K792 PhD Course
Security, Privacy, and Trust in e-Business
Winter 2023 Course Outline

Information Systems Area
DeGroote School of Business
McMaster University

COURSE OBJECTIVE

This advanced PhD course is designed to discuss security, privacy, and trust issues in e-business. Security, privacy, and trust are critical for the success and survival of electronic commerce. Today new technologies and new applications will not be widely adopted until it can be demonstrated that the security of the underlying ICT infrastructure and the privacy of information being processed are both protected. Only then will users trust and therefore use these innovations and then, and only then, will the developers and society as a whole reap the benefits of the innovation. In this course students will learn the technical, legal, and managerial aspects of security assurance, privacy protection, and trust building through paper reading, seminar presentation and class discussion. Students will also learn how to do research by writing a research paper. MBA students may attend this course with specific permission from the instructor.

INSTRUCTOR AND CONTACT INFORMATION

Dr. Yufei Yuan
Instructor
yuanyuf@mcmaster.ca
Office: DSB A204
Office Hours:
By appointment.
Tel: (905) 525-9140 x23982

Class Location: Virtual class through Zoom meetings
Meeting Time: Wednesdays 2:30 - 5:30 pm.
Classroom: DSB 321
Course Website: http://avenue.mcmaster.ca
Zoom meeting:
https://mcmaster.zoom.us/j/96388753025?pwd=NlBBSEV0ZjBvV1NxeVZUVVk5WkdSQT09

COURSE ELEMENTS

Credit Value:	3	Team skills:	Yes	IT skills:	Yes	Global:	Yes
Avenue:	Yes	Verbal skills:	Yes	Numeracy:	No	Political:	No
Participation:	Yes	Written skills:	Yes	Innovation:	Yes	Social:	No

COURSE DESCRIPTION

This advanced PhD course is designed to discuss issues on security, privacy and trust. Students will learn the technical, legal, and managerial aspects of security, privacy, and trust through paper reading, seminar presentation, and class discussion. Each student will be required to make two seminar presentations and write a research paper on a selected topic. MBA students may attend this course with specific permission from the instructor.

LEARNING OUTCOMES

Upon completion of this course, students will be able to learn the following topics:

- The issues on security, privacy, and trust
- Risk analysis and security management
- Security protection technologies
- Privacy concerns and privacy protection
- Trust building and trust repair

REQUIRED COURSE MATERIALS AND READINGS

Lecture notes posted on the course web site

OPTIONAL COURSE MATERIALS AND READINGS

Reference Papers

Security

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management*, 51(1), 138-151.

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: A review. International Journal of u-and e-Service, *Science and Technology*, 2(3), 13-28.

Bowyer, K. W. (2004). Face recognition technology: security versus privacy. *IEEE Technology and society magazine*, 23(1), 9-19.

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), 719-731.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10).

Cram, W. A., D’Arcy, J., & Proudfoot, J. G. (2019). Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly, 43*(2).

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2(6-10), 71.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, 20(1), 79-98.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, 28(2), 203-236.

Han, X., Wang, L., & Fan, W. (2021). Is hidden safe? Location protection against machine-learning prediction attacks in social networks. *MIS Quarterly*, 45(2), 821-858.

Hunt, R. (2001). Technological infrastructure for PKI and digital certification. Computer communications, 24(14), 1460-1471.

Jensen, M. L., Wright, R. T., Durcikova, A., & Karumbaiah, S. (2022). Improving Phishing Reporting Using Security Gamification. *Journal of Management Information Systems*, 39(3), 793-823.

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, 106, 102267.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, 64(5), 659-671.

Li, H., Yoo, S., & Kettinger, W. J. (2021). The roles of IT strategies and security investments in reducing organizational security breaches. *Journal of Management Information Systems*, 38(1), 222-245.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS Quarterly*, 71-90.

Liu, C. W., Huang, P., & Lucas Jr, H. C. (2020). Centralized IT decision making and cybersecurity breaches: Evidence from US higher education institutions. *Journal of Management Information Systems*, 37(3), 758-787.

