

# CS 773/873: Data Mining and Security

Fall 2026

**Course Credit:** 3 Credit Hours  
**Semester:** Fall 2026  
**Modality:** In-Person  
**Meeting Days:** Tuesdays and Thursdays (TR)  
**Meeting Time:** 9:30 AM–10:45 AM  
**Location:** Monarch Hall, Room 2113

## 1. Instructor Information

**Instructor:** Dr. Mohammad GhasemiGol  
**Email:** [mghasemi@odu.edu](mailto:mghasemi@odu.edu)  
**Office:** Monarch Hall 2123B  
**Office Hours:** By appointment (in person or virtual)

## Canvas

Canvas will be used as the primary course management system. The syllabus, lecture materials, readings, assignments, announcements, presentation instructions, rubrics, and other course resources will be posted on Canvas. Students are responsible for checking Canvas regularly for course updates.

## 2. Course Description

Introduction to data mining; algorithms including Naive Bayes, Decision Trees and Rules, Association Rules, Linear Classification, and Clustering; Cross Validation, Lift Charts, ROC Curves; SVM, Bayesian Networks, K-means Clustering; Data Transformation; PCA; Ensemble Learning; application of data mining to security and privacy including authentication, authorization, and intrusion detection; Privacy-Preserving Data Mining.

**Course Credit:** 3 Credit Hours.

This course provides a graduate-level introduction to data mining methods with an emphasis on their applications to cybersecurity and privacy. The course covers the complete data mining pipeline, including data preprocessing, feature engineering, dimensionality reduction, clustering, classification, model evaluation, ensemble learning, and advanced machine learning methods.

Students will study fundamental algorithms including Naive Bayes, decision trees and rules, linear classifiers, support vector machines (SVM), Bayesian networks, K-means clustering, association rules, principal component analysis (PCA), and ensemble learning. Particular attention will be given to evaluating data mining systems using cross-validation, precision and recall, ROC and precision-recall curves, lift analysis, and other metrics appropriate for highly imbalanced security datasets.

The course connects these foundations to security and privacy applications, including intrusion and anomaly detection, malware and malicious activity classification, authentication and authorization analytics, privacy-preserving data mining, adversarial machine learning, and machine unlearning.

Advanced topics will introduce students to emerging applications of deep learning, transformers, large language models (LLMs), explainable AI, and AI agents in cybersecurity. Students will critically analyze current research, conduct experiments using security datasets, and develop an original semester research project.

### 3. Prerequisites

**Prerequisites:** CS 471 and CS 455, or CS 555.

Students are expected to enter the course with the programming, algorithmic, and computer security background provided by these prerequisite courses. Python will be used for selected data mining exercises, demonstrations, and research experiments; prior Python experience is helpful but is not an additional formal prerequisite.

This is a graduate-level course intended for Master's and Ph.D. students. Students are expected to have basic programming skills and familiarity with fundamental concepts in algorithms, probability, statistics, and computer science. Prior experience with Python is helpful for course experiments and research projects.

No prior advanced coursework in machine learning or data mining is required; the course develops the necessary foundations before progressing to advanced topics.

### 4. Course Objectives

By the end of the course, students will be able to:

1. Understand the fundamental concepts and workflow of data mining and machine learning.
2. Prepare, transform, and engineer features from complex security datasets.
3. Apply clustering and unsupervised learning techniques to discover patterns and anomalies in security data.
4. Design and implement classification models using classical machine learning algorithms.
5. Select appropriate evaluation metrics and critically assess machine learning systems for cybersecurity applications.
6. Apply dimensionality reduction, feature selection, and ensemble learning techniques.
7. Understand adversarial threats against machine learning systems, including evasion, poisoning, and backdoor attacks.
8. Analyze privacy risks associated with machine learning and apply privacy-preserving approaches.
9. Understand emerging concepts such as machine unlearning and their implications for cybersecurity and privacy.
10. Critically evaluate advanced AI techniques, including deep learning, LLMs, and AI agents, for cybersecurity applications.
11. Read, critique, and synthesize state-of-the-art research in data mining and security.
12. Design, conduct, evaluate, and communicate graduate-level research.

