

Information Security, Privacy and Policy, Minor

Lujo Bauer, Director and Faculty Advisor

Minor in Information Security, Privacy and Policy

Interdisciplinary minor offered by both CIT and SCS

There is a growing demand for security and privacy experts, and increasing interest among CMU undergraduates in taking security and privacy courses. Security and privacy expertise is an asset in a variety of careers outside, not just in computer science, but also in areas that include business, management, and law. In addition, the policy side of security and privacy is becoming increasingly important and employers are interested in hiring people with an understanding of relevant policy issues, especially in the privacy and security area.

This minor is for undergraduate students across the university who are interested in policy issues related to security and privacy, including those who are planning careers in security/privacy as well as those who plan to focus their careers in other areas. The curriculum has been designed to accommodate students from any major as long as they have taken at least one introductory-level college programming course (such as 15-110 or 15-112).

After completing this minor, students will have a good understanding of how to identify potential security and privacy risks and relevant legal and policy issues; a working understanding of security topics such as cryptography, authentication, and Internet security protocols; as well as broad knowledge of several security- and privacy-related areas as they pertain to the design, development, deployment and management of technologies in a variety of practical contexts (e.g., Web, mobile, Internet of Things, social media, crypto currencies).

Admission

Students are not required to apply to enroll in this minor to start the required courses. However, they are encouraged to consult with the minor director on their elective course selection. In addition, students doing the independent study option must get approval from the minor director prior to enrolling in their independent study course. Finally, students must contact the minor director to certify their completion of the minor.

Curriculum

Minimum units required for minor **48 units**

Students are required to take five courses to complete this minor with a minimum of 48 units.

Introductory Security Course

	Units
17-331 Information Security, Privacy and Policy in the Age of AI	12

Students who have taken 15-213 Introduction to Computer Systems may substitute 15-330 Introduction to Computer Security/18-330 Introduction to Computer Security

Privacy and Policy Course

17-333 Privacy Policy, Law, and Technology	9
--	---

Students may substitute a 12-unit version of this course: 19-608, 17-333, or 95-818.

Privacy Electives

Complete a minimum of 9 units:

19-534/17-334 Usable Privacy and Security	9
19-602/17-702 Current Topics In Privacy Seminar	3
17-731 Foundations of Privacy	12

Technology and Policy Electives

Complete a minimum of 9 units:

19-211 Ethics and Policy Issues in Computing	9
--	---

17-562	Computer and AI Law	9
19-101	Introduction to Engineering and Public Policy	12
19-403	Policies of Wireless Systems	12
19-639	Policies of the Internet	12
84-387	Remote Systems and the Cyber Domain in Conflict	9

Crosslisted courses are also allowed.

Additional Approved Elective

Students must complete an additional elective of 9 units or more. Students may choose an additional privacy elective or technology policy elective from the list above, or the one of the following security electives:

15-316	Software Foundations of Security and Privacy	9
15-356	Introduction to Cryptography	12
19/17-303	Cryptocurrencies, Blockchains and Applications	Var.
19-534/17-334	Usable Privacy and Security	9
18-334	Network Security	12
18-435	Foundations of Blockchains	12

Students who have the necessary prerequisites may choose any approved elective from the SCS or ECE security and privacy undergraduate concentration. Check with the minor program director to determine which category of elective each course will fulfill.

Students should be careful to choose electives for which they have appropriate prerequisites. New elective options are expected as more courses are offered. Students may petition to count a course not on this list as an elective. Students should request permission *before* taking a course that is not on this list. Students may not count multiple electives that overlap substantially.

Optional Project: Subject to approval by the minor director, students may optionally count towards one of the elective requirements 9 units of an independent study or research project course in the security or privacy area, under the supervision of a faculty member in any department.

In order to receive credit towards the minor, students must submit a brief project proposal to their project advisor and to the minor director and have it approved prior to conducting the project. Depending on the topic of the project, the minor director may approve credits counting towards privacy electives, technology policy electives, security electives, or some combination of these. Students may work individually, with other undergraduates, or as part of project teams with graduate students or research staff. Students involved in a group project must identify specific project components for which they are responsible. In addition, they must submit a final project report to their project advisor and the minor director that includes a literature review and describes the work they completed. Students working on a group project must each submit their own final report, which should also situate their contribution in the context of the larger project. Note, students are expected to work approximately 1 hour per week for each unit of project in which they are enrolled (e.g. 9 units = 9 hours/week of project work).

Double Counting: At most 2 of the courses used to fulfill the minor requirements may be counted towards any other undergraduate major or minor program. This rule does not apply to courses counted for general education requirements.