Information Security and Policy, Minor

The minor in Information Security and Policy will prepare students to navigate the complex landscape of today's data-driven world by exploring fundamental aspects of information security, privacy, and provenance, with the ultimate goal of influencing organizational and societal policies. Students will learn the philosophical foundations of ethical hacking, key considerations for securing data and systems, digital forensics, and state-of-the-art tools to protect critical data in application spaces such as medicine and politics. This minor moves beyond traditional cybersecurity in order to formulate best policies and practices that highlight human needs in a world where data often comes first.

Students pursuing a minor in Information Security and Policy are required to:

- Complete 28 credits.
- Complete a minimum of 12 credits in the minor that are not duplicated by the major or any other minor.
- Complete 6 credits upper division credits in the minor in residence at Chapman.
- Complete a minimum of 12 upper division credits in the minor.
- Take all courses in the minor for a letter grade.
- Achieve a 2.000 cumulative GPA in the minor and a 2.000 GPA for all upper-division coursework in the minor.

technical core (22 credits)

CPSC 230 - Computer Science I

CPSC 230 - Computer Science I

Prerequisite, MATH 100. Students are introduced to problem-solving methods and algorithm development through an interactive and easy-to-learn programming language, Python. Letter grade with Pass/No Pass option. (Offered every semester.) **3 credits**

CENG 231 - Systems Programming

CENG 231 - Systems Programming

Prerequisite, CPSC 230. Corequisite, CENG 231L. This course introduces students to concepts and techniques in systems programming with the programming languages C and C++ in a *nix environment. Students will gain insight into hardware-software interfaces through hands-on projects involving system calls, concurrency, network programming,

memory mapping, and low-level mechanisms for inter-process communication. A laboratory component will allow students to implement conceptual ideas in code for enterprise, real-time, and embedded hardware targets. Letter grade with Pass/No Pass option. (Offered spring semester.) **3 credits**

CENG 231L - Lab - Systems Programming

CENG 231L - Lab - Systems Programming

Prerequisite, CPSC 230. Corequisite, CENG 231. Laboratory component of CENG 231. Letter grade with Pass/No Pass option. (Offered spring semester.) **1 credit**

CPSC 353 - Data Communications and Computer Networks

CPSC 353 - Data Communications and Computer Networks

Prerequisite, CENG 231 or CPSC 231 or CPSC 236. Students explore the principles and techniques of data communications and give special emphasis to networks and distributed systems. The I.S.O. Reference Model for open systems interconnection will be investigated and the function and operation of each protocol layer analyzed in detail. Letter grade with Pass/No Pass option. (Offered every semester.) **3 credits**

ISP 363 - Cybersecurity 1

ISP 363 - Cybersecurity 1

Prerequisite, CPSC 353. Students are exposed to the world of cybersecurity. Emphasis is placed on understanding, recognizing, and patching security exploits. Students will use standard industry tools and techniques to gain hands-on experience in this rapidly-growing field. Note that students majoring in computer science, computer engineering, software engineering, or data analytics may not use ISP 363 as an elective in the major if they are also minoring in Information Security and Policy. Letter grade with Pass/No Pass option. (Offered every year.) **3 credits**

ENGR 385 - Effective Technical Communication

ENGR 385 - Effective Technical Communication

Prerequisite, CPSC 231 or CENG 231. Students learn key aspects of communication in technical fields, in written and verbal formats. The course will emphasize practical, real-world examples and opportunities to practice and apply what is learned. The course covers understanding audience and purpose, applying a process of writing, collaboration, and visual and verbal presentation with an emphasis on communicating technical ideas to broad audiences. Letter grade with Pass/No Pass option. (Offered spring semester.) **3 credits**

ISP 452 - Fundamentals of Digital Forensics

ISP 452 - Fundamentals of Digital Forensics

Prerequisite, ISP 363. This course introduces students to the methodologies and procedures associated with digital forensic analysis and investigations within a network infrastructure. Students will develop an understanding of core topics such as topologies, protocols, and various software tools required to conduct forensic analysis/investigations. Students will comprehend the importance of network forensic principles, legal considerations, digital evidence controls, and proper documentation of forensic procedures and evidence collection. Letter grade with Pass/No Pass option. (Offered every year.) **3 credits**

CPSC 453 - Network Implementation and Security

CPSC 453 - Network Implementation and Security

Prerequisite, CPSC 353. Students explore the principles and techniques for implementing TCP/IP based networks using Microsoft Windows and Linux servers and clients, including the skills to configure, customize, optimize, troubleshoot, and integrate networks. Letter grade with Pass/No Pass option. (Offered as needed.) **3 credits**

social science (3 credits)

Students complete one section of POSC 317 - Media and Politics OR POSC 341 - The First Amendment OR POSC 343 - Constitutional Law: Civil Rights and Liberties.

advanced topics (3 credits)

complete three 1-credit sections from the following

ISP 371 - Advanced Topics in Cybersecurity

ISP 371 - Advanced Topics in Cybersecurity

Prerequisite, ISP 363. In this course students will be exposed to several in-depth topics in computer security through directed reading, guest speakers, hands-on labs and practicums. Letter grade with Pass/No Pass option. Repeatable for credit if the topic is different. (Offered every year.) **1 credit**

total credits 28