## 5. Course Outcomes

Students completing this course will gain:

- A strong foundation in classical and advanced data mining methods.
- Practical experience applying machine learning to cybersecurity datasets.
- An understanding of the challenges associated with noisy, high-dimensional, and highly imbalanced security data.
- The ability to critically evaluate security-oriented machine learning systems rather than relying solely on accuracy.
- Research-level exposure to adversarial machine learning, privacy-preserving machine learning, and machine unlearning.
- Exposure to modern AI approaches for cybersecurity, including LLMs and agentic AI.
- Improved scientific writing, experimentation, critical analysis, and presentation skills.

## 6. Course Materials

**Required Textbook:** None.

### 6.1 Recommended Resources

Course materials will primarily consist of instructor-provided notes, tutorials, datasets, and research papers.

Recommended references include:

- Pang-Ning Tan, Michael Steinbach, Anuj Karpatne, and Vipin Kumar, *Introduction to Data Mining*.
- Jiawei Han, Micheline Kamber, and Jian Pei, *Data Mining: Concepts and Techniques*.
- Trevor Hastie, Robert Tibshirani, and Jerome Friedman, *The Elements of Statistical Learning*.
- Christopher Bishop, *Pattern Recognition and Machine Learning*.
- Scikit-learn documentation and tutorials.
- NIST publications relevant to AI, privacy, and cybersecurity.
- MITRE ATT&CK and MITRE ATLAS.
- Current academic papers from IEEE S&P, USENIX Security, ACM CCS, NDSS, RAID, IEEE TDSC, ACM TOPS, IEEE Transactions on Information Forensics and Security, Computers & Security, and leading data mining and machine learning venues.

## 7. Expanded Topics

### 7.1 Module 1: Foundations of Data Mining and Security

- Course overview and research expectations

- What is data mining?
- Data mining vs. machine learning vs. AI
- Data mining workflow
- Supervised, unsupervised, and semi-supervised learning
- Features, labels, instances, and datasets
- Types of security data
- Network traffic and flow data
- Authentication and access logs
- Endpoint and system events
- Malware and threat data
- Data quality and missing data
- Class imbalance in cybersecurity
- Introduction to security data mining applications
- Open research problems and research topic selection

## **7.2 Module 2: Data Transformation, Feature Engineering, and Dimensionality Reduction**

- Data cleaning and preprocessing
- Numerical and categorical features
- Encoding categorical variables
- Normalization and standardization
- Feature construction
- Feature selection
- Correlation and redundant features
- Curse of dimensionality
- Dimensionality reduction
- Principal Component Analysis (PCA)
- Visualization of high-dimensional data
- Feature engineering for network and cybersecurity data
- Data leakage and common preprocessing mistakes

### 7.3 Module 3: Clustering and Unsupervised Learning

- Fundamentals of unsupervised learning
- Similarity and distance measures
- K-means clustering
- Hierarchical clustering
- Density-based clustering and DBSCAN
- Selecting the number of clusters
- Cluster validation
- Association rule mining
- Frequent patterns
- Introduction to anomaly and outlier detection
- Applications to attack discovery
- User and entity behavior analysis
- Malware and attack family clustering
- Discovering previously unknown attack patterns

### 7.4 Module 4: Classification

- Fundamentals of supervised classification
- Naive Bayes
- Decision trees
- Classification and decision rules
- Logistic and linear classification
- Support Vector Machines (SVM)
- Bayesian networks
- Hyperparameters and model complexity
- Overfitting and underfitting
- Bias-variance considerations
- Applications to intrusion detection
- Malware classification
- Phishing and malicious URL detection
- Authentication and access-control analytics

