Government and Public Administration Career Cluster
Army JROTC Cyber 1
Course Number: 28.03900

Course Description:

The course begins with fundamental JROTC Leadership Training. Cyber year one focuses on the foundational skills needed to begin a pathway into cybersecurity. It begins with an introduction to ethics and cybersecurity, moves on to global connectivity, and then transitions to understanding hardware, operating systems, networks, cryptography, and operating procedures. The course ends with a service learning-oriented capstone project that encourages problem solving and team building. This course covers topics associated with CompTIA A+ certification.

Professional communication skills and practices, problem-solving, ethical, and legal issues, and the impact of effective presentation skills are enhanced in this course to prepare students to be college and career ready. Employability skills are integrated into activities, tasks, and projects throughout the course standards to demonstrate the skills required by business and industry. Competencies in the co-curricular student organizations are integral components of both the employability skills standards and content standards for this course.

Army JROTC Cyber 1 is the first course in the Army JROTC Cybersecurity pathway in the Government and Public Administration career cluster. There is no pre-requisite for this course.

Course Standard 1

GPA-ACYB1-1

The following standard is included in all CTAE courses adopted for the Career Cluster/Pathways. Teachers should incorporate the elements of this standard into lesson plans during the course. The topics listed for each element of the standard may be addressed in differentiated instruction matching the content of each course. These elements may also be addressed with specific lessons from a variety of resources. This content is not to be treated as a unit or separate body of knowledge but rather integrated into class activities as applications of the concept.

Standard: Demonstrate employability skills required by business and industry.

The following elements should be integrated throughout the content of this course.

1.1   Communicate effectively through writing, speaking, listening, reading, and interpersonal abilities.

Person-to-Person Etiquette	Telephone and Email Etiquette	Cell Phone and Internet Etiquette	Communicating At Work	Listening
Interacting with Your Boss	Telephone Conversations	Using Blogs	Improving Communication Skills	Reasons, Benefits, and Barriers
Interacting with Subordinates	Barriers to Phone conversations	Using Social Media	Effective Oral Communication	Listening Strategies
Interacting with Co-workers	Making and Returning Calls		Effective Written Communication	Ways We Filter What We Hear
Interacting with Suppliers	Making Cold Calls		Effective Nonverbal Skills	Developing a Listening Attitude
	Handling Conference Calls		Effective Word Use	Show You Are Listening
	Handling Unsolicited Calls		Giving and Receiving Feedback	Asking Questions
				Obtaining Feedback
				Getting Others to Listen

Nonverbal Communication	Written Communication	Speaking	Applications and Effective Résumés
Communicating Nonverbally	Writing Documents	Using Language Carefully	Completing a Job Application
Reading Body Language and Mixed Messages	Constructive Criticism in Writing	One-on-One Conversations	Writing a Cover Letter
Matching Verbal and Nonverbal communication		Small Group Communication	Things to Include in a Résumé
Improving Nonverbal Indicators		Large Group Communication	Selling Yourself in a Résumé
Nonverbal Feedback		Making Speeches	Terms to Use in a Résumé
Showing Confidence Nonverbally		Involving the Audience	Describing Your Job Strengths
Showing Assertiveness		Answering Questions	Organizing Your Résumé
		Visual and Media Aids	Writing an Electronic Résumé
		Errors in Presentation	Dressing Up Your Résumé

1.2 Demonstrate creativity by asking challenging questions and applying innovative procedures and methods.

Teamwork and Problem Solving	Meeting Etiquette
Thinking Creatively	Preparation and Participation in Meetings
Taking Risks	Conducting Two-Person or Large Group Meetings
Building Team Communication	Inviting and Introducing Speakers
	Facilitating Discussions and Closing
	Preparing Visual Aids
	Virtual Meetings

1.3 Exhibit critical thinking and problem-solving skills to locate, analyze and apply information in career planning and employment situations.