Ng, K. C., Zhang, X., Thong, J. Y., & Tam, K. Y. (2021). Protecting against threats to information security: An attitudinal ambivalence perspective. *Journal of Management Information Systems*, 38(3), 732-764.

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Res*earch, 20(1), 121-139.

Samtani, S., Chai, Y., & Chen, H. (2022). Linking exploits from the dark web to known vulnerabilities for proactive cyber threat intelligence: An attention-based deep structured semantic model. *MIS Quarterly*, 46(2), 911-946.

Schuetz, S. W., Benjamin Lowry, P., Pienta, D. A., & Bennett Thatcher, J. (2020). The effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems*, 37(3), 723-757.

Sen, R., Verma, A., & Heim, G. R. (2020). Impact of cyberattacks by malicious hackers on the competition in software markets. *Journal of Management Information Systems*, 37(1),

191-216.

Silic, M., & Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems*, 37(1), 129-161.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM Sigmis Database, 38*(1), 60-80.

Snider, K. L., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, 7(1), tyab019.

Soomro, Z.A., Shah, M.H. and Ahmed, J., (2016), Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), pp.215-225.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS quarterly*, 441-469.

Talati, R., & Chaudhari, P. (2022, April). The Road-ahead for E-healthcare 4.0: A Review of Security Challenges. In *2022 1st International Conference on Informatics* (ICI) (pp. 208-213). IEEE.

Turel, O., He, Q., & Wen, Y. (2021). Examining the neural basis of information security policy violations: a noninvasive brain stimulation approach. MIS Quarterly, 45(4), 1715-44.

Vance, A., Eargle, D., Eggett, D., Straub, D. W., & Ouimet, K. (2022). Do security fear appeals work when they interrupt tasks? A multi-method examination of password strength. MIS Quarterly, 46(3).

Venter, H. S., & Eloff, J. H. (2003). A taxonomy for information security technologies. *Computers & Security*, 22(4), 299-307.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102.

Yoo, C. W., Goo, J., & Rao, H. R. (2020). Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. *MIS Quarterly*, 44(2).

Wang, W., Yuan, Y., & Archer, N. (2006). A contextual framework for combating identity theft. *IEEE security & privacy*, 4(2), 30-38.

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, 169-187.

Privacy

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science,* 347(6221), 509-514.

Chan, E. Y., & Saqib, N. U. (2021). Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Computers in Human Behavior*, 119, 106718.

Dinev, T. (2014), "Why would we care about Privacy?" *European Journal of Information systems*, (2014) 23, 97-102.

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. *Information Systems Research,* 26(4),

639-655.

Head, M. and Yuan, Y. (2001), "Privacy Protection in Electronic Commerce – A Theoretical Framework," *Human Systems Management*, Vol. 20, 2001, pp. 149-160

Liu, B., Ding, M., Shaham, S., Rahayu, W., Farokhi, F., & Lin, Z. (2021). When machine learning meets privacy: A survey and outlook. *ACM Computing Surveys* (CSUR), 54(2), 1-36.

Pavlou, P. A. (2011), "State of the Information Privacy Literature: Where Are We Now And Where Should We Go?" *MIS Quarterly*, December 2011, pp. 977-988.

Pollach, I. (2007), What's Wrong With Online Privacy Policies? *Communications of the ACM*, September 2007, Vol. 50, No. 9, pp. 103- 108.

Sanyal, P., Menon, N., & Siponen, M. (2021). An Empirical Examination of the Economics of Mobile Application Security. *MIS Quarterly*, 45(4).

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, 35(4), 989-1016.

Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. *Ai & Society*, 37(1), 167-175.

Tang, Z., Hu, Y., & Smith, M. D. (2008). Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. *Journal of Management Information Systems*, 24(4), 153-173.

Vimalkumar, M., Sharma, S. K., Singh, J. B., & Dwivedi, Y. K. (2021). 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior*, 120, 106763.

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. IEEE Communications Surveys & Tutorials.

Zalmanson, L., Oestreicher-Singer, G., & Ecker, Y. (2022). The Role of Social Cues and Trust in Users' Private Information Disclosure. *MIS Quarterly*, 46(2), 1109-1134.