## 7.5 Module 5: Model Evaluation and Selection

- Training, validation, and testing
- Cross-validation
- Confusion matrix
- Accuracy and error rate
- Precision and recall
- F1 score
- Sensitivity and specificity
- False-positive and false-negative rates
- ROC curves and AUC
- Precision-recall curves
- Lift charts
- Threshold selection
- Evaluating highly imbalanced datasets
- Cost-sensitive evaluation
- Model selection and hyperparameter tuning
- Reproducibility and experimental design
- Why high accuracy can be misleading in cybersecurity

## 7.6 Module 6: Ensemble and Advanced Learning

- Motivation for ensemble learning
- Bagging
- Random Forest
- Boosting
- AdaBoost
- Gradient boosting
- Introduction to XGBoost concepts
- Combining multiple detectors
- Advanced anomaly detection
- Introduction to neural networks
- Deep learning concepts
- Representation learning
- Applications of ensemble and deep learning methods to cybersecurity

## 7.7 Module 7: Adversarial ML, Privacy, and Machine Unlearning

### Security of Machine Learning

- Threat models for machine learning
- Adversarial examples
- Evasion attacks
- Data poisoning
- Backdoor attacks
- Model extraction
- Robustness and adversarial defenses

### Privacy of Machine Learning

- Privacy-preserving data mining
- Privacy threats in machine learning
- Membership inference
- Model inversion
- Differential privacy
- Federated learning
- Privacy-security-utility tradeoffs

### Machine Unlearning

- Why should machine learning models forget?
- Exact vs. approximate unlearning
- Retraining vs. efficient unlearning
- Removing private or sensitive training data
- Removing poisoned or compromised training samples
- Verification of forgetting
- Security and privacy implications of machine unlearning
- Open research challenges

**Special Guest Lecture:** Machine Unlearning and its Applications to Cybersecurity, IBM Research/IBM guest speaker.

## 7.8 Module 8: Modern AI and Emerging Security Research

- Deep learning for security analytics
- Representation learning for cybersecurity
- Transformers
- Foundation models
- Large Language Models (LLMs)
- Security applications of LLMs
- LLM-assisted security operations
- LLMs for threat analysis and detection
- Explainable AI for security
- Trustworthy AI
- Security of LLM-based systems
- Prompt injection and adversarial attacks
- AI agents and agentic cybersecurity
- Autonomous attack and defense
- Emerging research challenges and future directions

## 8. Course Expectations

### 8.1 Instructor Expectations

The instructor will:

- Provide clear explanations of course concepts and research topics.
- Provide clear guidelines, expectations, and grading criteria for assignments and presentations.
- Make course materials and relevant research resources available through Canvas.
- Provide constructive and timely feedback on student work.
- Apply grading criteria consistently and fairly.
- Be available to discuss course material, research ideas, and student progress during scheduled appointments.
- Encourage an inclusive, respectful, and research-oriented learning environment.

### 8.2 Student Expectations

Students are expected to:

- Attend and actively participate in class meetings.
- Complete assigned readings and preparation before class.
- Participate thoughtfully and respectfully in technical discussions.
- Read and critically analyze assigned research papers.
- Complete research activities, presentations, and written work by their assigned deadlines.
- Conduct experiments carefully and report methods and results accurately.
- Provide constructive feedback during student research presentations.
- Follow the ODU Honor Code and all applicable academic integrity requirements.
- Communicate with the instructor promptly when academic or logistical issues affect course participation.

## 9. Evaluation and Grading

This course is research-oriented. Students are expected to engage deeply with data mining techniques as well as current academic research at the intersection of machine learning, cybersecurity, and privacy.

The semester research workflow progresses from topic exploration and literature review to problem formulation, experimentation, evaluation, presentation, and final technical writing.

All major components will be evaluated according to detailed rubrics provided on the course site.

