

Information Security Strategies and Policies (PUBP/CS/MGT 6725)

Fall 2026 Section OCY, OAN	MS in Cybersecurity, School of Public Policy, IAC
Delivery: 100% Web-Based, Asynchronous	Canvas for Content Delivery
Dates: August 24 - December 7, 2026	

Instructor Information

Instructor	Dr. Brenden Kuerbis
Office	Remote
Office Hours	Zoom — See Canvas for scheduled times

General Course Information

Description

This course introduces students to the policy and management aspects of cybersecurity. It is based on the idea that cybersecurity policy can be sorted into three “layers” representing different levels of social organization: the organizational level, the national level, and the transnational level. The course is divided into four modules. The first exposes students to basic concepts and definitions regarding policy, governance, and threats. The second deals with cybersecurity policy at the organizational level; the third deals with cybersecurity public policy at the national level; the fourth deals with cyber conflict, policy and diplomacy at the transnational level. This course situates cybersecurity in the overall Internet ecosystem. Student deliverables include small group projects as well as individually completed quizzes, discussions, and a final term paper. This is a required core course for all tracks in the Online MS in Cybersecurity.

Pre- and/or Co-Requisites

Students will be expected to have a basic understanding of computers and data networking and will learn some technical material regarding internet protocols, vulnerabilities, exploits and incident response, but the primary focus of the course is on the public policy, management and international relations aspects of cybersecurity. The course does not require programming skills, although they can be useful in some assignments. Students should be able to blend and integrate economic, technical and political modes of analysis. Students are expected to be familiar with academic research and writing practices, including the proper use of academic citations. This course is best taken in conjunction with CS 6035 (Introduction to Information Security) for an introduction to the more technical aspects of cybersecurity.

Course Goals and Learning Outcomes

Upon successful completion of this course, you should be able to:

1. Recognize the different governance structures used to promote cybersecurity
2. Identify key cybersecurity policy frameworks and standards (e.g., NIST framework)
3. Write a cybersecurity policy for an organization
4. Analyze and assess the effects of existing and proposed cybersecurity laws and regulations
5. Propose actions or strategies that respond to the geopolitical dimension of cyber conflict
6. Recognize the intersections of cybersecurity governance with the governance, standards and operations of the Internet

Course Materials

Due to the dynamic nature of our subject matter, no single book exists that meets all course requirements. Each topical area has one or two required readings, which are listed in the course schedule under the “Readings” column. All required readings are available as pdfs or via the Georgia Tech library. Doing the readings is very important and forms a significant portion of your grade. Quizzes assess your comprehension of the readings. Additional recommended or supplemental materials may be posted on Canvas or Ed Discussion in response to relevant ongoing events in cybersecurity. Please use Ed

Discussion for any substantive or administrative questions. In addition, a Frequently Asked Question (FAQ) page features answers to common questions. Please familiarize yourself with this valuable resource which is updated on a regular basis.

Course Website and Other Classroom Management Tools

This class will use Canvas to deliver course materials to online students. ALL course materials and activities will take place on this platform, with supplemental discussion occurring on Ed Discussion. It is your responsibility to keep apprised of Instruction team communications made on these platforms. If you are new to Canvas, you can find Georgia Tech's [Canvas Resources for Students](#) here.

Assignment Distribution and Grading Scale

Here is a list of the assignments and activities required in the course. Grading is not “curved;” students will be graded based on how well they have met the requirements of the assignment and accomplished specific learning objectives. Except for quizzes, most assignments will have a rubric associated with them so that students can see what criteria are used for grading and what weight is given to them. TAs may ask students who submitted excellent assignments for their permission to share their submission with the course/class.