Zhang, N. A., Wang, C. A., Karahanna, E., & Xu, Y. (2022). Peer privacy concern: conceptualization and measurement. *MIS Quarterly*, 46(1).

Trust

Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems*, 71, 62-77.

Bedué, P., & Fritzsche, A. (2021). Can we trust AI? An empirical investigation of trust requirements and guide to successful AI adoption. *Journal of Enterprise Information Management*.

Benbasat, I., Gefen, D., & Pavlou, P. A. (2010). Introduction to the special issue on novel perspectives on trust in information systems. *MIS Quarterly*, 34(2), 367-371.

Dimoka, A. (2010). What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study. *MIS Quarterly*, 373-396.

Ebrahimi, S., Ghasemaghaei, M., & Benbasat, I. (2022). The Impact of Trust and Recommendation Quality on Adopting Interactive and Non-Interactive Recommendation Agents: A Meta-Analysis. *Journal of Management Information Systems*, 39(3), 733-764.

Ferrario, A., Loi, M., & Viganò, E. (2019). In AI we trust incrementally: a multi-layer model of trust to analyze human-artificial intelligence interactions. *Philosophy & Technology*, 1-17.

Gillath, O., Ai, T., Branicky, M. S., Keshmiri, S., Davison, R. B., & Spaulding, R. (2021). Attachment and trust in artificial intelligence. *Computers in Human Behavior*, 115, 106607.

Glikson, E., & Woolley, A. W. (2020). Human trust in artificial intelligence: Review of empirical research. *Academy of Management Annals*, 14(2), 627-660.

Grabner-Kräuter, S., & Kaluscha, E. A. (2003). Empirical research in on-line trust: a review and critical assessment. *International Journal of Human-Computer Studies*, 58(6), 783-812.

Guo, W., Straub, D., Zhang, P., & Cai, Z. (2021). How Trust Leads to Commitment on Microsourcing Platforms: Unraveling the Effects of Governance and Third-Party Mechanisms on Triadic Microsourcing Relationships. *MIS Quarterly*, 45(3).

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic commerce research and applications*, *29*, 50-63.

Höddinghaus, M., Sondern, D., & Hertel, G. (2021). The automation of leadership functions: Would people trust decision algorithms?. *Computers in Human Behavior*, 116, 106635.

Jacovi, Alon, Ana Marasović, Tim Miller, and Yoav Goldberg. Formalizing trust in artificial intelligence: Prerequisites, causes and goals of human trust in AI. In Proceedings of the *2021 ACM conference on fairness, accountability, and transparency*, pp. 624-635. 2021.

Jennings, W., Stoker, G., Valgarðsson, V., Devine, D., & Gaskell, J. (2021). How trust, mistrust and distrust shape the governance of the COVID-19 crisis. *Journal of European Public Policy*, 28(8), 1174-1196.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision support systems*, 44(2), 544-564.

Li, F., Pieńkowski, D., van Moorsel, A., & Smith, C. (2012). A holistic framework for trust in online transactions. *International Journal of Management Reviews*, 14(1), 85-103.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research*, 13(3), 334-359.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS quarterly*, 105-136.

Pennycook, G., Bear, A., Collins, E. T., & Rand, D. G. (2020). The implied truth effect: Attaching warnings to a subset of fake news headlines increases perceived accuracy of headlines without warnings. *Management Science*.

Sherchan, W., Nepal, S., & Paris, C. (2013). A survey of trust in social networks. *ACM Computing Surveys* (CSUR), 45(4), 47.

Shin, D. (2021). The effects of explainability and causability on perception, trust, and acceptance: Implications for explainable AI. *International Journal of Human-Computer Studies*, 146, 102551.

Vereschak, O., Bailly, G., & Caramiaux, B. (2021). How to evaluate trust in AI-assisted decision making? A survey of empirical methodologies. Proceedings of *the ACM on*

Human-Computer Interaction, 5(CSCW2), 1-39.

