

Curriculum

CompTIA Security+ Certificate



Table of Contents

Why Security+? 1

Pre-requisites 2

Possible Cybersecurity Career Paths 3

Performance Based Objectives 4

Curriculum 5

Module 1: General Security Concepts 6

Module 2: Threats, Vulnerabilities, and Mitigations 7

Module 3: Security Architecture 8

Module 4: Security Operations 9

Module 5: Security Program Management and Oversight 10

Module 6: Exam Preparation and Capstone 11

Pace & Schedule 12

Why Digital Workshop Center? 13

Apply Now 14

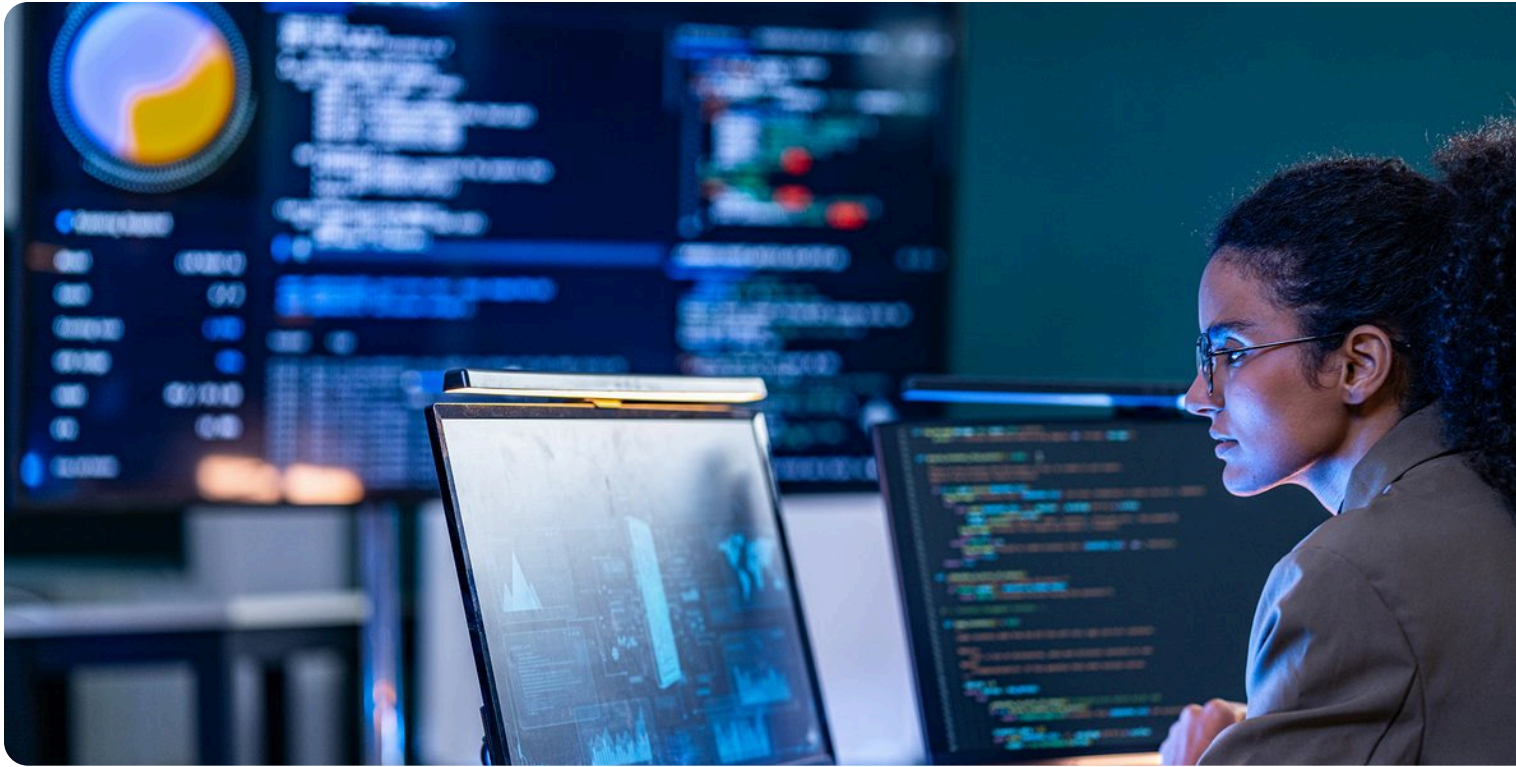
Contact Us 14

Schedule A Meeting 14

WHY DWC?

