TEXAS A&M UNIVERSITY

Course Syllabus

Course Information

Course Number:	CSCE 402/702; CYBR 602
Course Title:	Cybersecurity Law & Policy
Section:	CSCE 402/500; CSCE 702/600/CYBR 602/600
Time:	T, TR 3:55 – 5:10 p.m.
Location:	ZACH 310
Credit Hours:	3

Instructor Details

Instructor:	Paula deWitte, J.D., Ph.D., P.E.
Office:	Peterson 225
Phone:	Preferred mode of communication is email.
E-Mail:	paula.dewitte@tamu.edu

If in reference to homework or exams, please copy the Senior Graders:

Stuart Nelson at s.s.nelson@tamu.edu

Lakhan Saiteja Kamireddy at lakhan@tamu.edu

Office Hours: Thursday 1 – 2 p.m. (in office) or by appointment (in office or by Zoom)

Course Description

This course examines law and policy issues related to cybersecurity for the spectrum of cybersecurity jobs including those defined in the NIST NICE Framework (procurement, operations/maintenance, governance and oversight, protection/defense, analysis, intelligence collection/operation; and investigation) cybersecurity jobs. Tomorrow's cyber workers are exposed to more data and privacy issues that requires them to analyze law, policies, and regulations both under United States jurisdiction and international jurisdiction (Spoiler Alert: *The internet has changed our traditional notion of jurisdiction!)*. Law is traceable and based on precedent while technology is disruptive. Law necessarily lags technology resulting in an uncertain legal and ethical framework which requires cyber workers to be able to analyze and distinguish appropriate courses of action as part of their daily tasks without the luxury of relying on legal counsel. This is especially crucial given the dynamics of the threat and response landscape, The course will focus on international and federal law and not specific state data breach laws other than a cursory review and explanation of when states or federal has jurisdiction.

The course first examines the fundamentals and basics of law – jurisdiction, due diligence, case/controversy, standing, statute of limitations, remedies/damages, and evidence standards – to establish a foundation to apply and analyze legal issues that are especially problematic regarding cybersecurity. The course then explores the national and international legal frameworks that govern cybersecurity and their implications for attacks, motives, responses, and counter-attacks through the lens of what is permissible against attacking individuals or entities versus attacking nation-states including legal issues such as "hacking back" and problems such as accurate attack attribution. The course then examines the legal issues raised by the cloud related to privacy and third parties including emerging standards. The overarching goal of this course is to provide a cyber-worker in technical, business or policy domains with the knowledge and skills to better interpret threats and responses in a national and international law framework while understanding (and being sympathetic to) the limits of the current law and how law/policy can evolve for cybersecurity. This course is not intended to make you lawyers, but rather legal-savvy cyber workers.

The course includes current events discussion on relevant information and relies on extensive analysis of laws and policies whereby students will demonstrate their knowledge and skills by preparing short written assignments throughout the semester.

Course Prerequisites

Junior, senior, or graduate classification. Preferred to have some programming experience although not required.

Special Course Designation

This is a stacked course. All assignments and exams for undergraduate and graduate students are weighted differently as explained in the Grading Policy section below with all sections having the same assignments and exams.

Course Learning Outcomes

Upon successful completion of this course, a student will be able to:

- Acquire the common body of knowledge for cybersecurity law including concepts and legal terminology.
- Acquire the common body of knowledge related to both national and international laws related to cybersecurity and the differences between United States law and laws of other jurisdictions.
- Identify and explain common legal issues related to cybersecurity.
- Provide a high-level explanation of the legal issues governing the authorized conduct of cyber operations and the use of related tools, techniques, technology, and data.
- Apply legal concepts in issues related to cybersecurity including cases/controversies unique to cybersecurity.
- Assess and explain legal procedural requirements relevant to cybersecurity.
- Demonstrate the ability to use legal knowledge by analyzing cybersecurity issues from a cyber worker perspective such as whether a security incident violates a privacy principle or legal standard requiring specific legal action.