Xiao, B., & Benbasat, I. (2011). Product-related deception in e-commerce: a theoretical perspective. *MIS Quarterly*, 35(1), 169-196.

EVALUATION

Learning in this course results primarily from lecturing, reading, in-class discussion, specific topic presentation, and research paper. All work will be evaluated on an individual basis. Your final grade will be calculated as follows:

Components and Weights

Class participation	Attend and join class discussion, search and share information	10%
Specific Topic Presentation	Each student will make one presentation on existing research in selected topics (20%) and one presentation to discuss your own research ideas (10%)	30%
Research paper	Require the quality of journal or conference submission	60%
Total		100%

Grade Conversion

At the end of the course your overall percentage grade will be converted to your letter grade in accordance with the following conversion scheme.

Letter Grade	Percent	Points
A+	90-100	12
A	85-89	11
A-	80-84	10
B+	77-79	9
B	73-76	8
B-	70-72	7
F	0-69	0

COMMUNICATION AND FEEDBACK

Students that are uncomfortable in directly approaching an instructor regarding a course concern may send a confidential and anonymous email to the respective Area Chair or Associate Dean:

http://mbastudent.degroote.mcmaster.ca/contact/anonymous/

Students who wish to correspond with instructors or TAs directly via email must send messages that originate from their official McMaster University email account. This protects the confidentiality and sensitivity of information as well as confirms the identity of the student. Emails regarding course issues should NOT be sent to the Administrative Assistant.
Instructors are encouraged to conduct an informal course review with students by Week #4 to allow time for modifications in curriculum delivery. Instructors should provide evaluation feedback for at least 10% of the final grade to students prior to Week #8 in the term.

ACADEMIC INTEGRITY

You are expected to exhibit honesty and use ethical behaviour in all aspects of the learning process. Academic credentials you earn are rooted in principles of honesty and academic integrity.

Academic dishonesty is to knowingly act or fail to act in a way that results or could result in unearned academic credit or advantage. This behaviour can result in serious consequences, e.g. the grade of zero on an assignment, loss of credit with a notation on the transcript (notation reads: “Grade of F assigned for academic dishonesty”), and/or suspension or expulsion from the university.

It is your responsibility to understand what constitutes academic dishonesty. For information on the various types of academic dishonesty please refer to the Academic Integrity Policy, located at:

www.mcmaster.ca/academicintegrity

The following illustrates only three forms of academic dishonesty:

1. Plagiarism, e.g. the submission of work that is not one’s own or for which other credit has been obtained.
2. Improper collaboration in group work.
3. Copying or using unauthorized aids in tests and examinations

AUTHENTICITY/PLAGIARISM DETECTION

Some courses may use a web-based service (Turnitin.com) to reveal authenticity and ownership of student submitted work. For courses using such software, students will be expected to submit their work electronically either directly to Turnitin.com or via an online learning platform (e.g. A2L, etc.) using plagiarism detection (a service supported by Turnitin.com) so it can be checked for academic dishonesty.

Students who do not wish their work to be submitted through the plagiarism detection software must inform the Instructor before the assignment is due. No penalty will be assigned to a student who does not submit work to the plagiarism detection software.

All submitted work is subject to normal verification that standards of academic integrity have been upheld (e.g., on-line search, other software, etc.). For more details about McMaster's use of Turnitin.com please go to www.mcmaster.ca/academicintegrity.

ON-LINE PROCTORING

Some courses may use online proctoring software for tests and exams. This software may require students to turn on their video camera, present identification, monitor and record their computer activities, and/or lock/restrict their browser or other applications/software during tests or exams. This software may be required to be installed before the test/exam begins.

CONDUCT EXPECTATIONS

As a McMaster student, you have the right to experience, and the responsibility to demonstrate, respectful and dignified interactions within all of our living, learning and working communities. These expectations are described in the Code of Student Rights & Responsibilities (the "Code"). All students share the responsibility of maintaining a positive environment for the academic and personal growth of all McMaster community members, **whether in person or online**.

