

City University of New York – Hunter College

Intro to Cyber Risk – Spring 2022

Syllabus

Course Information:

CSCI 39598-02: Intro to Cyber Risk

In-person

Class Meets: Mondays 5:35 – 8:15pm

Term: Friday, January 28, 2022 – Tuesday, May 24, 2022

Office Hours: Please schedule individually

Contact Information:

Professor Jennifer Rothstein, Adjunct Lecturer

Department of Computer Science

jr5909@hunter.cuny.edu (for any communication or email assignments)

professorrothstein@gmail.com (for Google Doc sharing purposes)

XXX-XXX-XXXX (text/call for emergencies)

Course Objectives & Learning Outcomes:

Introduction to Cyber Risk will teach students about the types of global cyber security threats our society faces, how we are defending against them and how we are preparing for the future. It is not a technical course focused on coding, programming or the mechanics behind a successful hack, but rather an analytical course which will introduce the most common categories of attacks; who is responsible for them and who; who the targets are and why; and what information is at risk. Among the topics included are the deconstruction of the cyber attack chain, cyber risk management best practices, and relevant legal and regulatory implications. Students will apply interdisciplinary skills such as analysis, role-playing, and essay-writing to gain an understanding of the impact of cyber security, the practical implications of

the damages and will study real-life incidents in real-time. Students will also become familiar with today's cyber leaders in both the private and public sector and will engage in group discussions as well as group projects to be better prepared to work in the collaborative environment the cyber security workforce requires. We will explore diversity in cyber security and consider ways to foster an inclusive and productive environment.

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

Define different types of cyber attacks/incidents/breaches

Identify the stakeholders and potential victims or affected parties before, during and after an incident

Develop an awareness of attacks in our everyday lives, track them and summarize them

Describe the potential damage from each type of attack

Present the major cyber attacks from the past decade and discuss predictions for 2022

Analyze an organization's cyber preparedness using industry-accepted standards

Understand basic regulations – both US and Global

Identify methodologies and actions for implementing best practices in cyber security

Discuss the benefits of cyber risk transfer and cyber insurance

Understand the role of law enforcement in the defense and investigation of cyber crimes

Develop an Incident Response Plan

Outline the life cycle of a ransomware attack

Present findings and recommendations to C-level executives as well as Board of Directors

Consider a career in cyber security

Encourage the exchange of diverse perspectives and solutions for cyber security challenges

Appreciate the various cyber leaders from the public and private sector

Weekly Schedule of Topics to be Covered

Students are expected to come to class prepared and ready to participate in class discussions and group projects. The associated chapters and reading materials should be read ahead of time and every student will be asked to contribute actively in class. The schedule and reading materials are subject to change, but students will be notified with enough time in advance to prepare.

Each class will begin with a brief discussion of a cyber incident that took place during the previous week. Each student is encouraged to bring in an example of an attack they identified from the previous week and be prepared to share it with the class. Students will learn about the reliable sources in the news that track these events and will gain an appreciation for how much information is being circulated about cyber security on a daily basis.

Each class will also begin with a brief discussion of an alert issued by law enforcement to the public the previous week. These alerts may cover new threats, vulnerabilities, ransomware groups or litigation. Students will become familiar with the role different agencies and government have in in this sector, and how the public is informed in an actionable way.

READINGS

Accompanying each week in the syllabus is a list of readings. All of the books/links to publications/links to resources listed below are required reading and may be updated as important current events emerge. Any additional or substitute reading will be announced in class and on Blackboard:

Book (selections throughout the semester): Next Level Cyber Security by Sai Huda (available on Amazon)

Weekly Readings:

Week 2:

<https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html>

<https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html>

<https://www.cyberscoop.com/fireeye-mandia-face-the-nation-solarwinds/>

<https://www.advintel.io/post/storm-in-safe-haven-takeaways-from-russian-authorities-takedown-of-revil>

<https://www.cnn.com/2021/12/16/tech/kronos-ransomware-attack/index.html>

<https://www.aig.com/us/-/media/files/gallagher/us/collections/ransomware-crops-up-in-the-food-agriculture-industry.pdf>

<https://www.csoonline.com.cdn.ampproject.org/c/s/www.csoonline.com/article/3647756/how-to-prioritize-and-remediate-vulnerabilities-in-the-wake-of-log4j-and-microsofts-patch-tuesday-b.amp.html>

<https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure>

<https://www.zdnet.com/article/microsoft-and-mcafee-headline-newly-formed-ransomware-task-force/>

<https://www.us-cert.gov/ncas/tips/ST04-001>

<https://cybersecurityventures.com/50-cybersecurity-titles-that-every-job-seeker-should-know-about/>