- Demonstrate the ability to work through a case study identifying legal issues, analyzing the cybersecurity action required, and formulating a plan that complies with applicable laws.
- Identify the authorities applicable to a cyber-security operations scenario.
- Evaluate the relationship between ethics and law, describe civil disobedience and its relation to ethical hacking, describe criminal penalties related to unethical hacking, and apply the notion of "grey areas" to describing situations where law has not yet caught up to technological innovation.
- Describe steps for carrying out ethical penetration testing, describe 'ethical hacking' principles and conditions, distinguish between ethical and unethical hacking, and distinguish between nuisance hacking, activist hacking, criminal hacking, and acts of war.

Textbook and/or Resource Materials

Required Text

- Cybersecurity Law, 2nd Edition by Jeff Kosseff, ISBN-13: 978-1119517207

We will read all chapters (1 – 11) and selected Appendices as references.
I recommend that you buy this book!

Referenced Texts:

- Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations by Michael N. Schmitt, ISBN 978-1-316-82252-4. **I do not recommend that you buy this book!**
- You'll see this message when it is too late by Josephine Wolff, ISBN 978-0-262—3885-0.
- Twenty-six Words that Created the Internet by Jeff Kosseff, ISBN-10: 1501714414.
- This is How They Tell Me the World Ends by Nicole Perlroth, ISBN-10 : 1635576059.
- Other readings as assigned and either placed on Google Scholar or communicated with web references.

Grading Policy

The student's semester grade will be based on assignments, exams, and a semester paper.

Weekly/Bi-Weekly Assignments (5): There will be a total of 5 writing assignment. The topics for these assignments can be found in the course schedule. Each assignment should be answered in 1-2 pages according to the template posted on the GOOGLE SCHOLAR Learning Management System for this class.

Semester Paper: Students **should** select a topic to write for this paper before the fifth week of class. The requirements for the paper and the rubric for grading will be posted on the GOOGLE SCHOLAR Learning Management System for this class.

Exams: Two major exams will be given in this course at five and ten weeks during the course. Both exams will be essay tests. A final exam will be short answer and cover material from the last lectures.

Course grades will be assigned using the following scale:

Requirement:	Undergraduate Points	Graduate Points
Weekly/Bi-Weekly Assignments (5 assignments each worth 50pts for undergraduate students and 40 points for graduate students)	250 (25%)	200 (20%)
Semester Paper	250 (25%)	300 (30%)
First Exam	200 (20%)	200 (20%)
Second Exam	200 (20%)	200 (20%)
Third Exam	100 (10%)	100 (10%)
Total	1000 (100%)	1000 (100%)

***Points Grading Scale**:* *Out of 1000* assignable points	
A	900 - 1000 points
B	800 - 899 points
C	700 - 799 points
D	600 - 699 points
F	< 600 points

Assignments Rubric

The rubric for the assignment is based on IRAC: Issue + Rule + Analysis + Conclusion

20%	**Issue**: Did you come up with a relevant legal issue related to the course, and did you tie that issue to the course? Did you explain the problem/issue clearly? (If you fail to describe an issue, it will be difficult to analyze.)
20%	**Rule**: What makes this a relevant legal issue? What rules of law are you applying? Did you do a thorough research, that is clearly communicated?
20%	**Analysis**: You do not merely re-state the rule and research, but analyze what is leading to your subsequent conclusion. Tie your analysis to course knowledge to demonstrate what you learned from this course. This is also a good time to bring up any voids or gaps in current laws or to differentiate legal and ethical issues.
20%	**Conclusions:** Clearly state the conclusions based on the issue, rule, and analysis and ensure that there is a logical pathway to follow.
20%	**Presentation**: formatting, proper grammar, correct spelling, proper use of words, proper capitalization (e.g., Congress referring to the United States Congress is always capitalized as is the First Amendment. These are proper nouns.).

