Savannah River Environmental Sciences Field Station

Cybersecurity Program - 2025

The Savannah River Environmental Sciences Field Station (SRESFS) seeks to increase recruitment and retention of under-represented students in science, engineering, cybersecurity, and environmental science career professions. Coursework and extensive interactions with Savannah River National Laboratory (SRNL) scientists and engineers emphasize the current focus areas of the Department of Energy (DOE) Environmental Management Office and introduce interns to the work environment of a National Laboratory. Courses are held at the University of South Carolina Aiken (USCA) and the Savannah River Site (SRS). Apartment-style housing is provided on the USCA campus. This course driven cybersecurity program provides an introduction to cybersecurity, its real- world applications in a National Laboratory environment, and will help you determine whether a career in cybersecurity is for you.

Presenting research at SRNL's poster session

BENEFITS:

- Stipend of $3125/session
- Tuition and fees
- Housing
- Course credits

ELIGIBILITY:

- Rising Sophomore, Junior, or Senior attending a Minority Serving Institution with a GPA of 2.5 or better
- Must be a U.S. citizen

Interns preparing for mock cybersecurity audits at a local business.

TO APPLY:
We are accepting applications through March 15, 2025
at: **https://sresfs.net**

Applications accepted through March 1 on Handshake

Program questions? *Email Chris Walker at cwalker3@scsu.edu*

In-person & Virtual Option Available

CYBERSECURITY COURSES

Session I (Late May to Late June 2025)

Fundamentals of Cybersecurity (3 credits)
Introduction to core concepts, terminology, technologies, and skills associated with Cybersecurity. Major security topics such as vulnerability assessment, virus attacks, hacking, spyware, network defense, passwords, firewalls, VPNs and intrusion detection are covered. Includes hands-on laboratory exercises, term paper and presentation, simulation, participation in speaker series and team work.

Fundamentals of Digital/Computer Forensics (3 credits) Fundamentals of computer forensics and investigations. Historical and current computer forensic and investigative security issues; systematic approach to computer investigations; digital forensics, email and image file analysis; guidelines for investigation reporting. Various forensic tools will be used during the laboratory portion of the class.

Session II (Late June - Late July 2025)

Introduction to Legal and Ethical Issues in Cybersecurity (3 credits) Legal and ethical aspects of cybersecurity. Ethics, privacy laws, usability security, cybercrime and the social, psychological and cultural aspects of cybercrime. Emphasis is on the theoretical as well as the practical aspects of issues. Term paper and case study required.

Special Topics - Cybersecurity (3 credits)
Emerging topics and recent advances in cybersecurity in various disciplines, e.g. Business, Criminal Justice, Psychology. Emphasis is on theoretical as well as practical aspects of issues.