Assignment	Release Date	Due Date	Weight
Module 1 Perusall readings	Aug 24	Sep 8	5%
Assignment #1: Go Phish (group assignment)	Sep 3	Sep 14	15%
Quiz on Module 1	Sep 4	Sep 11	5%
Module 2 Perusall readings	Sep 14	Sep 28	5%
Assignment #2: Organizational Policy (group assignment)	Sep 14	Oct 7	15%
Quiz on Module 2	Oct 2	Oct 9	5%
Module 3 Perusall readings	Oct 12	Oct 26	5%
Assignment #3: Policy Challenge (individual assignment in the form of a small group discussion)	Oct 19	Oct 30	15%
Quiz on Module 3	Oct 30	Nov 6	5%
Module 4 Perusall readings	Nov 9	Nov 20	5%
Assignment #4: Term Paper (individual assignment)	Nov 16	Dec 7	15%
Quiz on Module 4	Nov 27	Dec 4	5%

Assignment Submission and Due Dates

All assignments must be submitted by 11:59:00pm EST on the due date, unless otherwise noted. All assignments are due relative to the Eastern Standard Time Zone (EST). Eastern Standard Time is UTC - 5. Eastern Daylight time is UTC -4. We will not accept assignments submitted late due to time zone issues. You should update your canvas to account for EST if you are in a different time zone.

Most assignments will be finalized by the student uploading a file in Canvas' assignment module. If not specified otherwise, use the Word file extension *.docx or *.doc. Some assignments use Turnitin to ensure academic integrity, proper citations, and check spelling/grammar. Please review any Turnitin report prior to your final submission of the assignment and make changes if warranted (see Plagiarism & Academic Integrity Policy in this syllabus). Do not send assignments directly to the instruction team. All

assignments must be submitted within the Canvas assignment; otherwise, they will be considered not submitted. If there are technical issues, please contact Canvas support, as well as notify the TAs immediately.

TAs will grade and provide feedback within one to two weeks after the assignment's due date. Submit questions about TA feedback and/or regrade requests via a private Ed Discussion post (please select category "regrade requests") are due within seven days (excluding weekends and official holidays) after the release of the graded assignment. Regrade requests must address specific errors in grading, will lead to a review of the entire assignment, and may result in a higher, the same, or a lower grade.

Quizzes

Quizzes become available a week before they are due and must be completed by the due date. Quizzes are open-book/open-notes and do not have a time limit. Your answers are recorded and graded as you enter them. Quizzes remain available for two days past the due date – after that, they become unavailable. If you fail to take a quiz before then, you lose the points. Quizzes are individual assignments intended to provide an incentive to study the readings and strengthen your recall and understanding of the reading and lecture material. Students should not help each other answer the quiz questions.

Late assignments, Missed Quizzes, Re -scheduling

There is a very simple policy governing late submissions: for all assignments and quizzes, a penalty of 5 percentage points off your score is applied for every day it is late, until the assignment becomes unavailable, which is usually 2 days after the submission deadline. At that point, a 0-point grade will be assigned. This policy will be applied regardless of the reason for your lateness; it doesn't matter whether you just forgot, your day job intervened, you had family problems, moved for private or professional reasons, etc. The only special circumstances that will be accommodated are those that literally incapacitate the student for a significant period of time, such as injury and hospitalization, floods, hurricanes, power outages for several days, etc. Please do not waste the instructors' time asking for extensions for any other reasons. If special circumstances apply, a student must contact the Office of Student Life (OSL), submit a request ([Class Absence Verification Form](#)) in a timely manner with required evidence. OSL will then provide a recommendation to the instructor for a possible course of action. Please note that for group assignments, options to accommodate extensions, etc. are very narrow due to the nature of the assignment. It is the student's responsibility to submit the request and forward any responses to the Instructor. If the Instruction team is not notified by the Office of Student Life by the end of the semester, the temporary extension may be reverted to the original assignment submission date, and grades adjusted accordingly.

Peer evaluations

During the semester students will fill out two peer evaluations to assess how each group member contributed to the group projects in assignments 1 and 2 and how the group functioned. This allows group members to praise their peers for their contribution, to identify "free riders" who did not contribute, or to identify and explain problems with group coordination or behavior that affected the quality or timeliness of the project. Submitting both peer evaluations is required. A peer evaluation that indicates insufficient contribution may lower a student's final grade. Please note that late and non-submissions will lead to a deduction in the respective assignment.