Semester Paper Rubric

The rubric for the semester paper is:

20%	**Idea selection and explanation**: Did you come up with a good idea for the course, and did you tie that idea to the course? Did you explain the problem/issue?
20%	**Research process**: Did you do good research, and is it clearly shown?
20%	**Analysis**: You do not merely re-state the research. You apply analysis and tie it to course knowledge to demonstrate what you learned from this course.
20%	**Presentation**: formatting, proper grammar, correct spelling, proper use of words, proper capitalization (e.g., Congress referring to the United States Congress is always capitalized as is the First Amendment. These are proper nouns.).
20%	**Style**: How well does this paper read? How well do you organize your ideas? How well do you reach logical conclusions based on your own arguments? Is the paper substantial?

- **Semester Paper Requirements:**
  - **Page Requirement**:
    - Undergraduate 5 - 7 Pages (Note: 5 complete pages are required. Not 4 and a half pages); Five pages of content excluding sources
    - Graduate 7 – 8 Pages (Note: 7 complete pages are required. Not 6 and a half pages);
  - **Margins**: 1" on all sides
  - **Line Spacing**: 1.5
  - **Font**: Calibri 11 Preferred; no bigger than 12 point font
  - **References Required**: Minimum of 10 valid references

Late Work Policy

Late work is work that is not turned in according to the class process by the assigned due date. The instructor may accept late work if the student notifies the instructor BEFORE the assigned due date except In truly emergency situations.

Typically, late and/or make-up work will not be accepted without a university excused absence. (See Student Rule 7.) If an absence is excused, then the student will be provided an opportunity to make up any homework assignments, quizzes, exams, or other work that contributes to the final grade with a due date that extends the original due date by the number of days of the excused absence. Individual arrangements will be made for exams and quizzes missed due to an excused absence. In all cases, TAMU Student Rule 7 will govern the process.

Course Schedule

Date	Topics	Assignment Milestones
Week 1 **Jan 18 - 20**	Introduction to Course & Expectations. Walk-through course syllabus. Discussion of Semester Paper. Using on-line resources and finding relevant current events. Differences between engineering and legal mindsets (*"It depends.")*. Basic cybersecurity terminology and concepts. (1st Lecture) **Overview of the American legal system** Legal concepts: Due diligence, Jurisdiction, Standing; Venue; Case/Controversy, Statute of Limitations; Evidence Standards (Civil vs Criminal); Remedies/Damages; "Reasonableness standards," etc. Other American legal concepts: Right to face accuser, double jeopardy, the role of "public policy" in court decisions, etc. **Legal Infrastructure:** State and federal laws. Federal executive, legislative, and judicial branches. Appellate review process—federal and state (or how a federal law can be interpreted differently within different areas of the US). *Whew! And that's just week 1! How fun was that!*	**Reading Kosseff Chapter 1 this week is essential. The remaining reading can be in the next few weeks. Don't be overwhelmed! This is background material (but – *it's so interesting!*).** **Read Kosseff Chapter 1: Data Security Laws and Enforcement Actions (skip Section 3.1 pp 48 - 56);** don't worry about specific case names and descriptions; focus on "Key Lessons" and look for the commonality in those key lessons for class discussion. **Appendix A: Section 5 of the FTC Act** Focus specifically on legal terminology and concepts as discussed in class. **Read SANS Paper: OPM vs. APT: How Proper Implementation of Key Controls Could Have Prevented a Disaster** (on GOOGLE SCHOLAR). Periodically through the semester, we'll refer to this SANS paper. As your legal analysis knowledge grows, you will realize how much you have learned using this paper as your guide. Your first read will probably be overwhelming. Your last read of the semester will be – *I know that!* Read **US Constitution (Articles I, II, III, IV, and VI).** http://constitutionus.com/ and https://www.law.cornell.edu/constitution Read **Federal Courts** and what they do: https://www.fjc.gov/content/federal-courts-and-what-they-do-2 **At the end of Week 1, you may not be able to recall all concepts and terminology from memory, however you should be able to analyze how and where to find the answer! We will refer to this as our framework of legal analysis that we will use through the rest of the course.** **And remember – first step -- always check to see if a term has a legal definition!**

