GBAA/R 5330: Cybersecurity Strategy

Rio Grande College of Business

Semester Year (Fall 2025)

Faculty Information

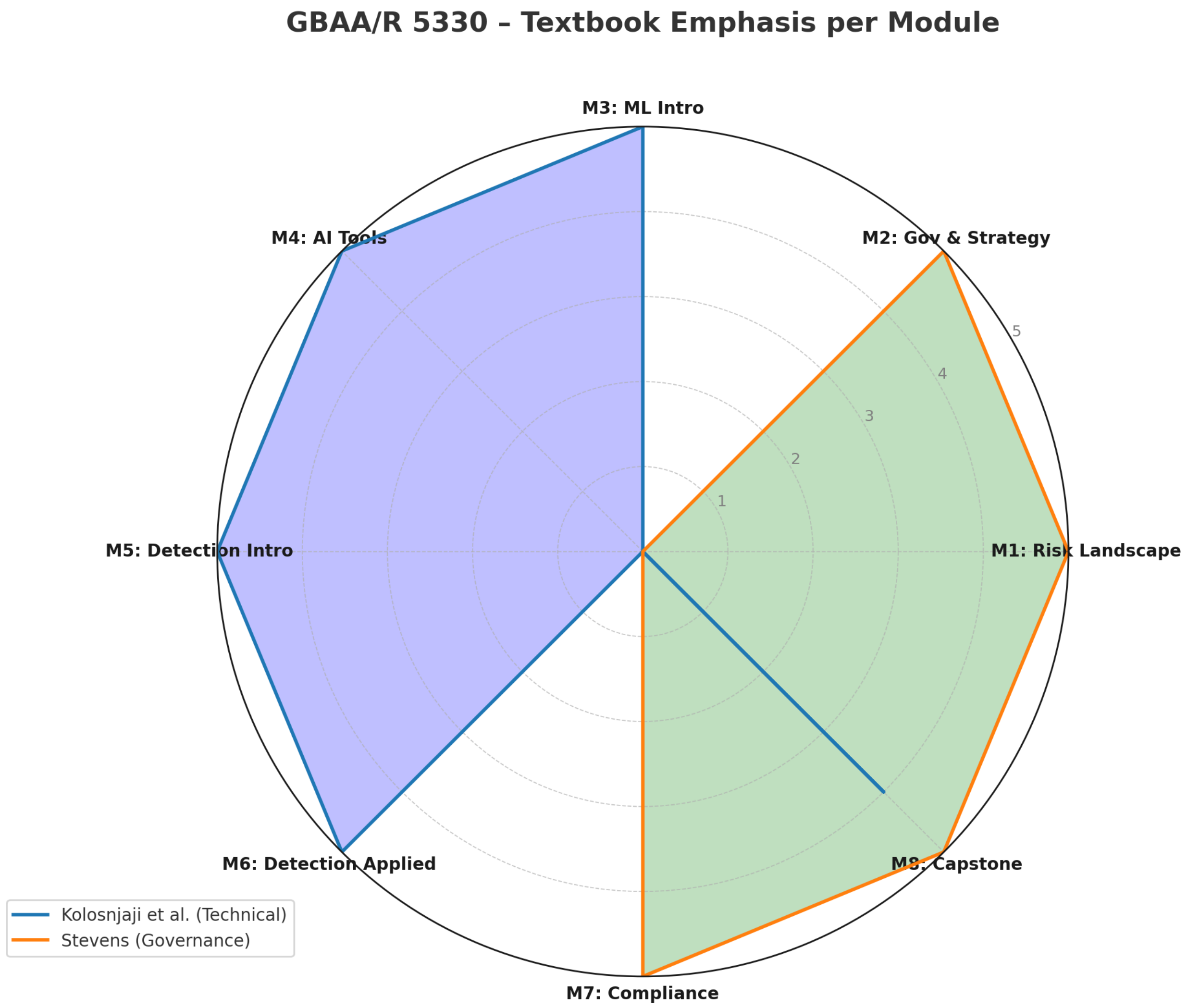
Dr. Mainuddin Shaik
Email: shaik.mainuddin@sulross.edu
Office Hours: Mondays & Wednesdays, 2:00 PM - 4:00 PM (via Zoom or by appointment)

Course Description

This course explores strategic frameworks for managing cybersecurity risk and protecting digital assets. Students will examine how machine-learning (ML) and artificial-intelligence (AI) technologies can augment traditional security strategies by automating threat detection, recognizing attack patterns and reducing human dependency in high-risk environments. Emphasis is placed on aligning security initiatives with business objectives and regulatory requirements in today's complex digital landscape

Course Materials

1. **Artificial Intelligence for Cybersecurity** (Kolosnjaji et al., 2024) – ML/anomaly detection.
2. **AI and the Future of GRC** (Stevens, 2024) – governance, risk, compliance integration.