Problem Solving	Customer Service	The Application Process	Interviewing Skills	Finding the Right Job
Transferable Job Skills	Gaining Trust and Interacting with Customers	Providing Information, Accuracy and Double Checking	Preparing for an Interview	Locating Jobs and Networking
Becoming a Problem Solver	Learning and Giving Customers What They Want	Online Application Process	Questions to Ask in an Interview	Job Shopping Online
Identifying a Problem	Keeping Customers Coming Back	Following Up After Submitting an Application	Things to Include in a Career Portfolio	Job Search Websites
Becoming a Critical Thinker	Seeing the Customer's Point	Effective Résumés:	Traits Employers are Seeking	Participation in Job Fairs
Managing	Selling Yourself and the Company	Matching Your Talents to a Job	Considerations Before Taking a Job	Searching the Classified Ads
	Handling Customer Complaints	When a Résumé Should be Used		Using Employment Agencies
	Strategies for Customer Service			Landing an Internship
				Staying Motivated to Search

1.4 Model work readiness traits required for success in the workplace including integrity, honesty, accountability, punctuality, time management, and respect for diversity.

Workplace Ethics	Personal Characteristics	Employer Expectations	Business Etiquette	Communicating at Work
Demonstrating Good Work Ethic	Demonstrating a Good Attitude	Behaviors Employers Expect	Language and Behavior	Handling Anger
Behaving Appropriately	Gaining and Showing Respect	Objectionable Behaviors	Keeping Information Confidential	Dealing with Difficult Coworkers
Maintaining Honesty	Demonstrating Responsibility	Establishing Credibility	Avoiding Gossip	Dealing with a Difficult Boss
Playing Fair	Showing Dependability	Demonstrating Your Skills	Appropriate Work Email	Dealing with Difficult Customers
Using Ethical Language	Being Courteous	Building Work Relationships	Cell Phone Etiquette	Dealing with Conflict
Showing Responsibility	Gaining Coworkers' Trust		Appropriate Work Texting	
Reducing Harassment	Persevering		Understanding Copyright	
Respecting Diversity	Handling Criticism		Social Networking	
Making Truthfulness a Habit	Showing Professionalism			
Leaving a Job Ethically				

1.5 Apply the appropriate skill sets to be productive in a changing, technological, diverse workplace to be able to work independently and apply teamwork skills.

Expected Work Traits	Teamwork	Time Management
Demonstrating Responsibility	Teamwork Skills	Managing Time
Dealing with Information Overload	Reasons Companies Use Teams	Putting First Things First
Transferable Job Skills	Decisions Teams Make	Juggling Many Priorities
Managing Change	Team Responsibilities	Overcoming Procrastination
Adopting a New Technology	Problems That Affect Teams	Organizing Workspace and Tasks
	Expressing Yourself on a Team	Staying Organized
	Giving and Receiving Constructive Criticism	Finding More Time
		Managing Projects
		Prioritizing Personal and Work Life

1.6 Present a professional image through appearance, behavior, and language.

On-the-Job Etiquette	Person-to-Person Etiquette	Communication Etiquette	Presenting Yourself
Using Professional Manners	Meeting Business Acquaintances	Creating a Good Impression	Looking Professional
Introducing People	Meeting People for the First Time	Keeping Phone Calls Professional	Dressing for Success
Appropriate Dress	Showing Politeness	Proper Use of Work Email	Showing a Professional Attitude
Business Meal Functions		Proper Use of Cell Phone	Using Good Posture
Behavior at Work Parties		Proper Use in Texting	Presenting Yourself to Associates
Behavior at Conventions			Accepting Criticism

International Etiquette			Demonstrating Leadership
Cross-Cultural Etiquette			
Working in a Cubicle			

Leadership Education Training

Course Standard 2

GPA-ACYB1-2

Cadets will demonstrate organizational awareness through the application of communication skills and explore law, policy, and ethics as related to cybersecurity and Army JROTC.

2.1 Identify how social goals reflect the foundational values held by society; these core societal values are reflected in cybersecurity choices.

2.2 Foster personal growth through careful examination of what it means to utilize ethical reflection and judgement to consider potential harms, benefits, and tradeoffs involved in cybersecurity.

2.3 Interpret how ethical foundations are applied to situations rising from the interconnected world through examining diverse ethical dilemmas arising from cybersecurity practices that can cause ethical conflicts.

2.4 Compare various cybersecurity career paths to prepare for expanding job types related to cybersecurity.

2.5 Explore cybersecurity careers related to skills being taught and tie these careers to opportunities in industry, military, and associated work roles.

