DIVERSITY CYBER COUNCIL
SECURING ACCESS TO OPPORTUNITY

# COMPANY OVERVIEW

Diversity Cyber Council, Inc. is a 501c3 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

DIVERSITY CYBER COUNCIL
SECURING ACCESS TO OPPORTUNITY

## TOTAL TERM OF APPRENTICESHIP :

Duration – 12 Months
800 hours ILT (Instructor Led Training) plus 1200 hours OJL (On Job Learning) hours

During the term of apprenticeship, the Apprentice shall receive such instruction and experience, in all branches of the occupation, as is necessary to develop a practical and versatile worker. Major processes in which Apprentices will be trained and approximate hours to be spent in each are as follows:

## Phase 1 (Duration – 1 Month)

For the first month of the program, candidates will be on a regimented schedule of instructor led training for approximately 8 hours a day (9am – 5pm) Monday – Friday to build the necessary foundational technology competency necessary to begin on the job training in the next phase. The core curriculum will be a blend of cyber related instruction, soft skills training, and practice exercises to prepare for the CompTIA IT Fundamentals exam. This exam focuses on the essential IT skills and knowledge needed to perform tasks commonly performed by advanced end-users and entry-level IT professionals alike, including using features and functions of common operating systems, establishing network connectivity, identifying common software applications and their purpose, and learning security best practices In order to proceed to the next phase, candidates must pass the CompTIA IT Fundamentals exam in which they will be updated to apprentice status and continue the program. Candidates that are unable to gain the CompTIA IT Fundamentals credential will be provided a week of retraining and extended another attempt to pass the exam. If after the second attempt is also unsuccessful the candidate will be dis-enrolled from the program but given priority entry for the next cohort.

## Phase 2 (Duration – 3 Months)

In Phase 2, apprentices will be taught the fundamentals of cybersecurity and trained to competency to successfully pass the CompTIA Security+ exam. This exam will certify apprentices possess the understanding and skills required to install and configure systems to secure applications, networks, and different devices. Apprentices will learn to install security systems, perform threat analysis techniques, and take precautionary measures to mitigate risks. Upon completion of Phase 2, apprentices will be able to Identify, analyze, and respond to security events and incidents as well as successfully implement an appropriate security solution for monitoring technology environments that includes cloud, IoT, and mobile. Apprentices will be provided an opportunity to take the CompTIA Security+ exam at the end of the phase, while it is not a requirement to pass the exam to continue the program it is HIGHLY encouraged. On the job training will be provided by our employer partners that are committed to train apprentices to gain hands on experience that match those needed to be proficient as a cyber security analyst. The tentative schedule for Phase 2 will consist of instructor led training 8 hours (9am – 5pm) a day Monday –Tuesday while performing on the job training with an employer for a period of eight hours a day (9am – 5pm) Wednesday – Friday. Apprentices will earn $15.00 an hour and undergo bi-weekly performance assessments to ensure development is on track.

## Phase 3 (Duration – 3 Months)

In Phase 3, apprentices will be taught the fundamentals of cloud technology and trained to competency to successfully pass the CompTIA Cloud+ exam. This exam validates the skills needed to deploy and automate secure cloud environments that support the high availability of business systems and data. CompTIA Cloud+ is the only performance-based IT certification that views cloud-based infrastructure services in the context of broader IT systems operations regardless of the platform. Apprentices will be provided an opportunity to take the CompTIA Cloud+ exam at the end of the phase, while it is not a requirement to pass the exam to continue the program it is HIGHLY encouraged. Similarly, to Phase 2, the training schedule will be retained consisting of instructor led training 8 hours (9am – 5pm) a day Monday –Tuesday and on the job training for a period of eight hours a day (9am – 5pm) Wednesday – Friday. Apprentices will continue to earn $15.00 an hour and undergo bi-weekly performance assessments to ensure development is on track

## Phase 4 (Duration – 3 Months)

In Phase 4, apprentices will be taught the fundamentals of incident response and monitoring in preparation to successfully pass the CompTIA Analyst+ exam. This exam will certify students for having the understanding to obtain the skills required to configure and use threat detection tools, perform data analysis and interpret the results to identify vulnerabilities, threats and risks to an organization, with the end goal of securing and protecting applications and systems within an organization. Apprentices will be provided an opportunity to take the CompTIA Analyst+ exam at the end of the phase, while it is not a requirement to pass the exam to continue the program it is HIGHLY encouraged. Similarly, to Phase 2 & 3, the training schedule will be retained consisting of instructor led training 8 hours (9am – 5pm) a day Monday –Tuesday and on the job training for a period of eight hours a day (9am – 5pm) Wednesday – Friday. Apprentices will earn $15.00 an hour and undergo bi-weekly performance assessments to ensure development is on track.

## Phase 5 (Duration – 3 Months)

In the final phase, apprentices will work fulltime for their respective employer sponsors to continue to exercise their acquired skills. Based on performance evaluations and acquired credentials apprentices will be eligible to receive between a $2.50 - $5.00 wage increase upon entering Phase 5. At the end of Phase 5, a graduation ceremony will commence to present apprentices with the Department of Labor Certification of Completion and program awards. Employer sponsors will also have the opportunity to present employment offers to apprentices they deem meet the qualifications of their respective organizational workforce needs. Resume writing, career services, and mentorship will be extended to graduating apprentices for a minimum of one year after program completion.

# 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/ or send an email to support@diversitycybercouncil.com**

# 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. The related training are aligned with the following cybersecurity workforce roles:

- Cybersecurity Analyst
- IT Help Desk Analyst
- IT Cybersecurity Specialist
- Cybersecurity Incident Responder
- Cybersecurity Architect
- IT Security Auditor
- IT Systems Administrator
- Junior Cyber Penetration Tester
- Network Security Analyst
- Governance, Risk, & Compliance Analyst

## 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 second 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

Send an email to
**partnerships@diversitycybercouncil.com**
Inquire directly on our website at
**https://diversitycybercouncil.com/employer-partnership-application-form/**

Complete a two minute Diversity, Equity, & Inclusion (DEI) Technology Workforce Development Survey at
**https://form.jotform.com/Diversity_Cyber_Coun/Technology-Workforce-Development**

DIVERSITY CYBER COUNCIL
SECURING ACCESS TO OPPORTUNITY

# THANK YOU