It is essential that students be mindful of their interactions online, as the Code remains in effect in virtual learning environments. The Code applies to any interactions that adversely affect, disrupt, or interfere with reasonable participation in University activities. Student disruptions or behaviours that interfere with university functions on online platforms (e.g. use of Avenue 2 Learn, WebEx or Zoom for delivery), will be taken very seriously and will be investigated. Outcomes may include restriction or removal of the involved students' access to these platforms.

MISSED ACADEMIC WORK

Missed Mid-Term Examinations / Tests / Class Participation

Please do not use the online McMaster Student Absence Form (MSAF) as this is for Undergraduate students only. The MBA program will not accept an MSAF.

When students miss regularly scheduled term work which contributes 10% or more to the final grade, for legitimate reasons as determined by the Student Experience – Academic Office (SEAO), the activity necessary to compensate for the missed work will be determined by the course instructor. The compensatory activities assigned will vary with the nature of the course and the missed requirement. They include, but are not restricted to, an alternative assignment, a rescheduled midterm exam, or re-weighting the marks for the missed component to other mark components. Documentation explaining such missed work must be provided to the SEAO within five (5) working days of the scheduled date for completion of the work.

Acceptable reasons for missed work, along with the Petition for Missed Term Work and the MBA Student McMaster University Student Health Certificate, can be found on the DeGroote

MBA Student website (mbastudent.degroote.mcmaster.ca). Please direct any questions about acceptable documentation to the MBA Academic Advisors (askmba@mcmaster.ca).

University policy states that a student may submit a maximum of three (3) Petition for Missed Term Work per academic year, after which the student must meet with the Director of the program.

If term work is missed without an approved reason, students will receive a grade of zero (0) for that component.

Missed Final Examinations

Students must be available for the duration of the posted exam period regardless of their personal exam schedule. This is to ensure student availability throughout the entire exam period in the event that an exam must be rescheduled due to unforeseen circumstances (university closure, power outage, storm policy, etc.). A student who misses a final examination without valid reason will receive a mark of 0 on the examination.

Students who have missed a final exam for a valid reason can apply to the SEAO to write a deferred examination by submitting an Application for Deferring a Final Exam with supporting documentation. The application must be made within five days of the scheduled exam date or the application may be denied.

The Application for Deferring a Final Exam and the MBA Student McMaster University Student Health Certificate can be found on the DeGroote MBA Current Student website (mbastudent.degroote.mcmaster.ca)

Deferred examination privileges, if granted, are normally satisfied during the examination period at the end of the following semester. In select cases, the deferred examination may be written at a time facilitated by the SEAO and agreed to by the course instructor.

Requests for a second deferral or rescheduling of a deferred examination will not be considered.

Failure to write an approved deferred examination at the pre-scheduled time will result in a zero (0) mark for that examination, except in the case of exceptional circumstances where documentation has been provided and approved. Upon approval, no credit will be given for the course, and the notation N.C. (no credit) will be placed on the student's transcript.

ACADEMIC ACCOMMODATION FOR STUDENTS WITH DISABILITIES

Student Accessibility Services (SAS) offers various support services for students with disabilities. Students are required to inform SAS of accommodation needs for course work at the outset of term. Students must forward a copy of such SAS accommodation to the instructor normally, within the first three (3) weeks of classes by setting up an appointment with the instructor. If a student with a disability chooses NOT to take advantage of an SAS accommodation and chooses to sit for a regular exam, a petition for relief may not be filed after the examination is complete. The SAS website is:

http://sas.mcmaster.ca

ACADEMIC ACCOMMODATION FOR RELIGIOUS, INDIGENOUS OR SPIRITUAL OBSERVANCES (RISO)

Students requiring academic accommodation based on religious, indigenous or spiritual observances should follow the procedures set out in the RISO policy. Students should submit their request to their Faculty Office ***normally within 10 working days*** of the beginning of term in which they anticipate a need for accommodation or to the Registrar's Office prior to their examinations. Students should also contact their instructors as soon as possible to make alternative arrangements for classes, assignments, and tests.

COPYRIGHT AND RECORDING

Students are advised that lectures, demonstrations, performances, and any other course material provided by an instructor include copyright protected works. The Copyright Act and copyright law protect every original literary, dramatic, musical and artistic work, including lectures by University instructors.