Introduction to Cybersecurity

Course Standard 3

GPA-ACYB1-3

Identify and apply basic concepts of cybersecurity, the Central Intelligence Agency triad, and types of cybersecurity attacks and associated risks.

3.1 List and describe the fundamental concepts of the cybersecurity discipline and put them into practice to provide system security.

3.2 Describe cybersecurity's reliance on confidentiality, integrity, and availability – the Confidentiality, Integrity, and Availability (CIA) triad – and how it is implemented.

3.3 Cadets will be able to identify and describe common attack types and adversary types.

3.4 Cadets will be able to identify/analyze cybersecurity risk through the measure of potential damage or loss a vulnerability could cause weighed against the likelihood of an attack.

Global Connectivity

Course Standard 4

GPA-ACYB1-4

Identify and explain key concepts of global connectivity including societal responses, the cyber system, networked systems and the evolution of the Internet.
  4.1 Discuss key historic events related to the evolution of computers and cybersecurity and delineate the impact of these events on society.
  4.2 Recognize and analyze online and offline behaviors in societies (i.e., themselves, peers, families, communities, and countries) and deduce the values that govern these behaviors.
  4.3 Explain how cyberspace is a very large, complex system of cyber systems that include hardware, software, social, economic, and political components.
  4.4 Explain how the decentralized and dynamic nature of networked systems create the potential for a system to fail or behave incorrectly due a component the designer did not even know existed.
  4.5 Summarize and interpret the impact of cybersecurity ideas and events on the evolution of the field.
  4.6 Explain how the idea of the open Internet led us to new innovations that impact our daily lives and our security.

Hardware Standards and Resources

Course Standard 5

GPA-ACYB1-5

Identify, explain, and apply knowledge of computer hardware equipment including assembly, maintenance, troubleshooting and software/hardware interface.
  5.1 Convey that computer hardware refers to the physical parts of a computer and related devices.
  5.2 Identify how hardware and software work together in complex ways to achieve an overall objective.
  5.3 Identify some common hardware-related vulnerabilities.
  5.4 Demonstrate the ability to replace hardware/devices.
  5.5 Demonstrate the installation of components within the display of a laptop.
  5.6 Use appropriate laptop features.
  5.7 Compare and contrast characteristics of various types of other mobile devices.
  5.8 Connect and configure accessories and ports of other mobile devices.
  5.9 Configure basic mobile device network connectivity and application support.
  5.10 Use methods to perform mobile device synchronization.
  5.11 Summarize power supply types and features.
  5.12 Install and configure common devices.
  5.13 Utilize the best practice methodology to resolve problems.
  5.14 Troubleshoot problems related to motherboards, RAM, CPUs, and power.
  5.15 Troubleshoot video, projector, and display issues.
  5.16 Troubleshoot common mobile device issues while adhering to the appropriate procedures.
  5.17 Troubleshoot common problems with printers.
  5.18 Troubleshoot common wired and wireless network problems.

Virtualization and OS

Course Standard 6

GPA-ACYB1-6

Compare and explain the variety of computer systems including cloud, virtual, and physical.

   6.1   Compare and contrast cloud computing concepts.
   6.2   Set up and configure client-side virtualization.
   6.3   Convey that computer hardware refers to the physical parts of a computer and related devices.
   6.4   Describe the hardware components of modern computing environments and their individual functions.
   6.5   Properly use the vocabulary associated with cybersecurity.

Operating Systems

Course Standard 7

GPA-ACYB1-7

Explain and apply software skills to initiate and maintain a network; utilize features of Linux to demonstrate basic cybersecurity operator functions.

   7.1   Explain how cybersystems are complex systems.
   7.2   Develop a script using Windows Command-Line Interface, Windows Management Instrumentation Command-Line (WMIC), and PowerShell to bring a network to an operational state per practical exercises.
   7.3   Identify Windows processes using Sysinternals tools to maintain it in an operational state.
   7.4   Demonstrate using the Registry hierarchy and primary components to check for suspicious activity in an operational environment.
   7.5   Demonstrate security techniques on user accounts using WMIC, Windows Command-Line Interface, and PowerShell to maintain an operational environment.
   7.6   Demonstrate an understanding of Linux Core Features by employing commands using common shells to analyze a Linux file system and parse HTML.
   7.7   Describe the Linux boot process.
   7.8   Identify Linux processes to bring a network to an operational state per the instruction given.
   7.9   Analyze an audit log, identifying all activities that affect an operation, procedure, event, file, or document.
   7.10 As a collection operator in an operational environment, Cadets will apply Linux operating system commands in accordance with applicable policy, instructions, doctrine, tactics, techniques, and procedures.