Program Student Learning Outcomes

Upon completion of the MS in Cybersecurity and Risk Assurance Program, students will be able to:
PO1: Analyze complex financial scenarios to identify, assess, and mitigate risks.
PO2: Analyze cybersecurity management scenarios to identify, assess, and mitigate risks. (Assessed in this course)
PO3: Design comprehensive governance frameworks and risk management strategies to ensure organizational resilience and regulatory compliance
PO4: Solve complex business problems and plan to manage organizational change effectively

Course Student Learning Outcomes

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

- **Critically analyze** evolving cyber-threat landscapes and risk management strategies.
- **Apply early-intervention frameworks** using ML-based detection systems to identify attack patterns.
- **Evaluate the use of AI/ML** in developing resilient, autonomous cybersecurity systems.
- **Develop strategic plans** that integrate regulatory compliance, governance models and digital-assurance tools.

Marketable Skills

Students can expect to develop in the Cyber Risk & Assurance Strategy course:

- **Strategic risk analysis** – Evaluate evolving cyber-threat landscapes and align security initiatives with business objectives.
- **AI-driven detection expertise** – Use machine learning for early warning and anomaly detection to identify attack patterns.
- **Regulatory compliance mapping** – Translate regulatory requirements into actionable policies and compliance roadmaps.
- **Risk-governance planning** – Develop comprehensive cyber-risk plans that balance governance, technology and operations.
- **Data analytics and visualization** – Produce clear, decision-ready dashboards and reports using tools like Python and Power BI/Tableau.
- **Executive communication** – Write concise memos and policy briefs to communicate technical risk insights to business leaders.

Course Assignments and Grading

Assignment	% of Final Grade
Case-Based Analysis – Real-world breach case with AI-driven risk strategy recommendations	20%
AI Tool Walkthrough – Hands-on review/demonstration of an AI security platform (vendor demo, sandbox, or lab)	15%
Tool Evaluation Report – Comparative review of two AI-driven security tools (e.g., Darktrace, Splunk ML Toolkit)	15%
Midterm Strategy Brief – AI/ML-integrated cyber risk strategy with focus on tool selection & application	20%
Compliance Policy Map – Mapping chosen AI tools to relevant compliance standards (NIST, ISO, GDPR)	15%
Final Presentation & Report – Comprehensive AI-enhanced cyber strategy plan integrating governance, compliance, and tools	15%
Total	**100%**

Late Assignment Statement:

Assignments are due by 11:59 pm on the posted due date. Late submissions will be accepted up to 48 hours past the deadline with a 10 % deduction per day. Work submitted more than 48 hours after the due date will not be accepted unless prior arrangements have been made with the instructor for extenuating circumstances. Participation in discussions must follow module timelines; late posts may not receive credit.

Case-Based Analysis – 20%

Criteria	Exceeds Standard	Meets Standard	Approaching Standard	Below Standard
Breach Understanding	Fully explains incident scope, root causes, and impact; links to broader threat trends.	Explains incident and impacts; makes some link to broader context.	Describes event but omits key impacts or context.	Misunderstands or omits major facts.
AI/Tool Strategy Proposal	Proposes a well-reasoned, tool-based mitigation strategy aligned to breach specifics.	Suggests relevant tool-based strategy with reasonable justification.	Suggests strategy but lacks alignment with breach specifics.	Offers vague or irrelevant strategy.
Evidence & Examples	Uses current threat data, vendor case studies, and course readings effectively.	Uses some supporting evidence; may need more detail.	Minimal evidence or outdated examples.	No supporting evidence.
Clarity & Professionalism	Well-structured, free of errors, professional tone.	Clear and organized with minor errors.	Some organization issues or frequent minor errors.	Disorganized or error-filled.