Week 2 **Jan 25 - 27**	Continuation of Legal Terminology and Concepts from Week 1 Common law (state) civil causes of action: Contract breach; breach of implied warranty; negligence; unjust enrichment; fraud; slander; invasion of privacy. Privileges: Attorney-client, Work Product Doctrine, and Non-testifying Expert … *in anticipation of litigation* **The concept of "standing" – Article III of the Constitution and SCOTUS interpretation** Fun facts: Google the cases in the footnotes regarding standing on pages 52 – 53, especially Whitmore v. Arkansas for the type of case/controversy. ***Whoa! Did not see that coming!!!!*** Putting it all together to bring a cybersecurity case to court—walk-thru the legal process—both civil and criminal. (Free legal advice: *Never ever ignore when served by a court of competent jurisdiction. Never. Ever.*).	**Read Kosseff Chapter 2: Cybersecurity Litigation and** **We will emphasize the legal concept of standing and how lack of standing affects cybersecurity cases.** **We will not discuss specific state consumer protection or data breach laws.** **Assignment 1: Write a one-to-two page paper on a fundamental legal issue as being confusing/critical to cybersecurity.** **Due in one week. Submit through GOOGLE SCHOLAR.** **5% of course grade for undergraduate students and 4% of course grade for graduate students.**
Week 3 **Feb 1 - 3**	**Privacy ("*The right to be let alone*"):** Is there a "right" to privacy? If so, how do we define privacy so that we can effectively legislate protecting that right? **Legislative:**	**Read Kosseff Chapter 7: Surveillance and Cyber and Appendix E: Electronic Communications Privacy Act** **Read Kosseff Chapter 9: Privacy Laws** **Read Kosseff Chapter 10 (Section 10.1, pages 386 – 396)**

	The Privacy Act (1974); The Stored Communications Act (1986) The Wiretap Act (Title III of the Omnibus Crime Control and Safe Streets ***Act*** of 1968) The Electronic Communications Privacy Act (1986)—amendment to the Wiretap Act **Judicial:** SCOTUS opinions on privacy (Griswold v. Connecticut, Roe v Wade, Lawrence v. Texas), expectation of privacy (Katz v. United States), recent decisions strengthening 4th Amendment protections (Carpenter v United States). **4th Amendment**: Review of SCOTUS decisions on the requirements for Fourth Amendment Warrants. *What's next after Carpenter v United States?* **14th Amendment:** Review of Scotus decisions on due process.	US Constitution Amendments 1, 3, 4, and 5 Assigned readings on Google Scholar **Shocker: NYT article on Google Scholar: "Roe v. Wade Was About More Than Abortion" [Note this statement from the article:** "The answer is that Roe's definition of privacy seemed different. More than other Supreme Court decisions, it connected privacy to ideas about individual identity and choice." … and then how this definition of privacy has been used in subsequent legal actions.]
Week 4 **Feb 8 - 10**	**Federal Laws on Hacking Back:** Computer Fraud Abuse Act -- CFAA (1986) and proposed revisions; effect on hacking back Digital Millennium Copyright Act (1998).	**Read Kosseff Chapter 5: Anti-Hacking Laws and** **Appendix C: Section 1201 of the Digital Millennium Copyright Act (DMCA) and** **Appendix D: Computer Fraud and Abuse Act** Assigned paper(s) on "hacking back;" Read: 2018 National Cyber Strategy https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf and the companion document: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