The recording of lectures, tutorials, or other methods of instruction may occur during a course. Recording may be done by either the instructor for the purpose of authorized distribution, or by a student for the purpose of personal study. Students should be aware that their voice and/or image may be recorded by others during the class. Please speak with the instructor if this is a concern for you.

POTENTIAL MODIFICATION TO THE COURSE

The instructor and university reserve the right to modify elements of the course during the term. The university may change the dates and deadlines for any or all courses in extreme circumstances. If either type of modification becomes necessary, reasonable notice and communication with the students will be given with explanation and the opportunity to comment on changes. It is the responsibility of the student to check their McMaster email and course websites weekly during the term and to note any changes.

RESEARCH USING HUMAN SUBJECTS

ONLY IF APPLICABLE

Research involving human participants is premised on a fundamental moral commitment to advancing human welfare, knowledge, and understanding. As a research intensive institution, McMaster University shares this commitment in its promotion of responsible research. The fundamental imperative of research involving human participation is respect for human dignity and well-being. To this end, the University endorses the ethical principles cited in the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans:
http://www.pre.ethics.gc.ca

McMaster University has mandated its Research Ethics Boards to ensure that all research investigations involving human participants are in compliance with the Tri-Council Policy Statement. The University is committed, through its Research Ethics Boards, to assisting the research community in identifying and addressing ethical issues inherent in research, recognizing that all members of the University share a commitment to maintaining the highest possible standards in research involving humans.

If you are conducting original research, it is vital that you behave in an ethical manner. For example, everyone you speak to must be made aware of your reasons for eliciting their responses and consent to providing information. Furthermore, you must ensure everyone understands that participation is entirely voluntary. Please refer to the following website for more information about McMaster University's research ethics guidelines:

http://reo.mcmaster.ca/

Organizations that you are working with are likely to prefer that some information be treated as confidential. Ensure that you clarify the status of all information that you receive from your client. You **MUST** respect this request and cannot present this information in class or communicate it in any form, nor can you discuss it outside your group. Furthermore, you must continue to respect this confidentiality even after the course is over.

ACKNOWLEDGEMENT OF COURSE POLICIES

Your registration and continuous participation (e.g. on A2L, in the classroom, etc.) to the various learning activities of MBA XXXX will be considered to be an implicit acknowledgement of the course policies outlined above, or of any other that may be announced during lecture and/or on A2L. **It is your responsibility to read this course outline, to familiarize yourself with the course policies and to act accordingly.**

Lack of awareness of the course policies **cannot be invoked** at any point during this course for failure to meet them. It is your responsibility to ask for clarification on any policies that you do not understand.

ONLINE COURSE DELIVERY

In this course we will meet in class as well as using online teaching tools to conduct leaning activities. Students should be aware that when they access the electronic components of this course, private information such as first and last names, usernames for the McMaster e-mail accounts, and program affiliation may become apparent to all other students in the same course. The available information is dependent on the technology used. Continuation in this course will be deemed consent to this disclosure.

If you have any questions or concerns about such disclosure, please discuss this with the course instructor.

LEARNING ACTIVITIES	DELIVERY	DESCRIPTION	TOOL(S)
Live Lectures	In class	3 hr. live session; opportunity to elaborate on content, present challenges, engage discussion	Every week during class time
Self-Study	Asynch	Read lecture note posted in Avenue and specified research papers	**Avenue to Learn** At your own time over the week
Discussion	Asynch	Participate in online discussion forum. Post and answer questions, share papers	**Avenue to Learn** At your own time over the week
Student Seminar presentation and Discussions	In class	Student in class seminar presentation and discussion	Selected week during class time

CLASS SCHEDULE (SUBJECT TO POSSIBLE MODIFICATION)

Week	Date	Topic	Readings/Assignments
1	Jan. 11	Introduction to security, privacy, and trust issues	Choo (2011), Von Solms & Van Niekerk (2013), Wang et al (2006), Head & Yuan (2001), Kim et al (2008).
2	Jan. 18	Risk analysis and security management	Siponen & Oinas-Kukkonen (2007), Straub & Welke (1998), Baskerville, et al. (2014).
3	Jan. 25	Information security technologies Blockchain and biometrics	Venter & Eloff (2003), Bhattacharyya et al (2009), Crosby, et al. (2016), Hunt (2001), Bowyer (2004).
4	Feb. 1	Security behaviour studies	D'Arcy et al. (2009), Guo et al. (2011), Liang & Xue (2009), Yoo et al. (2020), Vance et al. (2022).