AI Tool Walkthrough – 15%

Criteria	Exceeds Standard	Meets Standard	Approaching Standard	Below Standard
Tool Selection	Chooses an appropriate AI security tool and explains selection rationale.	Chooses a relevant tool with some rationale.	Tool choice is somewhat relevant but rationale is weak.	Tool is not relevant to topic.
Demonstration & Features	Clearly demonstrates tool features and explains how they address specific threat types.	Demonstrates main features; connects to general threats.	Demonstration is basic; weak connection to threats.	Demonstration is unclear or incomplete.

Criteria	Exceeds Standard	Meets Standard	Approaching Standard	Below Standard
Insights & Observations	Provides deep insights into tool capabilities, strengths, and limitations.	Identifies key capabilities and some limitations.	Identifies capabilities but omits limitations.	No meaningful insights offered.
Presentation Quality	Well-organized visuals/screenshots and professional narration.	Adequate visuals and narration.	Sparse visuals or weak narration.	Poor visuals or no narration.

Tool Evaluation Report – 15%

Criteria	Exceeds Standard	Meets Standard	Approaching Standard	Below Standard
Comparison Criteria	Uses clear, relevant, and well-justified evaluation criteria.	Uses criteria that are generally relevant and clear.	Criteria are vague or incomplete.	Criteria are missing or irrelevant.
Analysis Depth	Thoroughly analyzes tools against criteria with specific examples and data.	Analyzes tools with some examples; moderate depth.	Provides surface-level comparison with minimal data.	Comparison is incomplete or unsupported.
Strategic Fit	Explains how each tool supports governance and compliance goals.	Mentions governance/compliance fit.	Minimal mention of governance/compliance.	No connection to governance/compliance.
Documentation & Clarity	Report is well-structured, professional, and free from major errors.	Mostly clear and professional with minor errors.	Organization is inconsistent; multiple errors.	Disorganized or unprofessional.

Midterm Strategy Brief – 20%

Criteria	Exceeds Standard	Meets Standard	Approaching Standard	Below Standard
Integration of Tools & Strategy	Clearly integrates AI tools into a cohesive cyber risk strategy.	Integrates tools with some strategy linkage.	Lists tools without strategic connection.	No integration of tools and strategy.
Practical Recommendations	Recommendations are specific, actionable, and realistic for the given scenario.	Recommendations are generally clear and actionable.	Recommendations are vague or overly broad.	Recommendations are impractical or missing.
Evidence & Compliance Mapping	Supports recommendations with evidence and maps to relevant standards (e.g., NIST).	Maps to some standards; uses limited evidence.	Little mapping or evidence.	No mapping or evidence.
Clarity & Professionalism	Well-structured and concise; professional tone.	Organized with minor errors.	Some clarity/organization issues.	Disorganized or unclear.

Compliance Policy Map – 15%

Criteria	Exceeds Standard	Meets Standard	Approaching Standard	Below Standard
Mapping Accuracy	Correctly maps tools and processes to multiple compliance controls.	Maps to controls with minor errors.	Maps to some controls; incomplete coverage.	No or incorrect mapping.
Clarity of Framework Use	Clearly explains how frameworks (NIST, ISO, GDPR) apply.	Explains some framework connections.	Minimal explanation of frameworks.	No framework explanation.
Strategic Justification	Strong rationale for why chosen tools meet compliance needs.	Some rationale provided.	Minimal rationale.	No rationale.
Documentation Quality	Clear visuals, tables, or charts; free from major errors.	Adequate visuals and explanations.	Sparse visuals or unclear text.	Poorly documented.