		and the Solarium Report either the Executive Summary (22 pages) or the report (182 pages) **Assignment 2: Research the legal issues of privacy related to cybersecurity and write a one-to-two page paper discussing some legal issue.** **Due in one week. Submit through GOOGLE SCHOLAR.** **5% of course grade for undergraduate students and 4% of course grade for graduate students.**
Week 5 **Feb 15 – 17**	**US Federal Cybersecurity Laws:** **Legislative:** FISMA (Federal Information Security Management Act) and how it relates to common law recognition of NIST Standards and FIPS 199 and FIPS 200 NIST Standards in a Legal Sense: Documentation and how applying good cybersecurity practices may cause legal risk! **[Note: NIST is NOT a federal regulatory agency.]** **Executive:** (1) Presidential Directives and Introduction to Executive Orders. (2) Executive agencies (e.g., FTC). (3) Federal agencies—later lecture. **Judicial:** Common law. **Take-home Exam 1!**	**Read Kosseff Chapter 8: Cybersecurity and Federal Government Contractors** **Readings as assigned. Obviously one excellent source is https://csrc.nist.gov/publications/sp800 (as discussed and navigated in class).** **Review SANS paper on OPM regarding NIST controls** **Should have selected a topic for a semester paper by this week.**
Week 6 **Feb 22 - 24**	Cybersecurity and the Cloud: FEDRAMP Catch up week – this is our first semester "breather" week to either catch up (if we're behind) and/or to take time to fully	**Readings as assigned. Obviously one excellent source is www.fedramp.gov.** **Assignment 3: Write a one-to-two page paper on a specific NIST family of controls (pick out one or two controls) and think through any legal issues that should be considered. This is where the OPM paper might provide some ideas.**

	digest information so far. At least one lecture will be devoted to "Point/Counterpoint" classroom discussion where students will be given positions and argue whether to defend or reject. More fun if your assigned position is counter to your personal beliefs.	**Due in one week.** **Due in one week. Submit through GOOGLE SCHOLAR. 5% of course grade for undergraduate students and 4% of course grade for graduate students.**
Week 7 **Mar 1 - 3**	Scope and effect of federal regulations and how enforced. Regulatory Agencies (FTC, FCC, SEC, CFPB, DHS, Department of Education; other financial/banking regulations) relative to cybersecurity and/or privacy.	**Kosseff Chapter 3 (skip Section 3.7 pp 147 – 154) Cybersecurity Requirements for Specific Industries**; **Kosseff Chapter 4 Cybersecurity and Corporate Governance**
Week 8 **Mar 8 – 10**	**International Law:** Tallinn Manual 2.0 on International Law on Cyber Operations: Sovereignty Due diligence Jurisdiction United Nations Charter (Jus ad bellum) Hague Conventions & Geneva Conventions (Jus in bello)	**Read Kosseff Chapter 10: International Cybersecurity Laws and Chapter 11: Cyber and the Law of War** **Read Chapters 1, 2, & 3 of the Tallinn Manual: Sovereignty, Due Diligence, and Jurisdiction** **Skim through Table of Contents and organization of Tallinn Manual** **PLEASE DO NOT CONFUSE THE TALLINN MANUAL 2.0 AS ACTUAL BINDING INTERNATIONAL LAW!!!!!**
Mar 14 – 18	**Spring Break!**	
Week 9 **Mar 22 -24**	**Posse comitatus** **Other federal laws of interest.**	**Read Kosseff 6.4 Military Involvement in Cybersecurity and Posse Comitatus**
Week 10 **Mar 29 - 31**	**Take-home Exam #2!**	

