

COMPANY OVERVIEW

Diversity Cyber Council, Inc. is a Non-Profit Corporation that serves disadvantaged communities by facilitating the education, training, and staffing of underrepresented groups in cybersecurity to establish a diverse talent pipeline to the cyber workforce

CYBERSECURITY WORKFORCE DEVELOPMENT APPRENTICESHIP PROGRAM



Program Description

Diversity Cyber Council's Cybersecurity Workforce Development Apprenticeship Program, registered with the US Department of Labor, is designed to administer comprehensive cyber related curriculum and paid on the job training through our strategic employer partnerships. Our goal is to proactively improve the readiness and diversity of the cyber security workforce. The program serves as solution to enhance the cybersecurity workforce by targeting underrepresented minorities, women, veterans, and eligible youth to teach them the skills to become cybersecurity professionals. The goal of the program is to leverage content of industry leading vendors to educate our trainees and prepare them for exam certification. The strategic value of the program fortifies Diversity Cyber Council's ability to provide training and staffing services to employers within our network which establishes a viable cybersecurity workforce pipeline that provides access to talent and opportunity.



Program Schedule

The program consists of 3 four-month phases of training that combines on the job training and instructor led curriculum intended to build apprentice competency to successfully pass an industry recognized certification exam per phase.

Phase 1

For the first four months the program, apprentices will be on a regimented schedule of instructor led training 8 hours (9am – 5pm) for the first three days of the week (Monday –Wednesday) while performing on the job training for a period of eight hours (9am – 5pm) for the final two days of the week (Thursday – Friday). In Phase 1 apprentices will be taught the fundamentals of IT and trained to competency to successfully pass the CompTIA IT Fundamentals exam. OJT will be provided by our network of instructors that are committed to train apprentices through hands on experience that match those needed to be proficient as a cyber security analyst. In this phase, apprentices will earn \$15.00 an hour and undergo bi-weekly performance assessments to ensure development is on track.

Phase 2

Upon successfully passing the CompTIA IT Fundamentals exam, apprentices will receive a \$2.50 an hour rate increase entering Phase 2 of the program. In Phase 2, the instructor learning and on the job training working schedule will remain the same. Apprentices that do not pass the exam on their first attempt will be provided mandatory remedial training via virtual learning in addition to the Phase 2 schedule and be extended 30 days to pass the CompTIA IT Fundamentals exam before failing out of the program. The core of the Phase 2 curriculum will be based on the CompTIA Security+ exam as students will be trained to competency to pass the exam to clear

Phase 3

After earning their CompTIA Security+ certification, apprentices will receive another \$2.50 an hour rate increase entering Phase 3 of the Program. In Phase 2, the instructor learning and on the job training working schedule remains the same. Apprentices that do not pass the exam on their first attempt will be provided mandatory remedial training via virtual learning in addition to the Phase 3 schedule and be extended 30 days to pass the CompTIA Security+ exam before failing out of the program. The core of the Phase 3 curriculum will be based on the CompTIA CySA+ exam as students will again be trained to competency to pass the exam to complete the program.

VALUE TO APPRENTICES

As an apprentice, the cybersecurity workforce development apprenticeship program offers a service of paid training and learning to begin or transition to a cybersecurity career. It is recognized that there exists an identifiable need for diverse talent, Diversity Cyber Council pledges to equip the targeted demographic with the skills necessary to enter a thriving market that is oriented to compliment apprentices' career and life goals. Apprentices receive hands-on training resulting in improved skills and competencies as well as the potential to earn college credit toward an associate's or bachelor's degree. In addition, upon graduation apprentices earn a Department of Labor certification that is a recognized credential throughout the workforce.

How to Apply

- Candidates must meet the following eligibility requirements in order to be selected for the next step of the selection process:
- Be 18 years of age or older
- Commitment and availability for the entire program
- Qualify as a military veteran; woman; or racial minority
- Complete entry application
- Consent to a background check
- Complete the apprenticeship assessment

Interested candidates that meet the criteria above can apply directly on our website at: <https://diversitycybercouncil.com/candidate-application-form/>

EMPLOYER PARTNERSHIPS

ON THE JOB TRAINING

Through the apprenticeship program, employer partners will participate in proactively filling their organization's cybersecurity needs while further developing the workforce as a whole. The goal is to target the deficit of cybersecurity talent and supplement it by offering a cost-effective alternative to the current workforce recruiting structure. This is accomplished by establishing a direct pipeline to access viable entry level professionals to complement their overarching cybersecurity resourcing requirements.

EMPLOYER COMMITMENT

From the employer perspective, the dynamic of our partnership mirrors that of traditional third-party staffing provider that is a regularly common business practice. Most employers leverage third party vendors to fill a specific position, by participating in the apprenticeship employers support an organic talent pool to recruit and retain talent familiar with their business and culture. The only exceptions to the third-party vendor model is that our apprentices operate under limited hours, approximately 16 or 24 per week. This approach allows our apprentices to spend time in the classroom to further develop their competency. In addition, we work collaboratively with employers to ensure apprentices are meeting expectations and providing value. It is our goal to limit the perceived risks that a new program may inherent and our team is committed to altering partnership terms that reduce risk while accenting business value.

VALUE TO EMPLOYERS

As a registered apprenticeship with the Department of Labor, our program is entitled to funding and incentives as provided by the Workforce Innovation and Opportunities Act (WIOA). The Workforce Innovation and Opportunities Act covers a minimum of 300 hours in wage costs permitting employers to obtain a working resource without incurring expense for first phase of the program. There also exists additional federal tax benefits that collectively offers employers a cost-effective solution to developing entry level talent. Supplementary value drivers to employers include:

- Contributing to economic growth and business expansion by enhancing the talent the cyber security workforce.
- State and local boards will promote the use of industry and sector partnerships to address the workforce needs of multiple employers within the cyber security and IT industry to meet the workforce needs of local and regional employers.
- Recruit and develop a highly skilled workforce talent that proactively helps grow their business
- Improve productivity, profitability, and an employer's bottom line by pre-emptively developing the cyber security workforce

HOW TO APPLY

Interested employers can send an email to partnerships@diversitycybercouncil.com or inquire directly on our website at <https://diversitycybercouncil.com/employer-partnership-application-form/>



THANK YOU