Final Presentation & Report – 15%

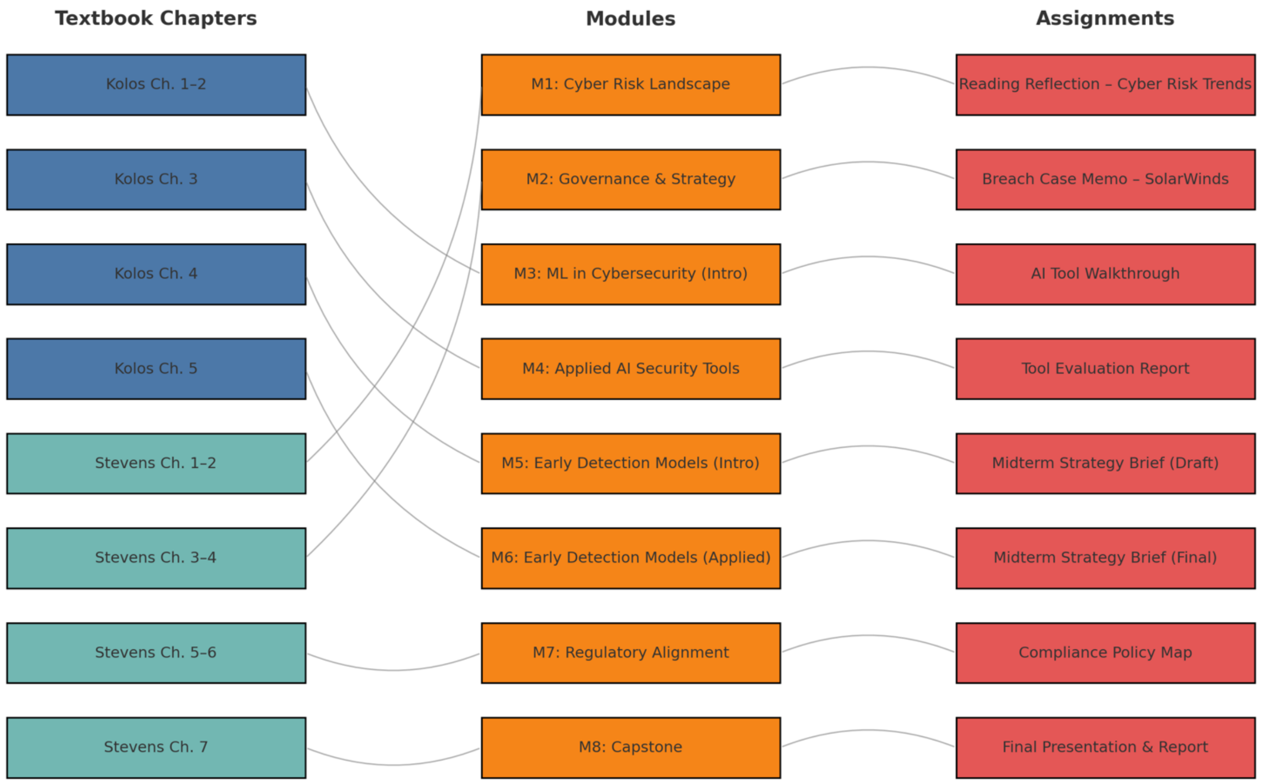
Criteria	Exceeds Standard	Meets Standard	Approaching Standard	Below Standard
Strategy Cohesion	Presents a cohesive AI-enhanced strategy integrating governance, compliance, and tools.	Strategy is mostly cohesive; minor gaps.	Strategy is fragmented or incomplete.	No clear strategy.
Tool Justification	Strong justification for chosen tools and configurations.	Justification is adequate but general.	Minimal justification.	No justification.
Evidence & Standards Integration	References industry data, tool results, and compliance standards.	Uses some data and standards.	Minimal references.	No references.
Presentation Delivery	Clear, engaging, professional visuals and delivery.	Delivery is clear with minor issues.	Delivery lacks engagement or clarity.	Poor or missing delivery.

Course Schedule

Course Schedule with Dates, Readings & Assignments

Module	Dates	Key Topics & Assignments	Readings
1	Aug 25 – Aug 31	**Cyber Risk Landscape** – Overview of current threats and risk concepts. **Due Aug 31:** • Discussion/IDA: *Introduce Yourself* • Discussion: *Current Threat Trends* • Assignment: *Reading Reflection – Cyber Risk Trends*	Stevens Ch. 1–2; current threat report (Verizon DBIR 2025 or ENISA Threat Landscape).
2	Sept 2 – Sept 7 (Sept 1 Labor Day – no class)	**Governance & Strategy** – Governance frameworks, strategic planning. **Due Sept 7:** • Discussion: *Governance Challenges in AI Security* • Assignment: *Breach Case Memo – SolarWinds or Similar*	Stevens Ch. 3–4; NIST CSF summary; case study reading.
3	Sept 8 – Sept 14	**ML in Cybersecurity (Intro)** – Fundamentals of ML in threat detection (light technical). **Due Sept 14:** • Discussion: *AI Use Cases in SOC Operations* • Assignment: *AI Tool Walkthrough* – demo or sandbox review of an AI-driven security	Kolosnjaji Ch. 1–2; vendor whitepaper/demo docs.