### 9.1 Assignments and Assessments

- **Literature Review and Review Presentation (25%).** Students will critically review recent research related to an approved topic, identify limitations and research gaps, and present their findings to the class.
- **Research Presentation (25%).** Students will present their original semester research, including the research problem, proposed approach, experimental methodology, results, limitations, and future directions.
- **Final Research Paper (40%).** Students will prepare an IEEE-format research paper describing their semester research project. The paper should resemble a conference-style technical paper and include appropriate experimental evaluation and references.
- **Participation and Research Discussions (10%).** Students are expected to participate actively in lectures, research discussions, paper discussions, peer feedback, and guest lectures.
- **Optional Assignments and Research Contributions (up to +20%).** Additional hands-on exercises, experimental activities, paper reviews, or research contributions may provide opportunities for bonus credit. Details will be announced through Canvas.

Specific deadlines, presentation schedules, submission instructions, and rubrics will be provided through Canvas.

## 9.2 Evaluation Breakdown

| Component                                       | Weight |
|-------------------------------------------------|--------|
| Review Presentation (Literature Review)         | 25%    |
| Research Presentation                           | 25%    |
| Research Paper (IEEE Format)                    | 40%    |
| Participation & Discussions                     | 10%    |
| Assignments & Research Contributions (Optional) | +20%   |

## 10. Grading Scale

Letter grades for CS 773/873 are based on the following percentage scale:

### CS 773

| Percentage | Grade |
|------------|-------|
| 100–93     | A     |
| 92–88      | A-    |
| 87–84      | B+    |
| 83–80      | B     |
| 79–75      | B-    |
| 74–70      | C+    |
| 69–65      | C     |
| 64–60      | C-    |
| 59–55      | D+    |
| 54–50      | D     |
| 49–45      | D-    |
| < 45       | F     |

### CS 873

| Percentage | Grade |
|------------|-------|
| 100–96     | A     |
| 95–93      | A-    |
| 92–89      | B+    |
| 88–85      | B     |
| 84–80      | B-    |
| 79–76      | C+    |
| 75–72      | C     |
| 71–68      | C-    |
| 67–64      | D+    |
| 63–60      | D     |
| 59–55      | D-    |
| < 55       | F     |

## 11. Research Process and Expectations

### 11.1 Topic Selection

During the first two weeks of the semester, each student must identify a research topic related to data mining, machine learning, cybersecurity, or privacy.

Topics must be:

- Relevant to course themes.
- Researchable within the semester timeframe.
- Supported by appropriate datasets or experimental resources.
- Approved by the instructor.

Students should begin identifying recent papers from leading conferences and journals and developing an understanding of the problem space.

## 11.2 Review Presentation: Literature Review

Students will conduct a structured review of recent research related to their selected topic.

Students should:

- Review recent research papers, with more than 10 papers recommended.
- Identify the major approaches used in the literature.
- Compare datasets, features, algorithms, and evaluation methodologies.
- Summarize major findings.
- Critically examine limitations.
- Identify unresolved challenges and research gaps.
- Propose possible directions for improvement or extension.

The objective is not simply to summarize papers, but to identify a meaningful research opportunity.

## 11.3 Research Development and Experimentation

Following the literature review, each student will refine one research question or idea based on novelty, feasibility, and instructor feedback.

Students are expected to:

- Formulate a clear research question.
- Identify appropriate datasets and baselines.
- Implement algorithms, models, or experimental prototypes.
- Select appropriate evaluation metrics.
- Conduct experiments.
- Compare results against relevant baselines.
- Analyze results rather than simply report numerical performance.
- Document negative as well as positive results when scientifically relevant.
- Iteratively refine the proposed approach.

## 11.4 Research Presentation

The final research presentation will simulate a conference-style technical presentation.

Students should present:

- Motivation and problem definition
- Research gap

- Proposed approach
- Dataset and experimental design
- Baselines and evaluation metrics
- Results and analysis
- Limitations
- Future research opportunities

### **11.5 Final Research Paper**

Students will submit a technical research report in IEEE conference format.

