**MS Data Privacy Courses and Descriptions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Prefix** | **Number** | **Course Title** | **Credit Hours** |
| **CLI** | **730** | **Global Privacy Law** | **3** |
| This course examines US and international privacy laws, exploring how different legal approaches regulate data collection, usage, and protection across jurisdictions. Particular focus will be on the EU’s GDPR, China’s Personal Information Protection Law, US federal surveillance laws, relevant Supreme Court decisions, the California Consumer Privacy Act, and the Colorado Privacy Act, among others. | | | |
|  |  |  |  |
| **CLI** | **732** | **Privacy Threats** | **3** |
| This course examines a wide range of threats to data privacy, including both criminal activities and legally sanctioned practices. Students will explore privacy risks associated with government and corporate surveillance, the data brokerage industry, digital voyeurism, consent fatigue, and the normalization of oversharing, among other topics. A key focus will be the policy tradeoffs between security and privacy, innovation and privacy, and profit and privacy. | | | |
|  |  |  |  |
| **CLI** | **734** | **Digital Rights** | **3** |
| This course explores the intersection of human rights and digital technologies, examining how fundamental freedoms are shaped by the online environment. The course covers issues like internet access as human rights, platform governance, and digital censorship. It also addresses copyright law’s impact on digital rights, including fair use, content moderation, and open-access initiatives. Together, these topics contribute to a broader normative understanding of privacy and privacy law. | | | |
|  |  |  |  |
| **HIMS** | **745** | **Cyber Ethics** | **3** |
| This course provides a foundation in ethical reasoning while examining the ethical challenges posed by emerging technologies, cybersecurity, and the widespread collection of personal digital data. Topics include digital rights, algorithmic bias, professional responsibilities, and ethical dilemmas in technology development and implementation. Students will explore major ethical theories and apply them to real-world challenges in cyberspace. | | | |
|  |  |  |  |
| **HIMS** | **746** | **Data Governance** | **3** |
| This course explores the principles and practices of data governance, focusing on the planning, oversight, and control of data management within organizations. Topics include data lifecycle management, regulatory compliance, and strategies for ensuring data integrity and security. Students will examine how effective governance supports an organization’s broader data management strategy, from data creation and storage to retrieval and disposal. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Prefix** | **Number** | **Course Title** | **Credit Hours** |
| **INFA** | **702** | **Data Privacy** | **3** |
| Students will examine the many different conceptions of what privacy is and the many ways in which privacy can be harmed, with a major focus on data privacy. This course provides analysis of privacy practices, privacy by design, technologies, compliance, management and engineering, personally identifiable information (PII), privacy principles, and important privacy regulations. Famous privacy incidents will be utilized as case studies to provide context for the curriculum. Students will learn about international privacy regulations, management frameworks and design methodologies, as well as privacy engineering and privacy enhancing technologies (PET). Assessment will be a combination of hands-on exercises, classroom discussions and a 2-part Privacy Impact Assessment “use case.”, and a data privacy research project of their choice. | | | |
|  |  |  |  |
| **INFA** | **722** | **Data Privacy Management** | **3** |
| This course explores computational techniques for releasing information in such a way that data privacy cannot be violated and provides a formal framework for privacy-enhancing technologies and models of privacy protection.  It explores privacy enhancements from economic, legal and policy perspectives and introduces cutting-edge, privacy-preserving frameworks for data-mining systems. | | | |
|  |  |  |  |
| **INFA** | **726** | **Data Privacy Technology** | **3** |
| This course examines privacy technologies important to data collecting, processing, sharing, and storage.  It explains the purpose and value of engineering Privacy by Design (PbD) principles into products and services.  It examines technologies for email, mobile platforms, online media, online baking and digital health.  The course addresses technical areas including identity and access management while identifying and mitigating privacy harms through data minimization, de-identification, and data anonymization technologies. Prerequisite(s): INFA 702 | | | |
|  |  |  |  |
| **INFA** | **744** | **AI and Data Privacy** | **3** |
| AI and Data Privacy is a non-technical course exploring how artificial intelligence (AI) impacts data privacy, focusing on ethical, legal, organizational, and technological considerations. Students will examine privacy challenges such as algorithmic bias, data protection regulations, and privacy-enhancing techniques like differential privacy and federated learning. The course covers AI-driven surveillance risks, compliance strategies, and governance frameworks, equipping students to analyze and implement AI solutions with privacy-first principles. | | | |
|  |  |  |  |
| **INFA** | **748** | **Digital Forensics for Data Privacy** | **3** |
| This non-technical course examines the identification, acquisition, preservation, and analysis of digital evidence while addressing legal, regulatory, and compliance challenges related to data privacy. Students will explore forensic tools, evidence handling, and recovery techniques across various digital environments, with a focus on privacy implications such as data minimization, encryption, and anonymization. Through case studies and discussions, students will develop a foundational understanding of forensic methodologies while assessing ethical, legal, and privacy risks in digital investigations. | | | |
|  |  | Subtotal | 30 |