Grading Scale

Your final grade will be assigned as a letter grade according to the following scale:

A	90-100%
B	80-89%
C	70-79%
D	60-69%
F	0-59%

Georgia Institute of Technology

Course Syllabus: Information Security Strategies and Policies (PUBP/CS/MGT 6725)

In general, it is best to accept the grade you get and learn from mistakes and shortcomings, rather than asking the instructor to change your grade. Never ask the Professor to change your grade because you are "close" to an A but didn't get one. Only ask to change if you think an error was made in grading.

Technology Requirements and Skills

To participate in this class, you need the following computer hardware and software:

- Broadband Internet connection
- Laptop or desktop computer with a **minimum** of a 2 GHz processor and 2 GB of RAM
- Working webcam (to complete the onboarding module/quiz which is required to access the course; there is no workaround for this)
- Windows for PC computers or MacOS for Apple computers.
- Complete Microsoft Office Suite or comparable applications and ability to use Adobe PDF software (install, download, open and convert)
- Edge, Firefox, Chrome and/or Safari browsers

Technology Help Guidelines

30-Minute Rule: When you encounter struggles with technology, give yourself 30 minutes to 'figure it out.' If you cannot, then post a message to the Ed Discussion board; your peers may have suggestions to assist you. You are also directed to contact the Helpdesk 24/7.

When posting or sending an email requesting help with technology issues, whether to the Helpdesk, message board, or the professor use the following guidelines:

- Include a descriptive title for the subject field that includes 1) the name of the course 2) the issue.
- List the steps or describe the circumstance that preceded the technical issue or error. Include the exact wording of the error message.
- When possible, include a screenshot(s) demonstrating the technical issue or error message.
- Also include what you have done to try to remedy the issue (rebooting, trying a different browser, etc.).

Communication Policy

For course-related communication to the professor/TAs, including grading questions, please create a private Ed Discussion post. All other posts on Ed Discussion should be public so that all students can benefit from the questions and answers. TAs may change a private into a public post, if a post benefits the entire class. Please note that "anonymous posts" are only anonymous to other students, not the instruction team. For concerns of a personal nature, please use the Canvas Inbox to contact the instructor.

Posts/messages will be checked at least twice per day Monday through Friday. On Saturday, posts/messages will be checked once per day. The instruction team will respond to posts/messages within 24 hours; on weekends and holidays, allow up to 48 hours.

Virtual office hours will be held using Zoom. Students are encouraged to join office hours. Office hours are not held during instructional days, reading period, final exam week and designated School as well as U.S. federal holidays. If you are not able to join, you can watch the recordings, which are available in Canvas' Media Gallery. Special topic office hours will be announced in advance.

Online Student Conduct and Netiquette

Communicating appropriately in the online classroom can be challenging. To minimize this challenge, please keep communications with your fellow students and the instructions team professional and courteous. It is important to remember several points of "internet etiquette" that will smooth communication for both students and instructors:

Read first, Write later. Read the ENTIRE set of posts/comments on a discussion board before posting your reply, to prevent repeating commentary or asking questions that have already been answered.

Georgia Institute of Technology

Course Syllabus: Information Security Strategies and Policies (PUBP/CS/MGT 6725)

Avoid language that may come across as strong or offensive. Language can be easily misinterpreted in written electronic communication. Review email and discussion board posts *before* submitting. Humor and sarcasm may be easily misinterpreted by your reader(s). Try to be as matter-of-fact and professional as possible.

Follow the language rules of the Internet. Do not write using all capital letters, because it will appear as shouting. Also, the use of emoticons can be helpful when used to convey nonverbal feelings.

Consider the privacy of others. Ask permission prior to giving out a classmate's email address or other personally identifiable information.

Keep attachments small. Avoid gigantic files; if it is necessary to send pictures, minimize the size.

No inappropriate material. Do not forward virus warnings, chain letters, jokes, porn, etc. to classmates or instructors. The instructor reserves the right to remove posts that are not collegial in nature and/or do not meet the Online Student Conduct and Etiquette guidelines listed above.