Module	Dates	Key Topics & Assignments	Readings
		platform (e.g., Darktrace demo, Microsoft Sentinel analytics)	
4	Sept 15 – Sept 21	**Applied AI Security Tools** – Integrating AI tools into SOC workflows. **Due Sept 21:** • Discussion: *Choosing the Right AI Security Tool* • Assignment: *Tool Evaluation Report* – compare two AI tools based on features, usability, and detection performance	Kolosnjaji Ch. 3; vendor docs (e.g., Splunk ML Toolkit, IBM QRadar Advisor).
5	Sept 22 – Sept 28	**Early Detection Models (Intro)** – Anomaly detection and early warning frameworks. **Due Sept 28:** • Discussion: *Best Practices for Anomaly Detection* • Assignment: *Midterm Strategy Brief (Draft)* – AI/ML integrated, tool-focused	Kolosnjaji Ch. 4; vendor case study on anomaly detection (e.g., CrowdStrike, Vectra AI).
6	Sept 29 – Oct 5	**Early Detection Models (Applied)** – Tuning and evaluating detection tools, reducing false positives. **Due Oct 5:** • Discussion: *Balancing Sensitivity & Accuracy* • Assignment: *Midterm Strategy Brief (Final)* – with refined tool recommendations	Kolosnjaji Ch. 5; blog/whitepaper on false-positive reduction strategies.
7	Oct 6 – Oct 12	**Regulatory Alignment** – Compliance mapping, NIST/ISO standards for AI security tools. **Due Oct 12:** • Discussion: *Aligning AI Tools to Compliance Standards* • Assignment: *Compliance Policy Map* – mapping chosen tools to NIST or ISO controls	Stevens Ch. 5–6; NIST SP 800-53 mapping guide.
8	Oct 13 – Oct 17	**Capstone** – Comprehensive AI-enhanced cyber strategy plan. **Due Oct 17:** • Discussion: *Lessons Learned & Capstone Reflection* • Assignment: *Final Presentation & Report* – strategy plan integrating governance and applied AI tool stack	Stevens Ch. 7; review Kolosnjaji Ch. 1–5 for technical integration.


Textbook Chapters
Modules
Assignments
Kolos Ch. 1–2
Kolos Ch. 3
Kolos Ch. 4
Kolos Ch. 5
Stevens Ch. 1–2
Stevens Ch. 3–4
Stevens Ch. 5–6
Stevens Ch. 7
M1: Cyber Risk Landscape
M2: Governance & Strategy
M3: ML in Cybersecurity (Intro)
M4: Applied AI Security Tools
M5: Early Detection Models (Intro)
M6: Early Detection Models (Applied)
M7: Regulatory Alignment
M8: Capstone
Reading Reflection – Cyber Risk Trends
Breach Case Memo – SolarWinds
AI Tool Walkthrough
Tool Evaluation Report
Midterm Strategy Brief (Draft)
Midterm Strategy Brief (Final)
Compliance Policy Map
Final Presentation & Report

Week-by-Week Focus & Deliverables

Week	Dates	Focus & Key Topics	Deliverables
Week 1	Aug 25 – Aug 31	Cyber Risk Landscape – threats & concepts.	Reflection due Aug 31.
Week 2	Sept 2 – Sept 7	Governance & Strategy – frameworks, planning.	Breach case memo due Sept 7.
Weeks 3–4	Sept 8 – Sept 21	ML in Cybersecurity – intro + applied tools.	Tool walkthrough (Sept 14) & tool evaluation report (Sept 21).
Weeks 5–6	Sept 22 – Oct 5	Early Detection Models – intro + applied tuning.	Midterm brief draft (Sept 28) & final (Oct 5).
Week 7	Oct 6 – Oct 12	Regulatory Alignment – compliance mapping.	Compliance policy map due Oct 12.
Week 8	Oct 13 – Oct 17	Capstone – AI-enhanced strategy plan.	Final presentation & report due Oct 17.

ADA Statement

SRSU Accessibility Services. Sul Ross State University (SRSU) is committed to equal access in compliance with the Americans with Disabilities Act of 1973. It is SRSU policy to provide reasonable accommodations to students with documented disabilities. It is the student's responsibility to initiate a request each semester for each class. Students seeking accessibility/accommodations services must contact Mrs. Mary Schwartze Grisham, LPC, SRSU's Accessibility Services Director or Ronnie Harris, LPC, Counselor, at 432-837-8203 or email mschwartze@sulross.edu or ronnie.harris@sulross.edu. RGC students can also contact Alejandra Valdez, at 830-758-5006 or email alejandra.valdez@sulross.edu. Our office is located on the first floor of Ferguson Hall, room 112, and our mailing address is P.O. Box C122, Sul Ross State University, Alpine. Texas, 79832.