\$16.4K

average increase in salary of
certificate program students



Why Security+?

The CompTIA Security+ Certificate at Digital Workshop Center is a 48-hour, live, online, instructor-led program for IT professionals and career changers moving into cybersecurity. This hands-on training prepares you for the current CompTIA Security+ exam and for entry-level roles like SOC analyst and security analyst.

What sets DWC apart is live instruction in small classes, official CompTIA CertMaster Labs, and personalized feedback throughout the course. You practice the real tasks of a security analyst: SIEM monitoring, log analysis, vulnerability scanning, and incident response.

(continued on next page)



PROGRAM LENGTH*
48 total hours.
16 total sessions
of 3 hours each.



TARGET STUDENT
Intermediate

*Additional coursework may need to be completed outside of class time.



We emphasize employer-aligned skills such as documentation, escalation, and incident reporting. Upon completion, you'll have a strong foundation in security operations and be prepared to take the CompTIA Security+ exam, with the exam voucher, courseware, and CertMaster Labs included in tuition.

What You'll Walk Away With:

- Hands-on experience in official CompTIA CertMaster Labs, guided live by your instructor
- Practice with SIEM monitoring, log analysis, and vulnerability scanning
- Experience working an incident from detection through documentation
- Scenario exercises in the exam's performance-based question (PBQ) format
- Preparation to earn CompTIA Security+, a credential recognized by employers worldwide
- A capstone incident scenario that showcases applied security skills
- An understanding of governance, risk, and compliance in real organizations
- Professional communication and documentation skills for security teams
- A full timed practice exam before you schedule the real one
- A competitive edge for SOC analyst and security analyst roles



PRE-REQUISITES

- **Computer Proficiency:** Comfortable using computers and operating systems (Windows, macOS, or Linux), including file management and software installation.
- **Networking Fundamentals:** Working knowledge of IP addressing, routing, switching, and common network services.
- **Operating System Skills:** Experience with user accounts, permissions, and basic system settings.
- **Troubleshooting Mindset:** Willingness to work methodically through logs, alerts, and scan results.
- CompTIA A+ or Network+ is helpful but not required; admissions can recommend the right starting point.

Possible Cybersecurity Career Paths

Graduates of the CompTIA Security+ Certificate can pursue entry-level cybersecurity roles, from SOC analyst and security analyst to incident response and compliance. The BLS projects information security analyst jobs to grow 21 percent from 2025 to 2035, with about 14,100 openings each year.

\$129,180

median pay for information security analysts (BLS, May 2025)



SOC ANALYST, TIER 1

Monitor alerts, triage suspicious activity, and escalate confirmed incidents in a security operations center.



SECURITY ANALYST

Investigate threats and vulnerabilities, run scans, analyze logs, and recommend fixes before attackers find the gaps.



INCIDENT RESPONSE ANALYST

Contain active attacks, preserve evidence, and document what happened and how to prevent it.



COMPLIANCE ANALYST

Support audits and translate security frameworks and regulations into controls IT teams can implement.

Performance Based Objectives

Upon successful completion of this program, students will:

- ✓ Explain security controls, the CIA triad, zero trust, and core cryptography.
- ✓ Profile threat actors and match common attacks to the controls that stop them.
- ✓ Recognize indicators of compromise in logs, traffic, and system behavior.
- ✓ Compare the security of enterprise, cloud, virtualized, and IoT architectures.
- ✓ Harden systems and manage vulnerabilities across their lifecycle.
- ✓ Apply identity and access management, including MFA and privileged access.
- ✓ Monitor with SIEM tools and work incidents from detection to report.
- ✓ Perform risk analysis and explain governance, compliance, and audits.
- ✓ Prepare for and pass the CompTIA Security+ certification exam.
- ✓ Document and communicate findings professionally on a security team.