University Use of Email

A university-assigned student e-mail account is the official university means of communication with all students at Georgia Institute of Technology. Students are responsible for all information sent to them via their university-assigned e-mail account. If a student chooses to forward information in their university e-mail account, he or she is responsible for all information, including attachments, sent to any other e-mail account. To stay current with university information, students are expected to check their official university e-mail account and other electronic communications on a frequent and consistent basis. Recognizing that some communications may be time-critical, the university recommends that electronic communications be checked minimally twice a week.

Plagiarism & Academic Integrity

Georgia Tech aims to cultivate a community based on trust, academic integrity, and honor. Students are expected to act according to the highest ethical standards. All students enrolled at Georgia Tech, and all its campuses, are to perform their academic work according to standards set by faculty members, departments, schools and colleges of the university; and cheating and plagiarism constitute fraudulent misrepresentation for which no credit can be given and for which appropriate sanctions are warranted and will be applied. For information on Georgia Tech's Academic Honor Code, please visit [Academic Honor Code](#) or [XVIII Code of Conduct](#).

This course uses Turnitin to identify and/or quantify material copied from other sources or created using generative AI technology. Students should review their Turnitin scores, and, if necessary, make revisions prior to submitting the assignment. Unacceptably copying, missing quotation marks, and/or failure to provide citations to others' work – as indicated by a high Turnitin score – will result in penalties to the grade. In such cases, the instruction team may request the student to re-do the paper and/or reject the assignment as failed in serious cases, resulting in 0 points. In addition, a student suspected of cheating or plagiarizing on an assignment will be reported to the Office of Student Integrity, which will investigate the incident and identify the appropriate penalty for violations.

Generative AI Tools Use

In this course, using generative AI tools in the work of the course (including programming, language editing) is allowed. However, as with any technology, generative AI tools need to be used critically and according to academic and professional expectations. When using generative AI tools, you are expected to adhere to the following principles:

- **Responsibility:** You are responsible for the work you submit. This means that any work you submit should be your own, and any AI-generated content appropriately cited (see Documentation below). It is your responsibility to ensure that any factual statements produced by a generative AI tool are true, and that any references or citations produced by the AI tool are correct and verifiable.

Georgia Institute of Technology

Course Syllabus: Information Security Strategies and Policies (PUBP/CS/MGT 6725)

- Transparency: Any unmodified text paragraphs, diagrams or code generated using an AI tool should be disclosed in a paragraph at the beginning of the paper. The specific model or service used should be indicated.
- Documentation: You should cite any content generated by an AI tool as you would when quoting, paraphrasing, or summarizing ideas, text, images, or other content made by other people.

Some words of advice: You are here, in part, to develop your professional expertise and judgement. Use of these tools should complement, not substitute, that objective. Please do not simply copy and paste generative AI output verbatim, retain your voice and critical thinking. We suggest keeping documentation of your prompts and outputs, so you can explain if/how these tools were used in the process of developing work. Using generative AI tools in the course without adhering to the above principles may be considered an infraction of Georgia Tech's Academic Honor Code, subject to investigation by the Office of Student Integrity. More generally, Georgia Tech's Library provides rich resources to make your research and writing a success. Consult the [Library's Public Policy Research Guide](#) and guidance on [Effective and Responsible Use of AI in Research](#), take a class at the library (<https://www.library.gatech.edu/research-help-support/library-classes>), and/or use the library's help & support (<https://library.gatech.edu/research-help-support>).

Accommodations for Students with Disabilities

If you are a student with learning needs that require special accommodation, contact the [Office of Disability Services](#) at (404)894-2563, as soon as possible, to make an appointment to discuss your special needs and to obtain an accommodations letter. Please also e-mail the instructor as soon as possible to set up a time to discuss your learning needs.

Student-Faculty Expectations Agreement

At Georgia Tech we believe that it is important to strive for an atmosphere of mutual respect, acknowledgement, and responsibility between faculty members and students. See the GT [catalog](#) for an articulation of some basic expectations that you can have of me and that I have of you. In the end, respect for knowledge, hard work, and cordial interactions will help build the environment we seek. I encourage you to remain committed to the ideals of Georgia Tech while in this class.