<https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework>

<https://digitalguardian.com/blog/innovation-diversity-cybersecurity>

<https://techcrunch.com/2022/01/03/connecting-the-dots-on-diversity-in-cybersecurity-recruitment/>

<https://www.uscybersecurity.net/history/>

<https://www.msn.com/en-us/money/news/a-diverse-cybersecurity-team-can-help-alleviate-the-talent-shortage/ar-AANie4U>

Week 3:

<https://niccs.us-cert.gov/about-niccs/glossary#A>

<https://www.sans.org/security-resources/glossary-of-terms/>

<https://www.imperva.com/cyber-threat-attack-map/>

<https://therecord.media/an-interview-with-blackmatter-a-new-ransomware-group-thats-learning-from-the-mistakes-of-darkside-and-revil/>

<https://www.solarium.gov/public-communications/2021-annual-report-on-implementation>

<https://www.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html>

<https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/>

<https://www.msspalert.com/cybersecurity-breaches-and-attacks/kaseya-rmm-cyberattack-warning/>

<https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-takes-additional-steps-to-prevent-evictions-as-the-delivery-of-emergency-rental-assistance-continues-to-increase/>

<https://gizmodo.com/kaseya-is-making-its-customers-sign-non-disclosure-agre-1847356517>

Huda, Chapters 1&2, Chapters 3- 4

Week 4:

<https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

<https://www-cnbccom.cdn.ampproject.org/c/s/www.cnbccom/amp/2019/12/23/stuxnet-target-equifax-worst-breaches-of-2010s.html>

<https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf>

Huda, (cont'd) Chapters 1&2, Chapters 3- 4

Week 5:

https://www.willistowerswatson.com/en-US/Insights/2021/08/hacking-back?utm_source=slipcase&utm_medium=affiliate&utm_campaign=slipcase

<https://healthitsecurity.com/features/this-years-largest-healthcare-data-breaches>

Huda, Chapter 12

Week 6:

<https://www.nist.gov/cyberframework>

<https://www.cisecurity.org/controls/> (Please download and read the controls)

<https://gdpr.eu/what-is-gdpr/>

<https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (look over list)

<https://studentprivacy.ed.gov/?src=fpc>

https://www.dfs.ny.gov/system/files/documents/2019/01/cyber_memo_12212_018.pdf

<https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf>

<https://oag.ca.gov/privacy/ccpa>

<https://lewisbrisbois.com/privacy/US>

https://www.crowdstrike.com/blog/lessons-from-past-cyber-operations-against-ukraine/?utm_source=bmbu&utm_medium=soc&utm_campaign=Blogs&blaid=2560793

Week 7:

<https://gdpr.eu/what-is-gdpr/>

<https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (look over list)

<https://studentprivacy.ed.gov/?src=fpc>

https://www.dfs.ny.gov/system/files/documents/2019/01/cyber_memo_12212_018.pdf

<https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf>

<https://oag.ca.gov/privacy/ccpa>

<https://lewisbrisbois.com/privacy/US>

<https://business.cch.com/CybersecurityPrivacy/eyemed-settlement.pdf>

<https://www.gllawgroup.com/wp-content/uploads/2022/01/Cyber-and-Silent-Cyber-Coverage.pdf>

Week 8:

<https://www.bbc.com/news/business-57423008>

<https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperRansomware.pdf>

<https://www.fireeye.com/blog/threat-research/2020/03/they-come-in-the-night-ransomware-deployment-trends.html>

<https://go.recordedfuture.com/hubfs/reports/cta-2020-0213.pdf>

<https://www.cnn.com/2019/10/08/business/ransomware-attacks-trnd/index.html>

<https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority>

<https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

<https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war>

<https://innovationinsurancegroup.com/merck-vs-ace/>

[https://www.wired.com/2015/05/silk-road-untold-story/ \(Part 1 & 2\)](https://www.wired.com/2015/05/silk-road-untold-story/)

Week 9: Midterm – in class

Week 10: Visit to NCFTA – in person

Week 11:

<https://www.ibm.com/downloads/cas/ZBZLY7KL>

<https://www.beazley.com/usa.html#> (please explore the site)

https://policies.dppl.com/policy.php?policy_number=BBR-5A8ED7A3-8OEF#pagenav-ag-1

<https://www.insurancejournal.com/news/international/2019/01/15/514558.htm>

<https://www.natlawreview.com/article/reasons-communicating-clearly-your-insurer-regarding-scope-coverage-purchasing-cyber>