The paper should include:

- Abstract
- Introduction and motivation
- Related work
- Problem definition
- Proposed method
- Dataset and experimental setup
- Evaluation methodology
- Results
- Discussion
- Limitations
- Conclusion and future work
- References

Students are encouraged to develop projects with sufficient novelty and experimental rigor to potentially be refined into publishable research.

## **12. Tentative Course Schedule – Fall 2026**

The course meets on Tuesdays and Thursdays. The schedule may be adjusted based on class progress, research presentations, guest-speaker availability, and emerging research topics.

| Week | Dates             | Module              | Topics / Activities                                                                                                                                                            | Research / Deliverables                   |
|------|-------------------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| 1    | Aug. 25 & 27      | Module 1            | Course introduction and expectations; introduction to data mining and security; data mining vs. ML/AI; supervised and unsupervised learning; security data and applications.   | Research project overview.                |
| 2    | Sept. 1 & 3       | Module 1            | Data mining workflow; datasets, instances, features, and labels; security datasets; data quality, missing values, and class imbalance. Discussion of potential research areas. | Research topic selection.                 |
| 3    | Sept. 8 & 10      | Module 2            | Data preprocessing and transformation; categorical encoding; normalization and standardization; feature engineering for cybersecurity data.                                    | Initial paper collection.                 |
| 4    | Sept. 15 & 17     | Module 2            | Feature selection; correlation; curse of dimensionality; PCA and dimensionality reduction; security-data case study.                                                           | Literature review development.            |
| 5    | Sept. 22 & 24     | Module 3            | Unsupervised learning; similarity and distance measures; K-means and hierarchical clustering; clustering security events and network traffic.                                  | Research problem refinement.              |
| 6    | Sept. 29 & Oct. 1 | Module 3            | DBSCAN; cluster validation; association rules; anomaly and outlier detection; unknown attack discovery.                                                                        | Literature review preparation.            |
| 7    | Oct. 6 & 8        | Module 4            | Classification fundamentals; Naive Bayes; decision trees and classification rules; cybersecurity classification examples.                                                      | Review presentation preparation.          |
| 8    | Oct. 13 & 15      | Module 4            | <b>Oct. 13: Fall Break – No Class.</b> Oct. 15: Linear/logistic classification and introduction to SVM.                                                                        | Research gap identification.              |
| 9    | Oct. 20 & 22      | Module 4 / Research | SVM; Bayesian networks; overfitting and model complexity. <b>Student Literature Review Presentations.</b>                                                                      | Literature review presentation.           |
| 10   | Oct. 27 & 29      | Module 5            | Model evaluation; train/validation/test design; cross-validation; confusion matrix; accuracy, precision, recall, F1, sensitivity, and specificity.                             | Finalize research question and baselines. |
| 11   | Nov. 3 & 5        | Module 5            | <b>Nov. 3: Election Day – No Class.</b> Nov. 5: ROC/AUC, precision-recall curves, lift, threshold selection, class imbalance, and cost-sensitive evaluation.                   | Experimentation phase.                    |
| 12   | Nov. 10 & 12      | Module 6            | Ensemble learning; bagging; Random Forest; boosting; AdaBoost and gradient boosting; introduction to advanced anomaly detection and deep learning.                             | Experiments and analysis.                 |

| Week              | Dates        | Module         | Topics / Activities                                                                                                                                                                                                                                                                                | Research / Deliverables                                      |
|-------------------|--------------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| 13                | Nov. 17 & 19 | Module 7       | Adversarial machine learning: evasion, poisoning, adversarial examples, backdoors, model extraction; privacy attacks including membership inference and model inversion.                                                                                                                           | Research progress and refinement.                            |
| 14                | Nov. 24 & 26 | Module 7       | Nov. 24: Privacy-preserving data mining; differential privacy; federated learning; introduction to machine unlearning. <b>Nov. 26: Thanksgiving Holiday – No Class.</b>                                                                                                                            | Complete core experiments.                                   |
| 15                | Dec. 1 & 3   | Modules 7 & 8  | <b>Guest Lecture: Machine Unlearning and Cybersecurity (IBM, tentative).</b> Modern AI for cybersecurity: deep learning, transformers, LLMs, explainable AI, foundation models, and agentic cybersecurity. Course wrap-up and emerging research directions. <b>Student Research Presentations.</b> | Final research presentation.                                 |
| Final Exam Period | Dec. 5–11    | Research Paper | <b>Final student research paper/report.</b>                                                                                                                                                                                                                                                        | Final IEEE-format research paper due as specified on Canvas. |