Curriculum

All instruction is held live on Zoom, with class links in your student portal. The program meets twice per week for 3 hours per session. Your class schedule is set once enrollment fills.*

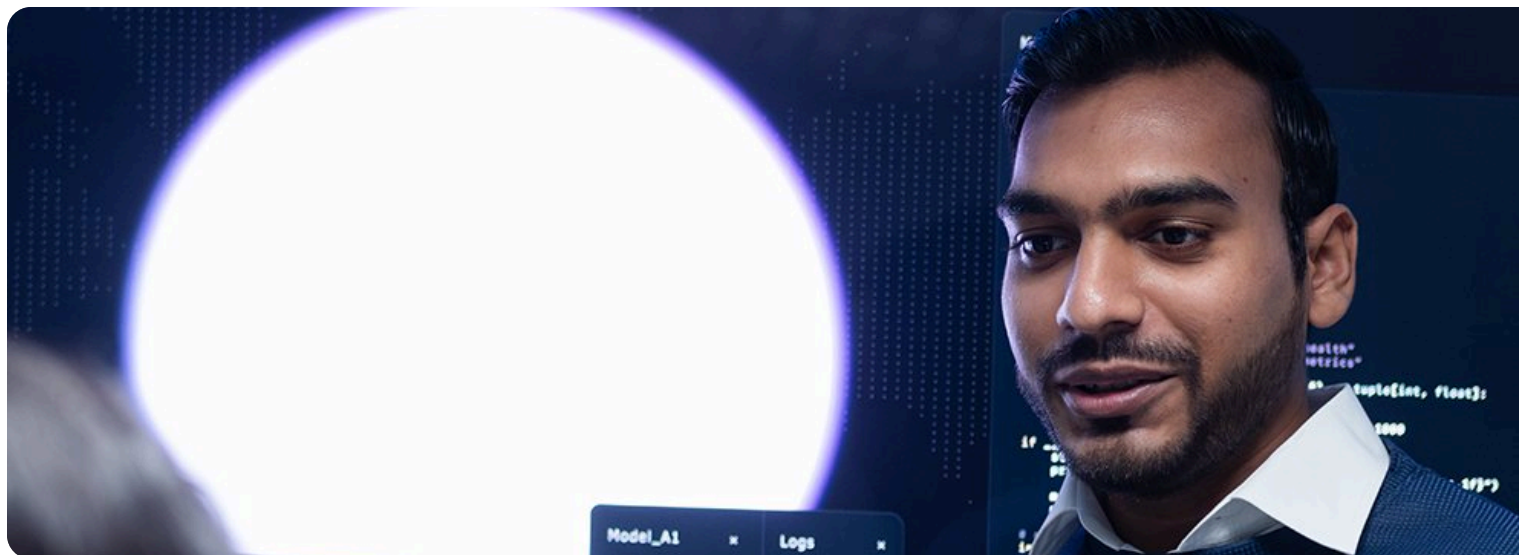
MODULES		HOURS*	SESSIONS
MODULE 1	General Security Concepts	6	2
MODULE 2	Threats, Vulnerabilities, and Mitigations	9	3
MODULE 3	Security Architecture	6	2
MODULE 4	Security Operations	12	4
MODULE 5	Security Program Management and Oversight	9	3
MODULE 6	Exam Preparation and Capstone	6	2
Total		48	16

*All schedules are approximate and subject to change. Your instructor reserves the right to alter this calendar as circumstances may dictate.

*Each module may require registration in multiple stand-alone classes

* Class start timing depends on enrollment and cannot be guaranteed.

Official CompTIA courseware and CertMaster Labs access are included in tuition.



MODULE 1 / 6 HRS / 2 SESSIONS

General Security Concepts

Students build the foundational vocabulary and conceptual framework of cybersecurity: security control categories, the CIA triad, zero trust architecture, change management, and practical cryptography. By the end, students can classify security controls, explain how confidentiality, integrity, and availability shape security decisions, and describe how hashing, encryption, and PKI protect data in real systems.

Session 1: Security Controls and Core Concepts

- Security control categories and control types
- The CIA triad, zero trust architecture, and gap analysis
- Physical security and change management processes

Session 2: Cryptographic Solutions

- Hashing, symmetric and asymmetric encryption, and where each is used
- Public key infrastructure (PKI) and digital certificates
- Hands-on lab: working with certificates and hashing

ALUMNI SUCCESS STORIES



Easy to contact and enroll in courses. I found they have a course that I need to further my career, contacted them and enrolled in said course in less than two weeks.