<https://www.databreachninja.com/wp-content/uploads/sites/63/2019/01/MONDELEZ-INTERNATIONAL-INC-Plaintiff-v-ZURICH-AMERICAN-INSURANCE-COMPANY-Defenda.pdf>

<https://www.marshmma.com/blog/cyber-insurance-rates-could-rise-50-in-2021>

<https://www.natlawreview.com/article/four-new-cyber-war-exclusions-lloyd-s-market-association>

<https://www.gllawgroup.com/wp-content/uploads/2022/01/Cyber-and-Silent-Cyber-Coverage.pdf>

Week 12:

<https://www.bitcoin.com/bitcoin.pdf>

<https://gemini.com/learn>

<https://www.nasdaq.com/articles/a-blockchain-primer%3A-what-is-it-whos-using-it-when-itll-go-mainstream-and-how-to-invest-in>

Week 13:

<https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=8789>

https://www2.deloitte.com/content/dam/insights/us/articles/3749_Industry4-0_cybersecurity/DUP_Industry4-0_cybersecurity.pdf

<https://www.acq.osd.mil/cmmc/index.html>

<https://www.fbi.gov/investigate/cyber>

<https://www.infragard.org/> (review site)

<https://www.recordedfuture.com/threat-intelligence/>

Week 1: January 31st - First Day of Class!

Class Discussion:

- a. Introduction to Class & to Cyber Security Leaders
- b. Review of Syllabus
- c. Assignments of Roles
- d. Overview of Discussion Board
- e. Cyber Security in our Interconnected World:
 - i. Definition of Cyber Security
 - ii. What it is, what it's not, why it's important - who works in the field and what are they trying to accomplish?
- f. Brief History of Cyber Security & History of Cyber Risk
- g. Introduction to Ransomware

No Reading Due

Week 2: February 7th

Class Discussion:

- a. Solar Winds (case study/cyber attack)
- b. Kronos (case study/cyber attack)
- c. Log4j (study in vulnerability)
- d. Diversity in Cyber Security
- e. Careers in Cyber Security

<https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html>

<https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html>

<https://www.cyberscoop.com/fireeye-mandia-face-the-nation-solarwinds/>

<https://www.advintel.io/post/storm-in-safe-haven-takeaways-from-russian-authorities-takedown-of-revil>

<https://www.cnn.com/2021/12/16/tech/kronos-ransomware-attack/index.html>

<https://www.ajg.com/us/-/media/files/gallagher/us/collections/ransomware-crops-up-in-the-food-agriculture-industry.pdf>

<https://www.csoonline.com.cdn.ampproject.org/c/s/www.csoonline.com/article/3647756/how-to-prioritize-and-remediate-vulnerabilities-in-the-wake-of-log4j-and-microsofts-patch-tuesday-b.amp.html>

<https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure>

<https://www.zdnet.com/article/microsoft-and-mcafee-headline-newly-formed-ransomware-task-force/>

<https://www.us-cert.gov/ncas/tips/ST04-001>

<https://cybersecurityventures.com/50-cybersecurity-titles-that-every-job-seeker-should-know-about/>

<https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework>

<https://digitalguardian.com/blog/innovation-diversity-cybersecurity>

<https://techcrunch.com/2022/01/03/connecting-the-dots-on-diversity-in-cybersecurity-recruitment/>

<https://www.uscybersecurity.net/history/>

<https://www.msn.com/en-us/money/news/a-diverse-cybersecurity-team-can-help-alleviate-the-talent-shortage/ar-AANie4U>

Week 3: February 14th

Class Discussion:

- a. Cyber Terms
- b. Kaseya (case study/cyber attack)
- c. ILOVEYOU Virus (case study)
- d. Cyber Attack Chain
- e. Review for Quiz #1

<https://niccs.us-cert.gov/about-niccs/glossary#A>

<https://www.sans.org/security-resources/glossary-of-terms/>

<https://www.imperva.com/cyber-threat-attack-map/>

<https://therecord.media/an-interview-with-blackmatter-a-new-ransomware-group-thats-learning-from-the-mistakes-of-darkside-and-revil/>

<https://www.solarium.gov/public-communications/2021-annual-report-on-implementation>

<https://www.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html>

<https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/>

<https://www.msspalert.com/cybersecurity-breaches-and-attacks/kaseya-rmm-cyberattack-warning/>

<https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-takes-additional-steps-to-prevent-evictions-as-the-delivery-of-emergency-rental-assistance-continues-to-increase/>

<https://gizmodo.com/kaseya-is-making-its-customers-sign-non-disclosure-agre-1847356517>