Course Schedule

Module 1: The Basics

Week/Dates	Topic	Deliverables	Readings
Week 1 Aug 24	Topic 1: Introduction, Lessons 1-4		
Week 2 Aug 31	Topic 2: Concepts and vocabulary, Lessons 1-3	Assignment 1: Go Phish begins	Institutional Landscape of Cybersecurity, by B. Kuerbis and F. Badii (2017)
Week 3 Sept 7	Topic 3: Analysis tools, Lessons 1-3	Assignment 1 due Quiz 1 and Perusall readings due	The Diamond Model of Intrusion Analysis, by S. Caltagirone et al (2016)

Module 2: Cybersecurity in the Organization

Week/Dates	Topic	Deliverables	Readings
Week 4 Sept 14	Topic 1: Organizational security policies, Lessons 1-3	Assignment 2: Organizational Policy begins	NIST Cybersecurity Framework 2.0 , pages 1-5, 15-23 Information Risk Insights Study by Cyentia Institute (2025) (optional) Evidence-based cybersecurity policy? A meta-review of security control effectiveness, by Woods & Seymour (2023)
Week 5 Sept 21	Topic 2: Managing cyber risk, Lessons 1-3		Lessons Lost: Incident Response in the Age of Cyber Insurance and Breach Attorneys, by Woods, Bohme, et al (2023) Measuring Risk: Computer Security Metrics, Automation, and Learning, by Slayton (2015)
Week 6 Sept 28	Topic 3: Public Key Infrastructure (PKI), Lessons 1-2 Topic 4: Compliance, Lessons 1-2		
Week 7 Oct 5	Topic 5: Industry-level cybersecurity efforts, Lessons 1-3	Assignment 2 due Quiz 2 and Perusall readings due	(optional) The Justice Department Sues Georgia Tech: A Teachable Moment in Cybersecurity Management, by Mueller (2024)

Module 3: Cybersecurity Policy at the National Level

Week/Dates	Topic	Deliverables	Readings
Week 8 October 12	Topic 1: Public policy, Lessons 1-2	Assignment 3: Discussion Board (Policy Challenge) begins	Read the proposed bill for legislative challenge
Week 9 October 19	Topic 2: Closer Look at US laws & bureaucracy, Lessons 1-3		Cyber Risk Reduction in China, Russia, the US, and the European Union, by SIPRI (2024)
Week 10 October 26	Topic 2: Closer Look at US laws & bureaucracy, Lessons 4 - 7	Assignment 3 discussion board closes	Regulating risks within complex sociotechnical systems, by A. Clark-Ginsberg and Slayton, R. (2019) (optional) Complex Supply Chains in Renewable Energy Technologies, by J. Anjanappa (2025)
Week 11 November 2	Topic 3: Critical infrastructure, Lessons 1-2	Quiz 3 and Perusall readings due	

Module 4: Cybersecurity Policy at the Transnational Level

Week/Dates	Topic	Deliverables	Readings
Week 12 November 9	Topic 1: States, sovereignty, cyberspace, & geopolitical conflict, Lessons 1-4		M. Warner, "US Cyber Command's First Decade." Hoover Institution, Aegis Series Paper No. 2008 (2020)
Week 13 November 16	Topic 2: Global cybersecurity governance, Lessons 1-4	Assignment 4: Term Paper begins) Perusall Readings due	Grindal, Mueller, Srivastava, Non-governmental governance of trust on the internet: WebPKI as public good (2025)
Week 14 November 23	Thanksgiving break		
Week 15 November 30	Topic 3: Technological change and governance, Lessons 1-2	Quiz 4 and Perusall readings due	Executive Order 14409, "Promoting Advanced AI Innovation and Security" (2026) "On Transparent AI Cyber Protections", by Cybersecurity experts (2026) (optional) Against Sovereignty in Cyberspace, by M. Mueller (2019)
Week 16 December 7		Assignment 4 due	