Week 11 **Apr 5 - 7**	**Critical Infrastructure as a cybersecurity threat.** **Executive:** Presidential Directives and Executive Orders related to Securing Critical Infrastructure and the United States Patriot Act. **Legislative:** The *Cybersecurity Information Sharing Act* -- CISA (2015), Cybersecurity Enhancement Act (2014); NIST Cybersecurity Framework	**Read Kosseff Chapter 6: U.S. Government Cyber Structure and Public-Private Partnerships** **Assignment 4: Research a legal issue related to protecting critical infrastructure from one of the critical infrastructure sectors and write a one-to-two page paper Due in one week.** **Due in one week. Submit through GOOGLE SCHOLAR.** **5% of course grade for undergraduate students and 4% of course grade for graduate students.**
Week 12 **Apr 12 - 14**	**Intellectual Property Theft as a Cyber Threat** **Legislative:** Economic Espionage Act (1996) **Uniform Trade Secrets Act --** UTSA (1985)	**Assigned readings.**
Week 13 **Apr 19 - 21**	**Cyber Ethics: What's right, what's wrong, what's legal, and what's ethical.** **New and emerging issues in cybersecurity law & policy since class started.**	**Semester papers due! – 25% of course grade for CSCE 402 & MARA 403, 35% for CSCE 702.** **Assignment 5: Summarize and write a one-to-two page paper on your assessment of the current state of ethics in cybersecurity – think through the Tallinn Manual, hacking back, CFAA, etc. and class discussions. Potential topics could include some aspect that causes controversy or conflict with US law.** **Due in one week. Submit through GOOGLE SCHOLAR.** **5% of course grade for undergraduate students and 4% of course grade for graduate students.**
Week 14 **Apr 26 - 28**	**In class Exam #3.** **Course Evaluations; Wrap-Up.**	

Attendance Policy

The university views class attendance and participation as an individual student responsibility. Students are expected to attend class and to complete all assignments.

Please refer to Student Rule 7 in its entirety for information about excused absences, including definitions, and related documentation and timelines.

Makeup Work Policy

Students will be excused from attending class on the day of a graded activity or when attendance contributes to a student's grade, for the reasons stated in Student Rule 7, or other reason deemed appropriate by the instructor.

Please refer to Student Rule 7 in its entirety for information about makeup work, including definitions, and related documentation and timelines.

Absences related to Title IX of the Education Amendments of 1972 may necessitate a period of more than 30 days for make-up work, and the timeframe for make-up work should be agreed upon by the student and instructor" (Student Rule 7, Section 7.4.1).

"The instructor is under no obligation to provide an opportunity for the student to make up work missed because of an unexcused absence" (Student Rule 7, Section 7.4.2).

Students who request an excused absence are expected to uphold the Aggie Honor Code and Student Conduct Code. (See Student Rule 24.)

Academic Integrity Statement and Policy

"An Aggie does not lie, cheat or steal, or tolerate those who do."

"Texas A&M University students are responsible for authenticating all work submitted to an instructor. If asked, students must be able to produce proof that the item submitted is indeed the work of that student. Students must keep appropriate records at all times. The inability to authenticate one's work, should the instructor request it, may be sufficient grounds to initiate an academic misconduct case" (Section 20.1.2.3, Student Rule 20).

You can learn more about the Aggie Honor System Office Rules and Procedures, academic integrity, and your rights and responsibilities at aggiehonor.tamu.edu.

***NOTE**: Faculty associated with the main campus in College Station should use this Academic Integrity Statement and Policy. Faculty not on the main campus should use the appropriate language and location at their site.*

Americans with Disabilities Act (ADA) Policy

Texas A&M University is committed to providing equitable access to learning opportunities for all students. If you experience barriers to your education due to a disability or think you may have a disability, please contact Disability Resources in the Student Services Building or at (979) 845-1637 or visit disability.tamu.edu. Disabilities may include, but are not limited to attentional, learning, mental health, sensory, physical, or chronic health conditions. All students are encouraged to discuss their disability related needs with Disability Resources and their instructors as soon as possible.

***NOTE**: Faculty associated with the main campus in College Station should use this Americans with Disabilities Act Policy statement. Faculty not on the main campus should use the appropriate language and location at their site.*

Title IX and Statement on Limits to Confidentiality

Texas A&M University is committed to fostering a learning environment that is safe and productive for all. University policies and federal and state laws prohibit gender-based discrimination and sexual harassment, including sexual assault, sexual exploitation, domestic violence, dating violence, and stalking.

With the exception of some medical and mental health providers, all university employees (including full and part-time faculty, staff, paid graduate assistants, student workers, etc.) are Mandatory Reporters and must report to the Title IX Office if the employee experiences, observes, or becomes aware of an incident that meets the following conditions (see University Rule 08.01.01.M1):

- The incident is reasonably believed to be discrimination or harassment.
- The incident is alleged to have been committed by or against a person who, at the time of the incident, was (1) a student enrolled at the University or (2) an employee of the University.

