512-471-3614 (JES A332).

# Title IX Reporting

Title IX is a federal law that protects against sex and gender-based discrimination, sexual harassment, sexual assault, sexual misconduct, dating/domestic violence and stalking at federally funded educational institutions. UT Austin is committed to fostering a learning and working environment free from discrimination in all its forms where all students, faculty, and staff can learn, work, and thrive. When sexual misconduct occurs in our community, the university can:

1. Intervene to prevent harmful behavior from continuing or escalating.
2. Provide support and remedies to students and employees who have experienced harm or have become involved in a Title IX investigation.
3. Investigate and discipline violations of the university's relevant policies.

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 at UT Austin. All three of your course instructors are **Responsible Employees and must report any Title IX related incidents** that are disclosed in writing, discussion, or one-on-one. Before talking with us, 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](mailto:advocate@austin.utexas.edu). For more info about reporting options and resources, visit [the campus resources page](https://titleix.utexas.edu/campus-resources) or e-mail the Title IX Office at [titleix@austin.utexas.edu](mailto:titleix@austin.utexas.edu).

# Campus Carry

“The University of Texas at Austin is committed to providing a safe environment for students, employees, university affiliates, and visitors, and to respecting the right of individuals who are licensed to carry a handgun as permitted by Texas state law.” [More information](http://campuscarry.utexas.edu/students).