

Supervised Cybersecurity Workforce Program

University Partnership Program | Academic Year 2026–2027

ABOUT THE PROGRAM

The TechStep Cyber Clinic places career changers and students into supervised cybersecurity engagements with nonprofit organizations. Participants work alongside experienced practitioners, producing deliverables for real clients. Services are provided at no cost to community organizations.

WHO THIS IS FOR

Students and career changers transitioning into roles such as GRC analyst, risk assessor, security consultant, or data governance specialist. Candidates are referred through university faculty. Prior cybersecurity experience is not required.

ENGAGEMENT TYPES

Engagement	Description	Skills Developed
Cybersecurity Risk Assessment	Structured interviews, device inventory, gap analysis against NIST CSF, written findings report, and leadership briefing.	Risk interviewing, NIST CSF, documentation, client reporting
Security Policy Development	Drafting core policies the organization lacks — incident response, acceptable use, and data classification.	Policy writing, incident response, data classification
Vendor & Third Party Risk Review	Identification of all tools in use, vendor data handling research, risk ratings, and a prioritized inventory.	Vendor analysis, risk scoring, third party risk management
AI Use & Data Governance	Assessment of AI tools in use, data exposure risks, and development of an AI acceptable use policy.	AI governance, data exposure analysis, policy development
Security Awareness Training	Development and delivery of a tailored security awareness session based on the organization's risk profile.	Training development, phishing awareness, risk communication

ENROLLMENT PROCESS

01 Faculty Referral	Faculty submit candidate information to TechStep using the provided referral form. Bulk referrals may be submitted via the Faculty Referral Spreadsheet.
02 Interview	TechStep staff conducts a 30-minute interview with each referred candidate, assessing communication, professionalism, and ability to commit to a 6–10 week engagement.
03 Placement	Accepted participants complete a background check and are matched to a community partner and engagement type. A participation agreement is signed before the engagement begins.
04 Engagement	Participants work under close supervision for the full engagement period. All deliverables are reviewed and approved by TechStep staff before being shared with the client.

COMMUNITY PARTNERS

Participants are placed with nonprofit organizations in the DC, Maryland, and Virginia region that have verified security needs but no dedicated internal cybersecurity staff. Partner organizations include healthcare facilities, educational institutions, senior care providers, housing nonprofits, cultural organizations, and refugee services organizations.

