APPLIED CYBERDEFENSE NETWORK OPERATIONS, BACHELOR OF SCIENCE

The Bachelor of Science in Applied Cyberdefense Network Operations (ACNO) prepares students for advanced roles securing, operating, and defending enterprise and cloud computing environments. Building on lower-division coursework in information technology, cybersecurity, or related fields, the program emphasizes cybersecurity operations, secure networking, cloud services and cloud security, incident response, and responsible use of artificial intelligence tools to support analysis and documentation. The curriculum combines lecture with intensive laboratory experiences aligned with industry standards and regional workforce needs.

Admission is by application through a multi-criteria selection process due to limited program capacity. Applicants are expected to demonstrate appropriate lower-division preparation, typically through completion of an Associate of Science degree in Information Technology, Cybersecurity, or a closely related discipline, or equivalent coursework. Students entering the program should possess foundational skills in networking, operating systems, and cybersecurity principles to ensure readiness for upper-division study.

The program provides a clear pathway for graduates of regional community college information technology and cybersecurity programs, minimizing duplication of coursework and supporting timely completion. Students with relevant Associate of Science degrees are strong transfer candidates.

Graduates will demonstrate the ability to implement, secure, monitor, and troubleshoot complex digital infrastructures; apply defensive cybersecurity practices; respond to security incidents; manage risks in enterprise and cloud environments; and communicate technical information effectively. The program aligns with industry-recognized certifications and prepares graduates for high-demand careers in cybersecurity, network operations, and cloud security while supporting continued professional development.

Admission to the Applied Cyberdefense Network Operations (ACNO) Bachelor's Degree

To qualify for admission into the BS in Applied Cyberdefense Network Operations program, students must have:

1. Earned an Associate degree in a related Information Technology or Cybersecurity Major. Consult with the discipline faculty if you have coursework that is not from Moorpark College.
2. Completed the California General Education Transfer Curriculum (Cal-GETC) pattern. Students with catalog rights and who have maintained continuous enrollment can continue to complete the CSU GE or IGETC.
3. Met all admission program requirements, including but not limited to the courses listed below in the Program Requirements for the Associate Degree.
4. Provided transcripts from all colleges attended.

After admission to the ACNO program, students must:

1. Complete all upper-division major coursework as designated in the Program Requirements. Each course for the major must be completed with a grade of "C" or better.
2. Complete 9 semester units of upper division general education (from two different disciplines outside of the major) as designated in the program requirements.
3. Complete the 128-136 units required for the bachelor's degree.

Course ID	Title	Units/ Hours
Lower-Division Major Requirements (AS Degree)		
CNSE M01	Networking Fundamentals	4
CNSE M06	Cisco Fundamentals of IT Essentials: PC Hardware & Software	4
CNSE M18	Cisco System Computer Networking A	4
CNSE M30	MS Windows Administration	3
CNSE M55	Linux Networking and System Administration	3
CNSE M57	Scripting for Security Management	3
CNSE M80	Work Experience Education in Computer Network Systems Engineering	1-4
CNSE M82	Introduction to Network Security	3
LIST A: Select one of the following courses (3-4 units)		
CNSE M13	Internetworking and TCP/IP	4
CNSE M19	Cisco System Computer Networking B	4
CNSE M31	MS Windows Network Server	3
LIST B: Select and complete two courses (5-6 units)		
CNSE M56	CompTIA Advanced Security Practitioner Preparation	3
CNSE M83	Introduction Computer Forensics	3
CNSE M84	Certified Ethical Hacker	2
CNSE M86	Firewall Administration	3
CNSE M100	Cybersecurity Analysis	3
CNSE M105	AWS Cloud Foundations	3
CNSE M111	Azure Cloud Fundamentals	3
CNSE M170	Cloud Security	3
Total Units for the Lower-Division Major Requirements		**33-38**
Upper-Division Major Requirements		
ACNO M301	Advanced Cisco II	3
ACNO M302A	Microsoft Hybrid Server 1	3
ACNO M302B	Microsoft Hybrid Server 2	3
ACNO M304	Virtualization Technology	3
ACNO M305	AWS Cloud Foundations	3
ACNO M306	Azure Cloud Administrator	3
ACNO M307	Cloud Architecture	3
ACNO M308	Firewall Security	3
ACNO M401	Cloud Databases	3
ACNO M402	Certified Ethical Hacker	3
ACNO M403	Cisco CyberOps	3
ACNO M404	Identity Protection Security	3
ACNO M405	Azure Cloud Security	3
ACNO M406	CompTIA Security Practitioner	3
ACNO M407	AWS Cloud Security	3
ACNO M408	Device and Network Forensics	3

ACNO M409	Risk Management	3
ACNO M480	Work Experience Education in Applied Cyberdefense Network Operations Program	1-4
Upper-Division General Education (GE)		
BUS M400	Project Management	3
ENGL M300	Technical Writing	3
PHIL M400	Ethics in the Age of Emerging Technology	3
Total Units for the Upper-Division Major and GE Requirements		**61-64**

Course ID	Title	Units/ Hours
Total Units for the Major (Lower and Upper-Division)		**94-102**
Cal-GETC Pattern		**34**
Double-Counted Units		0
Elective Units		0
Total Units for the BS Degree		**128-136**

Upon successful completion of this program, students will be able to:

- design, configure, and validate secure routed/switched networks and perimeter defenses using enterprise networking and firewall security platforms .
- deploy cloud workloads and hybrid integrations with secure networking, identity, monitoring, and resilience controls using cloud administration and cloud architecture competencies.
- secure virtualization-based environments (segmentation, hardening baselines, patch/upgrade strategy, backup/recovery validation) suitable for modern cyber labs and enterprise deployments.
- assess identity protection controls to reduce account takeover and lateral movement risk in cloud/hybrid environments.
- plan and execute ethical hacking workflows (recon, vulnerability validation, exploitation in controlled conditions) and deliver professional findings and prioritized mitigations.
- triage and investigate security events, apply automation/scripting and AI-assisted analytics to improve detection/response speed and consistency, perform device/network forensics, and communicate results through professional writing, project execution, and internship-based practice.
- implement robust security controls and risk-mitigation frameworks, ensuring all project lifecycles are built upon a foundation of proactive defense and resilience.