Student Responsibilities Statement

All full-time and part-time students are responsible for familiarizing themselves with the Student Handbook and the Undergraduate & Graduate Catalog and for abiding by the University rules and regulations. Additionally, students are responsible for checking their Sul Ross email as an official form of communication from the university. Every student is expected to obey all federal, state and local laws and is expected to familiarize themselves with the requirements of such laws.

SRSU Distance Education Statement

Students enrolled in distance education courses have equal access to the university's academic support services, such as library resources, online databases, and instructional technology support. For more information about accessing these resources, visit the SRSU website.

Students should correspond using Sul Ross email accounts and submit online assignments through Blackboard, which requires a secure login. Students enrolled in distance education courses at Sul Ross are expected to adhere to all policies pertaining to academic honesty and appropriate student conduct, as described in the student handbook. Students in web-based courses must maintain appropriate equipment and software, according to the needs and requirements of the course, as outlined on the SRSU website. Directions for filing a student complaint are located in the student handbook.

Counseling

Sul Ross has partnered with TimelyCare where all SR students will have access to nine free counseling sessions. You can learn more about this 24/7/365 support by visiting Timelycare/SRSU. The SR Counseling and Accessibility Services office will continue to offer in-person counseling in Ferguson Hall room 112 (Alpine campus), and telehealth Zoom sessions for remote students and RGC students.

Libraries

The Bryan Wildenthal Memorial Library and Archives of the Big Bend in Alpine offer FREE resources and services to the entire SRSU community. Access and borrow books, articles, and more by visiting the library's website, library.sulross.edu/. Off-campus access requires logging in with your LoboID and password. Librarians are a tremendous resource for your coursework and can be reached in person, by email (srsulibrary@sulross.edu), or by phone (432-837-8123).

No matter where you are based, public libraries and many academic and special libraries welcome the general public into their spaces for study. SRSU TexShare Cardholders can access additional services and resources at various libraries across Texas. Learn more about the TexShare program by visiting library.sulross.edu/find-and-borrow/texshare/ or ask a librarian by emailing srsulibrary@sulross.edu.

Mike Fernandez, SRSU Librarian, is based in Eagle Pass (Building D-129) to offer specialized library services to students, faculty, and staff. Utilize free services such as InterLibrary Loan (ILL), ScanIt, and Direct Mail to get materials delivered to you at home or via email.

Academic Integrity

Students in this class are expected to demonstrate scholarly behavior and academic honesty in the use of intellectual property. Students should submit work that is their own and avoid the temptation to engage in behaviors that violate academic integrity, such as turning in work as original that was used in whole or part for another course and/or professor; turning in another person's work as one's own; copying from professional works or internet sites without citation; collaborating on a course assignment, examination, or quiz when collaboration is forbidden. Students should also avoid using open AI sources ***unless permission is expressly given*** for an assignment or course. Violations of academic integrity can result in failing assignments, failing a class, and/or more serious university consequences. These behaviors also erode the value of college degrees and higher education overall.

Classroom Climate of Respect

Importantly, this class will foster free expression, critical investigation, and the open discussion of ideas. This means that all of us must help create and sustain an atmosphere of tolerance, civility, and respect for the viewpoints of others. Similarly, we must all learn how to probe, oppose and disagree without resorting to tactics of intimidation, harassment, or personal attack. No one is entitled to harass, belittle, or discriminate against another on the basis of race, religion, ethnicity, age, gender, national origin, or sexual preference. Still, we will not be silenced by the difficulty of fruitfully discussing politically sensitive issues.

Supportive Statement

I aim to create a learning environment for my students that supports various perspectives and experiences. I understand that the recent pandemic, economic disparity, and health concerns, or even unexpected life events may impact the conditions necessary for you to succeed. My commitment is to be there for you and help you meet the learning objectives of this course. I do this to demonstrate my commitment to you and to the mission of Sul Ross State University to create a supportive environment and care for the whole student as part of the Sul Ross Familia. If you feel like your performance in the class is being impacted by your experiences outside of class, please don’t hesitate to come and talk with me. I want to be a resource for you.