5	Feb. 8	Selected research review topics	Student presentation
6	Feb. 15	Privacy basics	Acquisti et al. (2015), Smith, et al. (2011), Dinev (2014).
7	Feb 20-25	Spring break	No class
8	Mar. 1	Privacy research	Pavlou (2011), Tang et al. (2008), Dinev et al. (2015), Vimalkumar et al. (2021).
9	Mar. 8	Selected research review topics	Student presentation
10	Mar. 15	Trust basics	McKnight, et al. (2002), Grabner-Kräuter & Kaluscha (2003), Dimoka (2010), Pavlou, et al. (2007),
11	Mar. 22	Trust research	Xiao & Benbasat (2011), Bansal & Zahedi (2015), Glikson & Woolley (2020), Jennings et al (2021).
12	Mar. 29	Discuss of your research idea	Student presentation
13	Apr. 5	Research paper presentation	Research paper due

Specific Topic Presentation Guidelines

Objective: To make a seminar presentation that addresses a current issue on security, privacy and trust in electronic business. Each student will be required to make two presentations. One is mainly a literature review for existing studies in a specific topic (one hour), another is to discuss your research ideal for your research paper (half hour).

Topic Selection: Following are the suggested topics of student presentation. Each topic may be presented by up to two students. Each student can select one topic from the list. You may select a subtopic based on the recommendation or your own interests. Please make sure your subtopics are not overlap with each other.

Topic	**Subtopics**
Specific topics on security	• Cyber security • Intrusion and fraud detection • Identity issues with AI technology • Effectiveness of security measures • Security breach • Blockchain
Specific topics on privacy protection	• Privacy protection in healthcare • Privacy protection in social media • Privacy issues with AI technology • Privacy issues in big data and cloud computing • Privacy paradox
Specific topics on trust	• Trust building in e-business • Trust repair • Trust in social media • Trust towards AI enabled service • The relationship between security, privacy, and trust

Presentation and paper sharing: For each subtopic, please prepare a PowerPoint presentation and provide a copy of most valuable papers (three to four) and a list of references for students to share.

Research Paper Guidelines

Objective:

To write a research paper that addresses a current issue on security, privacy and trust in electronic business. The topic of your research paper can overlap with your seminar presentation but should be more in depth study. Students are expected to work more closely with the instructor for possible conference or journal publication.

Topic Selection:

The topic of your research paper may be on any contemporary issue relating to security, privacy, and identity theft in electronic business. A one page proposal of your research topic must be handed in by the third week. You may build a theoretical framework or evaluate existing technologies. Your topic should not cover too broad a field, since your report will not be long enough to do justice to the material and will result in a poor mark. For example, "Network Security" is too broad as a topic, while "Hackers on Internet" is considerably narrower, and "Intrusion detection techniques" has an even sharper focus.

Guidelines:

1. Since many students will not have much experience within their selected topic, most of the material for the research paper will be gathered from literature surveys. The University library has many books and journals which may be of use, and your instructor may also help you in your search if you are short of material. Your best sources of information will likely be the World Wide Web and the electronic libraries available in the Innis Room. **Do not** consult your instructor until you have looked at topics from this source. Books are good sources of material, but to obtain up-to-date material, journals should also be consulted.

2. Since the purpose of this research paper is to show that you have studied a particular topic area well, do not simply repeat information you find in your literature review. In particular, beware of the unbridled enthusiasm on many topics often appearing in the popular press. This may be a mask to cover a lack of facts. You should not consider yourself as a reporter, but as an analyst. Present your own views on the material gathered, since this develops your ability to think logically and creatively. Remember, marks are given for originality.