Robert H.
DWC Student

[READ TESTIMONIALS](#)

MODULE 2 / 9 HRS / 3 SESSIONS

Threats, Vulnerabilities, and Mitigations

Students learn to think like the attackers they will defend against: threat actors and their motivations, social engineering including AI-assisted phishing, common vulnerabilities and attack types, and the mitigations that stop them. By the end, students can profile threat actors, recognize indicators of malicious activity in logs and traffic, and match each attack type to the defense that counters it.

Session 3: Threat Actors and Social Engineering

- Threat actor types, motivations, and capabilities
- Attack surfaces and common threat vectors
- Social engineering, including AI-assisted phishing and impersonation

Session 4: Vulnerabilities and Attack Types

- Vulnerabilities across applications, operating systems, hardware, and cloud
- Malware types, password attacks, and injection attacks
- Hands-on lab: analyzing common attacks in CertMaster Labs

Session 5: Indicators and Mitigations

- Indicators of malicious activity in logs, traffic, and system behavior
- Mitigation techniques from segmentation to least privilege
- Hands-on lab: identifying indicators of compromise



**MODULE 3 / 6 HRS / 2 SESSIONS**

Security Architecture

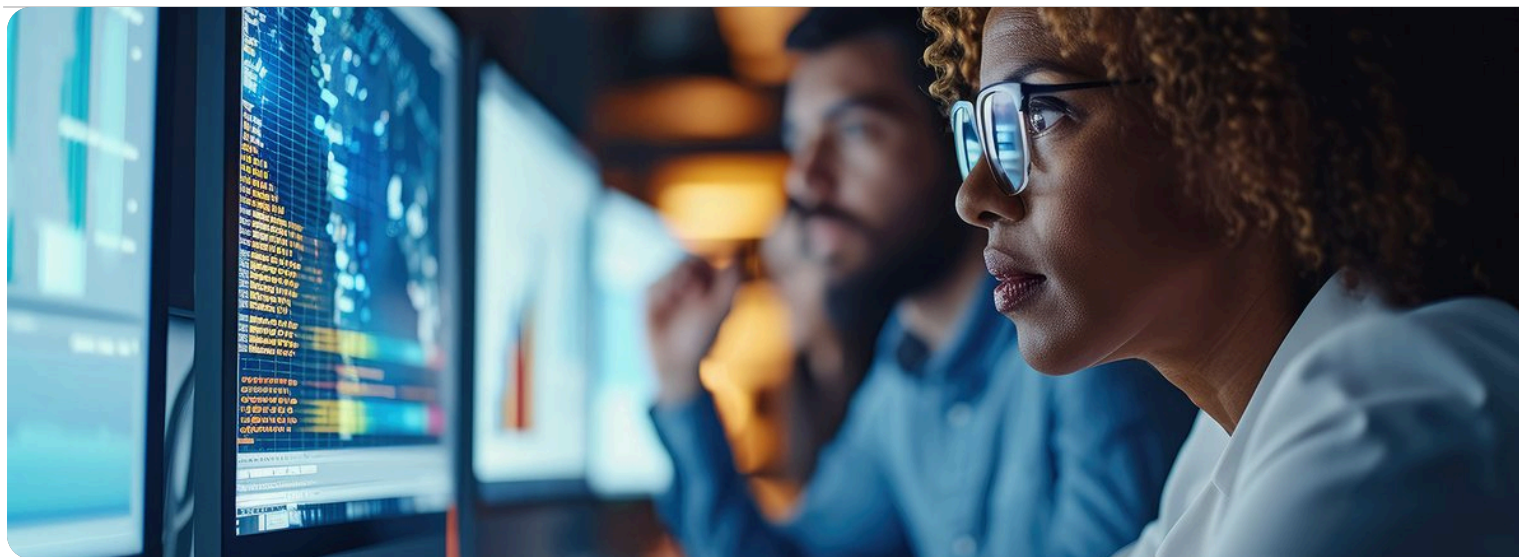
Students learn how secure environments are designed: enterprise, cloud, virtualized, IoT, and industrial control environments, the appliances and access technologies that protect them, and data protection and recovery strategy. By the end, students can compare the security implications of different architecture models, place security appliances correctly in a network design, and explain how backups, failover, and continuity planning keep organizations running through an incident.