### 13. Attendance and Participation Policy

Regular attendance and active participation are strongly encouraged. This is a research-oriented graduate course in which in-class discussions, technical demonstrations, paper discussions, research feedback, guest lectures, and student presentations are important components of the learning experience.

Students who must miss a class should notify the instructor in advance when possible and are responsible for reviewing course materials and announcements posted on Canvas.

Quality participation includes thoughtful questions, constructive feedback, engagement with assigned readings, and respectful participation in research discussions.

### 14. Late and Make-Up Work Policy

Students are expected to submit assignments and research deliverables by the deadlines posted on Canvas. If circumstances beyond a student's control may prevent timely completion of an assignment or presentation, the student should contact the instructor as early as possible.

Extensions or make-up opportunities may be granted when appropriate based on the circumstances. Unless an extension has been approved, late work may be subject to a grading penalty as specified in the assignment instructions.

Missed presentations will normally be rescheduled only when the absence is approved by the instructor or otherwise covered by University policy.

## 15. Use of Artificial Intelligence Tools

Artificial intelligence tools are relevant to the subject matter of this course and may be used responsibly when their use supports learning and research rather than replacing the student's own intellectual contribution.

Unless otherwise specified for an individual assignment, students may use generative AI and AI-assisted tools for activities such as brainstorming, exploring alternative approaches, programming assistance, debugging, language improvement, and organizing ideas.

Students remain fully responsible for all submitted work. In particular:

- Students must understand and be able to explain any material, analysis, code, or methodology included in their submissions.
- AI-generated information must be independently verified for correctness.
- AI tools must not be used to fabricate references, experimental results, datasets, analyses, or other research evidence.
- Substantive use of AI tools in research papers, assignments, code, or presentations must be disclosed when appropriate and according to assignment instructions.
- Students must comply with applicable privacy, confidentiality, copyright, licensing, and data-use requirements when providing information to external AI systems.
- The student's research question, scientific reasoning, experimental analysis, conclusions, and original research contribution must represent the student's own intellectual work.

The instructor may establish additional restrictions on AI use for specific assignments or activities. Using AI in a manner inconsistent with these instructions or presenting AI-generated work as one's own may constitute an academic integrity violation.

## 16. Incomplete Grades

A grade of "I" indicates assigned work yet to be completed in a given course, or absence from a required final assessment, and is assigned only upon instructor approval of a student request.

The "I" grade may be awarded only in exceptional circumstances beyond the student's control. University policies and deadlines governing incomplete grades apply.

## 17. Student Accountability and Academic Integrity

The Office of Student Accountability and Academic Integrity oversees the administration of the student conduct system as outlined in the Old Dominion University Code of Student Conduct. Students are expected to maintain the highest standards of academic integrity in all activities associated with this course.

Academic integrity violations include, but are not limited to, cheating, plagiarism, fabrication, and facilitating academic misconduct.

### 17.1 Cheating

Using unauthorized assistance, materials, study aids, software, AI tools, or other information in an academic exercise when such use has not been authorized by the instructor.

### 17.2 Plagiarism

Using another person's language, ideas, code, results, figures, or other original material without appropriate acknowledgment.

### 17.3 Fabrication

Inventing, altering, manipulating, or falsifying data, citations, experimental results, or other information in an academic exercise.

### 17.4 Facilitation

Helping another student commit or attempt to commit an academic integrity violation.