Huda, Chapters 1&2 (focus on pages 16-17), Chapters 3- 4

***Week 4: February 21st (NO CLASS – President’s Day)**

Reading:

<https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

<https://www-cnb-com.cdn.ampproject.org/c/s/www.cnb-com/amp/2019/12/23/stuxnet-target-equifax-worst-breaches-of-2010s.html>

<https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf>

Huda, (cont’d) Chapters 5 - 7

Week 5: February 28th (Quiz 1 – in class)

Class Discussion:

- a. Cyber Attacks in Hollywood
- b. Threat Attack Map
- c. Cyber Attacks and Trends
 - i. Sectors
 - ii. Attribution
 - iii. Motive
- d. Notable and Historic Cyber Attacks

Reading:

https://www.willistowerswatson.com/en-US/Insights/2021/08/hacking-back?utm_source=slipcase&utm_medium=affiliate&utm_campaign=slipcase

<https://healthitsecurity.com/features/this-years-largest-healthcare-data-breaches>

Huda, Chapter 12

Week 6: March 7th

Class Discussion:

- a. Introduction to Standards and Frameworks (NIST & CRC)
- b. Additional Defenses/Offenses

Reading:

<https://www.nist.gov/cyberframework>

<https://www.cisecurity.org/controls/> (Please download and read the controls)

https://www.crowdstrike.com/blog/lessons-from-past-cyber-operations-against-ukraine/?utm_source=bmbu&utm_medium=soc&utm_campaign=Blogs&blaid=2560793

Week 7: March 14th (Assignment 1 – in class)

Class Discussion:

- a. Regulations
 - i. GDPR, HIPPA, FERPA, DFS, CCPA, NY Shield Act
- b. Litigation

Reading:

<https://gdpr.eu/what-is-gdpr/>

<https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (look over list)

<https://studentprivacy.ed.gov/?src=fpco>

https://www.dfs.ny.gov/system/files/documents/2019/01/cyber_memo_12212018.pdf

<https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf>

<https://oag.ca.gov/privacy/ccpa>

<https://lewisbrisbois.com/privacy/US>

<https://business.cch.com/CybersecurityPrivacy/eyemed-settlement.pdf>

Week 8: March 21st

1. Class Discussion
 - a. Ransomware
 - i. Variants
 - ii. Attribution
 - iii. Merck, Maersk, JBS
 - b. Silk Road

Reading:

<https://www.bbc.com/news/business-57423008>

<https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperRansomware.pdf>

<https://www.fireeye.com/blog/threat-research/2020/03/they-come-in-the-night-ransomware-deployment-trends.html>

<https://go.recordedfuture.com/hubfs/reports/cta-2020-0213.pdf>

<https://www.cnn.com/2019/10/08/business/ransomware-attacks-trnd/index.html>

<https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority>

<https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

<https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war>

<https://innovationinsurancegroup.com/merck-vs-ace/>

[https://www.wired.com/2015/05/silk-road-untold-story/ \(Part 1 & 2\)](https://www.wired.com/2015/05/silk-road-untold-story/)

Week 9: March 28th Midterm – In Class & Prepare for NCFTA Visit

Week 10: April 4th – Visit to NCFTA (The National Cyber-Forensics and Training Alliance @ One Penn Plaza) (Tentative)

Week 11: April 11th

Class Discussion:

- a. Cyber Insurance
 - i. Types of Coverage
 - ii. Underwriting Applications and Relevant Data
- b. Cyber Insurance Litigation
- c. Underwriting and Cyber Risk Prediction

Reading:

<https://www.ibm.com/downloads/cas/ZBZLY7KL>

<https://www.beazley.com/usa.html#> (please explore the site)

https://policies.dppl.com/policy.php?policy_number=BBR-5A8ED7A3-8OEF#pagenav-ag-1

<https://www.insurancejournal.com/news/international/2019/01/15/514558.htm>

<https://www.natlawreview.com/article/reasons-communicating-clearly-your-insurer-regarding-scope-coverage-purchasing-cyber>

<https://www.databreachninja.com/wp-content/uploads/sites/63/2019/01/MONDELEZ-INTERNATIONAL-INC-Plaintiff-v-ZURICH-AMERICAN-INSURANCE-COMPANY-Defenda.pdf>

<https://www.marshmma.com/blog/cyber-insurance-rates-could-rise-50-in-2021>

<https://www.natlawreview.com/article/four-new-cyber-war-exclusions-lloyd-s-market-association>

<https://www.gllawgroup.com/wp-content/uploads/2022/01/Cyber-and-Silent-Cyber-Coverage.pdf>

***Week 12: April 18th (NO CLASS)**

Reading:

<https://www.bitcoin.com/bitcoin.pdf>

<https://gemini.com/learn>

<https://www.nasdaq.com/articles/a-blockchain-primer%3A-what-is-it-whos-using-it-when-itll-go-mainstream-and-how-to-invest-in>

Week 13: April 25th (Assignment 2 - in class)

Class Discussion:

- a. Cryptocurrency
- b. Blockchain

Week 14: May 2nd (Last in-person class)

Class Discussion

- a. Threat Intel & Information Sharing
- b. Predictions for 2023

Reading:

<https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=8789>

https://www2.deloitte.com/content/dam/insights/us/articles/3749_Industry4-0_cybersecurity/DUP_Industry4-0_cybersecurity.pdf

<https://www.acq.osd.mil/cmmc/index.html>

<https://www.fbi.gov/investigate/cyber>

<https://www.infragard.org/> (review site)

<https://www.recordedfuture.com/threat-intelligence/>

Week 15: May 9th

Work on Final Paper

Week 16: May 16th

Work on Final Paper

Week 17: May 23rd – FINAL PAPER DUE

Grading Policy –

- 10% - 1 quiz
- 20% - Discussion Forum:
 - At least 10 posts in the Discussion Forums and 2/10 posts must be in response to another student's post to create a dialogue
- 20% - Midterm
- 20% - 2 Assignments (each assignment is 10%)
- 20% - Final Exam
- 10% - Participation, in-class group work, attendance

Communication

Preferred method to contact instructor for urgent / non-urgent matters: email

Secondary method to contact instructor for urgent/non – urgent matters: text/call

Response time to outreach for urgent/non-urgent matters – same day

Academic Integrity/Honesty Policy

Hunter College regards acts of academic dishonesty (e.g., plagiarism, cheating on examinations, obtaining unfair advantage, and falsification of records and official documents) as serious

offenses against the values of intellectual honesty. The College is committed to enforcing the CUNY Policy on Academic Integrity and will pursue cases of academic dishonesty according to the Hunter College Academic Integrity Procedures.

ADA Policy

In compliance with the American Disability Act of 1990 (ADA) and with Section 504 of the Rehabilitation Act of 1973, Hunter College is committed to ensuring educational parity and accommodations for all students with documented disabilities and/or medical conditions. It is recommended that all students with documented disabilities (Emotional, Medical, Physical, and/or Learning) consult the Office of AccessABILITY, located in Room E1214B, to secure necessary academic accommodations. For further information and assistance, please call: (212) 772- 4857 or (212) 650-3230.

Hunter College Policy on Sexual Misconduct

In compliance with the CUNY Policy on Sexual Misconduct, Hunter College reaffirms the prohibition of any sexual misconduct, which includes sexual violence, sexual harassment, and gender-based harassment retaliation against students, employees, or visitors, as well as certain intimate relationships. Students who have experienced any form of sexual violence on or off campus (including CUNY-sponsored trips and events) are entitled to the rights outlined in the Bill of Rights for Hunter College.

a. Sexual Violence: Students are strongly encouraged to immediately report the incident by calling 911, contacting NYPD Special Victims Division Hotline (646-610-7272) or their local police precinct, or contacting the College's Public Safety Office (212-772-4444).

b. All Other Forms of Sexual Misconduct: Students are also encouraged to contact the College's Title IX Campus Coordinator, Dean John Rose (jtrose@hunter.cuny.edu or 212-650-3262) or Colleen Barry (colleen.barry@hunter.cuny.edu or 212-772-4534) and seek complimentary services through the Counseling and Wellness Services Office, Hunter East 1123.

CUNY Policy on Sexual Misconduct Link:

<http://www.cuny.edu/about/administration/offices/la/Policy-on-SexualMisconduct-12-1-14-with-links.pdf>

Diversity & Inclusivity Policy

It is critical in every learning environment to create not only a spirit of tolerance, but a strong feeling of support, encouragement and celebration amongst students and faculty who are come to the course with distinct backgrounds, ethnicity, race, religion, sexual orientation, sexuality, disability, age, socioeconomic status, nationality, gender identity and culture. Everyone is welcome equally, and it is my intent to conduct this course with equality in mind and respect for each other's differences. I will require the same of all students, and in the event something is said or done in this classroom that causes discomfort or offense, please let me know immediately, as it will always be treated with the attention it deserves. Please do approach any

concerns with the assumption that there was no intent to cause any harm or negative feelings and with an open mind toward prompt resolution.

Syllabus Change Policy

Any changes to the syllabus will be provided with enough advance notice depending on the change. Changes will be announced on Blackboard as well as through email and during class if appropriate.