Mandatory Reporters must file a report regardless of how the information comes to their attention – including but not limited to face-to-face conversations, a written In-Class Work or paper, class discussion, email, text, or social media post. Although Mandatory Reporters must file a report, in most instances, you will be able to control how the report is handled, including whether or not to pursue a formal investigation. The University's goal is to make sure you are aware of the range of options available to you and to ensure access to the resources you need.

Students wishing to discuss concerns in a confidential setting are encouraged to make an appointment with Counseling and Psychological Services (CAPS).

Students can learn more about filing a report, accessing supportive resources, and navigating the Title IX investigation and resolution process on the University's Title IX webpage.

***NOTE**: Faculty associated with the main campus in College Station should use this Title IX and Statement on Limits of Liability. Faculty not on the main campus should use the appropriate language and location at their site.*

Statement on Mental Health and Wellness

Texas A&M University recognizes that mental health and wellness are critical factors that influence a student's academic success and overall wellbeing. Students are encouraged to engage in proper self-care by utilizing the resources and services available from Counseling & Psychological Services (CAPS). Students who need someone to talk to can call the TAMU Helpline (979-845-2700) from 4:00 p.m. to 8:00 a.m. weekdays and 24 hours on weekends. 24-hour emergency help is also available through the National Suicide Prevention Hotline (800-273-8255) or at suicidepreventionlifeline.org.

COVID-19 Temporary Amendment to Minimum Syllabus Requirements

Campus Safety Measures

To promote public safety and protect students, faculty, and staff during the coronavirus pandemic, Texas A&M University has adopted policies and practices for the Spring 2021 academic term to limit virus transmission. Students must observe the following practices while participating in face-to-face courses and course-related activities (office hours, help sessions, transitioning to and between classes, study spaces, academic services, etc.):

- Self-monitoring—Students should follow CDC recommendations for self-monitoring. **Students who have a fever or exhibit symptoms of COVID-19 should participate in class remotely and should not participate in face-to-face instruction.**
- Face Coverings—Face coverings (cloth face covering, surgical mask, etc.) must be properly worn in all non-private spaces including classrooms, teaching laboratories, common spaces such as lobbies and hallways, public study spaces, libraries, academic resource and support offices, and outdoor spaces where 6 feet of physical distancing is difficult to reliably maintain. Description of face coverings and additional guidance are provided in the Face Covering policy and Frequently Asked Questions (FAQ) available on the Provost website.
- Physical Distancing—Physical distancing must be maintained between students, instructors, andothers in course and course-related activities.
- Classroom Ingress/Egress—Students must follow marked pathways for entering and exiting classrooms and other teaching spaces. Leave classrooms promptly after course activities have concluded. Do not congregate in hallways and maintain 6-foot physical distancing when waiting to enter classrooms and other instructional spaces.
- To attend a face-to-face class, students must wear a face covering (or a face shield if they have an exemption letter). If a student refuses to wear a face covering, the instructor should ask the student to leave and join the class remotely. If the student does not leave the class, the faculty member should report that student to the Student Conduct office for sanctions. Additionally, the faculty member may choose to teach that day's class remotely for all students.

Personal Illness and Quarantine

Students required to quarantine must participate in courses and course-related activities remotely and **must not attend face-to-face course activities**. Students should notify their instructors of the quarantine requirement. Students under quarantine are expected to participate in courses and complete graded work unless they have symptoms that are too severe to participate in course activities.

Absences will be excused only if the absence due to COVID (or other medical conditions) complies with university regulations.

Students experiencing personal injury or Illness that is too severe for the student to attend class qualify for an excused absence (See Student Rule 7, Section 7.2.2.) To receive an excused absence, students must comply with the documentation and notification guidelines outlined in Student Rule 7. While Student Rule 7, Section 7.3.2.1, indicates a medical confirmation note from the student's medical provider is preferred,