Session 6: Architecture Models and Infrastructure Security

- Security implications of enterprise, cloud, virtualized, IoT, and ICS environments
- Network appliances, secure communication, and access technologies
- Hands-on lab: configuring secure network segments

Session 7: Data Protection, Resilience, and Recovery

- Protecting data at rest, in transit, and in use
- Backup strategies, failover, and high availability
- Continuity planning and recovery concepts

**MODULE 4 / 12 HRS / 4 SESSIONS**

Security Operations

The largest module in the program, because it is the daily work of the analyst roles this certificate targets. Students practice system hardening, vulnerability management, identity and access management, SIEM monitoring, and incident response. By the end, students can harden a system against a baseline, run and interpret vulnerability scans, investigate SIEM alerts, and work an incident from detection through documentation the way a working SOC analyst does.

Session 8: Hardening, Assets, and Vulnerability Management

- Secure baselines and hardening targets across systems and devices
- Asset management and the vulnerability management lifecycle
- Hands-on lab: running vulnerability scans and interpreting results

Session 9: Identity and Access Management

- Provisioning, deprovisioning, and account types
- Multifactor authentication, password best practices, and privileged access management

Session 10: Monitoring, Security Tools, and Automation

- SIEM monitoring and log analysis workflows
- Enterprise security tools and automation and orchestration in security operations

Session 11: Incident Response and Digital Forensics

- The incident response lifecycle from preparation to lessons learned
- Digital forensics fundamentals: evidence handling and documentation
- Hands-on lab: working an incident from detection through reporting

**MODULE 5 / 9 HRS / 3 SESSIONS**

Security Program Management and Oversight

Students learn the governance layer that turns security work into a security program: governance structures, risk management, third-party risk, compliance, audits, and security awareness. By the end, students can perform the risk calculations that appear on the exam, evaluate third-party and supply chain risk, and explain how audits, penetration testing, and awareness programs keep an organization compliant and its users alert.

Session 12: Governance and Risk Management

- Governance structures, policies, standards, and procedures
- The risk management process and risk analysis
- Hands-on lab: performing key risk calculations

Session 13: Third-Party Risk and Compliance

- Vendor assessment and supply chain risk
- Compliance monitoring, privacy requirements, and data roles

Session 14: Audits, Penetration Testing, and Security Awareness

- Audit and assessment types, internal and external
- Penetration testing concepts and rules of engagement
- Security awareness programs that change user behavior

MODULE 6 / 6 HRS / 2 SESSIONS

Exam Preparation and Capstone

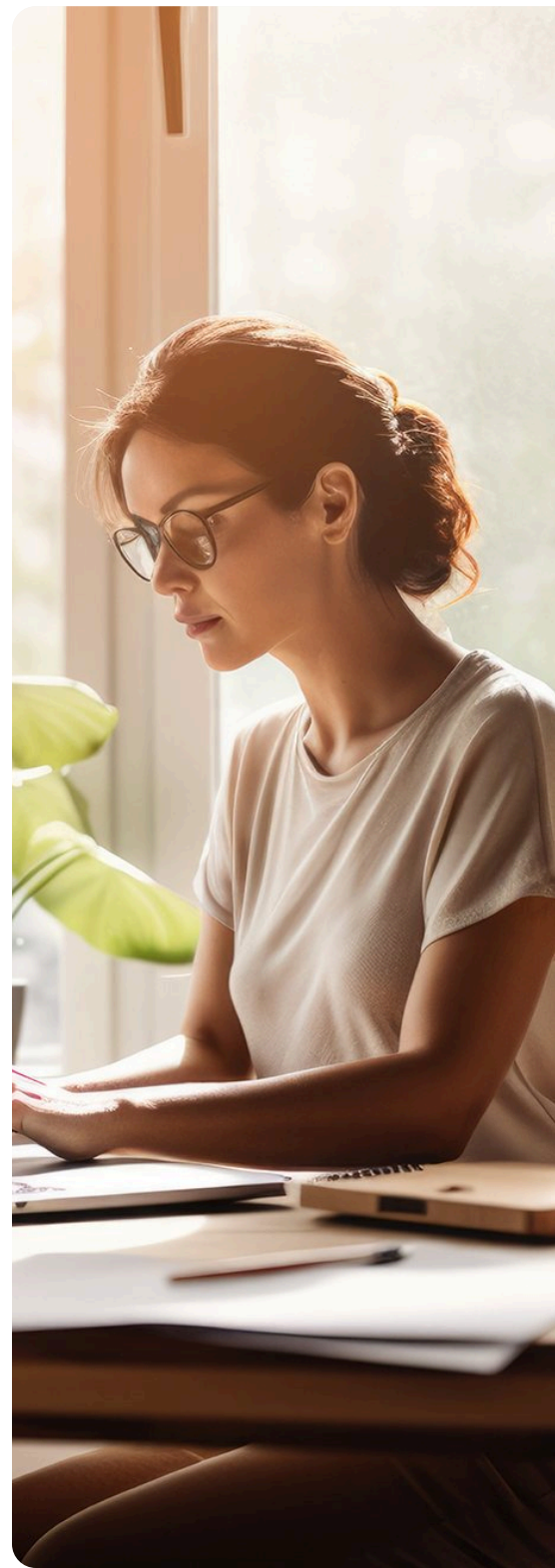
Students consolidate everything into exam readiness and a portfolio-worthy capstone: structured review across every Security+ domain, performance-based question practice, and a full timed practice exam. By the end, students have calibrated their readiness against the real exam format and completed a capstone incident scenario, analyzing evidence, responding, and reporting findings the way a working analyst would.