Introduction to Cryptography

Course Standard 8

GPA-ACYB1-8

Investigate the uses of cryptography and apply key cryptography concepts.
  8.1 Properly use the vocabulary associated with cybersecurity.
  8.2 Define cryptography and explain how it is used in data security.
  8.3 Convert numbers into scientific notation.
  8.4 Perform Modulo-2 addition.

Networking

Course Standard 9

GPA-ACYB1-9

Explain secure network concepts and demonstrate the ability to set up a secure network.
  9.1 Differentiate between threats, vulnerabilities, and attacks.
  9.2 Analyze how the cybersecurity attack lifecycle/kill chain is essential to adversarial thinking.
  9.3 Convey that computer hardware refers to the physical parts of a computer and related devices.
  9.4 Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.
  9.5 Compare and contrast common networking hardware devices.
  9.6 Install and configure a basic wired/wireless Small Office/Home Office (SOHO) network.
  9.7 Compare and contrast wireless networking protocols.
  9.8 Summarize the properties and purposes of services provided by networked hosts.
  9.9 Explain common network configuration concepts.
  9.10 Compare and contrast Internet connection types, network types, and their features.
  9.11 Use appropriate networking tools.
  9.12 Demonstrate security techniques on user accounts using WMIC, Windows Command-Line Interface, and PowerShell to maintain an operational environment.
  9.13 Demonstrate their skills by applying Linux concepts in support of offensive and defensive cyber operations and successfully passing the Linux final examination

Security

Course Standard 10

GPA-ACYB1-10

Apply cybersecurity skills in a variety of scenarios including system security, threat evaluation, wireless security protocols, data security and disposal.
  10.1 Describe potential system attacks and the actors that might perform them.
  10.2 Properly use the vocabulary associated with cybersecurity.
  10.3 Evaluate physical and environmental security concerns.
  10.4 Identify physical controls that are used to secure data.
  10.5 Summarize the importance of physical security measures and explain logical security concepts.
  10.6 Compare and contrast wireless security protocols and authentication methods.

10.7   Detect, remove, and prevent malware using appropriate tools and methods.
10.8   Compare and contrast social engineering, threats, and vulnerabilities.
10.9   Compare and contrast the differences of basic Microsoft Windows OS security
         settings.
10.10   Implement security best practices to secure a workstation and mobile devices.
10.11   Implement appropriate data destruction and disposal methods.

Operating Procedures

Course Standard 11

GPA-ACYB1-11

Identify, describe, and apply cybersecurity practices including security testing, documentation, change management, disaster prevention and recovery methods.

11.1   Describe appropriate measures to be taken should a system compromise occur.
11.2   Properly use the vocabulary associated with cybersecurity.
11.3   Conduct standard security testing and assessments.
11.4   Explain how cybersystems are complex systems.
11.5   Compare and contrast best practices associated with types of documentation.
11.6   Implement basic change management best practices.
11.7   Implement basic disaster prevention and recovery methods.
11.8   Explain common safety procedures, environmental impacts and appropriate controls, and the processes for addressing prohibited content/activity, and privacy, licensing, and policy concepts.
11.9   Utilize proper communication techniques and professionalism.
11.10   Identify the basics of scripting.
11.11   Utilize remote access technologies.

JROTC Leadership Education Training & Capstone Project

Course Standard 12

GPA-ACYB1-12

Cadets will work with a team to complete a cybersecurity service-learning project to benefit the school, community, or region.

12.1   Apply the knowledge and skills acquired in their courses to a service-learning project.
12.2   Extend academic experience into areas of personal career interests, to include working with new ideas, organizations, and individuals in a service-learning environment.
12.3   Apply creative and critical thinking about academic, professional, and/or social issues to further develop analytical and ethical leadership skills.