### 17.5 Research Integrity

Because this course includes graduate-level research, particular attention will be given to research integrity. Students must accurately document datasets, experimental procedures, algorithms, software, results, and sources.

Fabricating or manipulating experimental results, inventing citations, misrepresenting the performance of a model, selectively altering results without scientific justification, or representing another person's work as one's own constitutes a serious academic integrity violation.

### 17.6 Honor Pledge

By attending Old Dominion University, students accept the responsibility to abide by the Honor Pledge:

**“I pledge to support the honor system of Old Dominion University. I will refrain from any form of academic dishonesty or deception, such as cheating or plagiarism. I am aware that as a member of the academic community it is my responsibility to turn in all suspected violations of the Honor Code. I will report to a hearing if summoned.”**

### 17.7 Honor Code

Students are expected to follow the Old Dominion University Honor Code:

“We, the students of Old Dominion University, aspire to be honest and forthright in our academic endeavors. Therefore, we will practice honesty and integrity and be guided by the tenets of the Monarch Creed. We will meet the challenges to be beyond reproach in our actions and our words.

We will conduct ourselves in a manner that commands the dignity and respect that we also give to others.”

## **18. University Email and Communication**

The Old Dominion University email system is an official means for University communication. Students are responsible for activating and regularly monitoring their ODU email accounts.

Course announcements and other important communications may be sent through ODU email or Canvas. Students are expected to check both regularly.

Students should communicate with the instructor using their official ODU email account.

## **19. Withdrawal**

A syllabus constitutes an agreement between the student and the instructor regarding course requirements and expectations. Participation in this course indicates acceptance of its teaching focus, requirements, and policies.

Students are responsible for reviewing University deadlines for adding, dropping, or withdrawing from courses and should consult the ODU Academic Calendar and Office of the University Registrar for official deadlines.

## **20. Privacy of Student Information**

Old Dominion University recognizes its responsibility to protect student information and educational records. Student records are protected in accordance with the Family Educational Rights and Privacy Act (FERPA) and applicable University policies.

Students should also exercise appropriate care when using security datasets in research projects and must comply with applicable privacy, ethical, licensing, and data-use requirements.

## **21. Educational Accessibility and Accommodations**

Old Dominion University is committed to ensuring equal access to all qualified students with disabilities in accordance with applicable law and University policy.

If you experience a disability that will impact your ability to access any aspect of this course, please provide the instructor with an accommodation letter from the Office of Educational Accessibility (OEA) so that appropriate accommodations can be arranged.

Students who anticipate barriers to learning or assessment but do not currently have an accommodation letter are encouraged to contact OEA to determine whether academic accommodations are appropriate.

The Office of Educational Accessibility is located in Student Success Center 1021 and can be reached at 757-683-4655. Additional information is available through the ODU Office of Educational Accessibility.

## **22. Discrimination and Harassment**

Old Dominion University is committed to equal access to programs, facilities, admission, and employment for all persons and to maintaining an environment free from unlawful discrimination and harassment.

Students are expected to conduct themselves respectfully and professionally during lectures, research discussions, group activities, presentations, and online course interactions.

Applicable requirements are described in ODU University Policy #1005 and related University policies.

## **23. Copyright**

All instructor-provided course materials, including lecture slides, assignments, demonstrations, recordings, datasets prepared for the course, and other materials, are protected by applicable copyright law.

Students may use course materials and make copies for their own educational purposes as needed. Unauthorized distribution, posting, sharing, recording, sale, or uploading of course materials without the instructor's express permission is prohibited.

## **24. Syllabus and Schedule Changes**

The course schedule is tentative and may be adjusted during the semester because of class progress, guest-speaker availability, University closures, weather-related events, emerging research topics, or other circumstances.

Changes to topics, readings, assignments, deadlines, or course activities will be communicated through Canvas. If substantial changes to the syllabus are necessary, an updated version will be provided to students.