Session 15: Exam Review and PBQ Practice

- Structured review across all Security+ exam domains
- Practice questions with instructor explanations
- Performance-based question (PBQ) practice in the exam format

Session 16: Practice Exam and Capstone Incident Scenario

- Full timed practice exam mirroring the real exam
- Capstone: analyze, respond to, and report on a simulated security incident
- Exam scheduling, voucher use, and test day preparation



Pace & Schedule

At Digital Workshop Center, we know that how you choose to learn is one of the key factors driving your success. Combining live online learning through Zoom and individualized support, all students have access to a personalized and mentored learning experience.

Learn online. With guidance every step of the way.

DWC students have access to career coaching, Slack channels, and team support throughout the program.

Your program is a small live class with rolling enrollment: enroll any time, and your class schedule is set once enrollment fills, typically within 2 to 3 weeks.*

Length	About 8 weeks
Time Commitment	48 hours
Career Services Support	Yes
1:1 With Instructors	Yes
Live Lectures	Yes
Small Live Classes	Yes

* Start timing depends on enrollment and cannot be guaranteed.

Why Digital Workshop Center?

DWC has delivered live, instructor-led career training nationwide since 2006. Most CompTIA Security+ prep is a video library and a discussion forum, or a large bootcamp where the instructor teaches to the middle.

At DWC your instructor works in security, your class stays small, you train in official CertMaster Labs, and you graduate with the DWC CompTIA Security+ Certificate, a professional certificate issued by Digital Workshop Center.

Included with tuition, for every student:

- ✓ Exam voucher, official CompTIA courseware, and CertMaster Labs
- ✓ Admissions advisors from pre-enrollment through your first day
- ✓ Instructor mentoring before, during, and after class
- ✓ One-on-one career coaching on your resume and job search
- ✓ Tech support by Slack, email, or phone while you train
- ✓ Parker Dewey micro-internships and the DWC alumni community

WE OFFER SCHOLARSHIPS

You may only apply for one of the following scholarships:

Tech Skills Scholarship

For unemployed, dislocated workers, or those looking to up-skill, re-skill, or add new skills

Women and Tech Scholarship

For women looking to re-skill, up-skill or add new skills in a technology career

Next Mission Scholarship

For active or retired military service members and their families

[LEARN MORE](#)

WHERE OUR GRADS HAVE BEEN HIRED



VAIL RESORTS



Ready to Transform Your Career in Just 3 Simple Steps?

STEP 1

Talk to an Advisor

Schedule a quick 15-minute meeting with a student advisor. Ask questions about the enrollment process, tuition, schedules & more.

[SCHEDULE MEETING](#)

STEP 2

Discover the Digital Workshop Center Difference

Experience our unique approach before you commit. Attend our mandatory program orientation to get a feel for our hands-on, practical teaching style.

[LEARN MORE](#)

STEP 3

Easy Enrollment

Begin your journey effortlessly with our straightforward online application. It's fast, easy, and your first step towards a brighter future.

[APPLY NOW](#)

Contact Us

Phone: [970-980-8091](tel:970-980-8091)

Email: info@digitalworkshopcenter.com

Have Questions?

Have questions about our programs? Reach out to our admissions team for more help.

[CONTACT US](#)