3. Your report must be typed. It should be a minimum of 20 (maximum of 35) double spaced 8 x 11 typewritten pages, (not including references, figures, and appendices). However, you will not be penalized if you can put forward a good presentation in less than 20 pages.

4. Your report should be written in a concise, crisp, business-like style such as would be used in writing a report for high level management. Try to use diagrams and tables to get your point of view across and to "dress up" your report's appearance.

5. Your report should include the following sections:

   - A cover page which includes the title, the course name and number, the date, and the author’s' name.

   - Abstract: The abstract should cover the most important points presented in your paper as well as any conclusions that should be derived from the report.

- Introduction: This section includes background material to bring the reader "up to speed" before launching into the main thrust of your report. It should also briefly discuss a general outline of the report which follows.

- Report body: The body of the report should be broken into reasonably sized sections on various aspects of the topic under consideration. Each section should be numbered and given an appropriate heading.

- Major findings and conclusions: This section should reflect the important results that the reader should have learned from the paper.

- References: You must show several references from more advanced literature (you may also reference the popular press, but it may tend towards uncritical enthusiasm). Guidelines for reference format are provided below.

- Appendices: If appropriate, appendices should be included after your reference section.

6. Jargon should not be used unless the words are carefully defined when they are first used in your report. In general, make sure you carefully define your topic, assuming that potential readers may have little or no background knowledge within the area.

7. References to gender should not appear in the paper, unless referring to an actual person. A minimal use of "he or she" is permitted instead of "he" or "she", but it is normally possible to eliminate such references entirely. For example, consider the following sentence: "The manager will normally rely on his secretary to perform her work as rapidly as possible, regardless of whether or not she has access to a word processor". A statement like this one will cost you marks in your paper, so consider the following statement as a replacement: "Managers will normally rely on their secretaries to work as rapidly as possible, regardless of whether they have access to word processors". There are other ways to achieve this effect, but this should demonstrate what is desired.

8. Sources for your material must be referenced. If you develop original material in your report, be sure to substantiate the grounds upon which you build your arguments, through references to other published material or personal communications. All of your reference material should be referred to by numbers in square brackets, corresponding to numbers used in your reference list at the end of your paper. In your reference section, references should be listed in alphabetic order of the first author's last name. An example of proper reference format is shown below:

   Cofta, P. (2007), *Trust, Complexity and Control: Confidence in a Convergent World*, Wiley &Sons, 2007.

   Pollach, I. (2007), What’s Wrong with Online Privacy Policies? *Communications of the ACM*, September 2007, Vol. 50, No. 9, pp. 103- 108.

9. Short footnotes may be used, provided that they are referenced on the same page with a special symbol such as a dagger or an asterisk. Longer footnotes should be included as appendices, to avoid breaking the continuity of the presentation.

10. Figures or tables should be numbered and should appear as soon as possible after they are referenced in the paper. However, if a large number of tables or figures are referenced in one place, it is best to move all the tables and/or figures to the end of the report.

11. Appendices should have titles and be numbered using Roman numerals.

12. All pages of the report, except the title page, should be numbered.

13. Equations should be numbered if they are referred to elsewhere in the report.

14. Grammar, spelling, sentence and paragraph structure are important. A good general reference which may be useful is the Harbrace College Handbook published by Longman Canada Limited. Other references which contain helpful sections on business report writing style are:

    - Ewing, E.W. (1979), Writing For Results, New York: Wiley, 1979.
    - Himstreet, W.C., and W.M. Baty (1977) Business Communications, Belmont, California : Wadsworth, 1977.
    - Smith, R.S. (1976), Written Communications for Data Processing, New York: Van Nostrand, 1976.
    - Weiss, A. (1977), Write What You Mean, New York: Amacom, 1977.

15. PowerPoint presentation. You should prepare and submit (email me) your PowerPoint presentation document one day before the scheduled presentation time. You will have 25 minutes presentation followed by 10 minutes discussion.