Principles of Cyber Defense and Ethics

Exam Information	Description
Exam number **831** **Items** **31** **National Career Cluster** **Digital Technology** **Certification available** **No, in pilot status**	This course will give you a broad perspective on Cybersecurity and how it affects different aspects of an organization. You will learn how to leverage the security features of modern operating systems, identify and mitigate the vulnerabilities of wireless and wired networks, and safeguard your own and your employer's information assets. You will also gain an insight into the various Cybersecurity career paths and how to prepare yourself for advanced topics such as ethical hacking, incident response, and digital forensics. This course will help you develop the skills and knowledge required to succeed in the fast-growing field of Cybersecurity.

Exam Blueprint and Performance Skills

Standard	Percentage of exam score
1. Security Careers and Ethics*	6%
2. Security Basics	37%
3. Social Engineering	9%
4. Authentication Methods	14%
5. Encryption	9%
6. Malware	11%
7. Network Security	14%

*Includes performance skill evaluation

Standard 1 - Security Careers and Ethics (6% of exam score)

Objective 1 Understand Careers and Professional organizations in Cybersecurity.

1. Identify careers in Cybersecurity.
2. Identify education and/or certifications needed to work in the Cybersecurity field.
3. Identify Cybersecurity professional organizations.

Objective 2 Understand Ethics of Cybersecurity

1. Understand the different categories of hacking including: authorized hacker, unauthorized hacker, semi-authorized hacker.
2. Understand the purpose of an Acceptable Use Policy.
3. Understand the major events in Cybersecurity that have influenced the laws and governance of Cybersecurity.

Optional: Standard performance evaluations on the final page of this document

Standard 2 - Security Basics (37%)

Objective 1 Understand core security principles

1. Understand the concepts of the cia triad (confidentiality, integrity, availability).
2. Understand how threat and risk impact principles; principles of least privilege.
3. Understand the purpose of the NIST Security Framework.
4. Understand what Personally Identifiable Information (PII) is and the importance of securing it.

Objective 2 Understand physical security

1. Understand site security - tailgating, limited access, door locks, server locks, cable locks.
2. Understand device security -
3. Removable devices and drives - juice jacking and evil usbs
4. Access control - remote device wipe, password lockout, data recovery on lost / stolen devices, and device destruction.
5. Reformatting a device - partial vs full write.

Objective 3 Understand Internet security

1. Understand browser settings including things like password management, cookies, and storing personal information.
2. Understand the difference between http and https. How to identify if a website is secure.

Standard 3 - Social Engineering (9%)

Objective 1 Understand Social Engineering

1. Understand the definition and intent of social engineering.
2. Understand the principles of social engineering - authority, intimidation, consensus, scarcity, urgency, familiarity/ trust.

Objective 2 Understand types of Social Engineering

1. Understand the methods and prevention of the following social engineering methods - Phishing (and similar attacks), tailgating, shoulder surfing, dumpster diving, reconnaissance, and watering holes.

Standard 4 - Authentication Methods (14%)

Objective 1 Understand user authentication

1. Understand multifactor, smart cards, and RADIUS
2. Understand the certificate chain, biometrics, Kerberos, and time skew using Run As to perform administrative tasks and password reset procedures.
3. Disable Log On Locally and guest accounts.

Objective 2 Understand permissions.

1. Understand the following: file; share; registry; Active Directory; enabling or disabling inheritance.
2. Understand behavior when copying and moving files within the same disk or onto another disk.
3. Understand basic and advanced user permissions; take ownership; delegation.
4. Understand multiple user groups and that users can belong to multiple groups.
5. Understand operating systems native encryption options.

Objective 3 Understand password policies

1. Understand password policies: password complexity; account lockout; password length; password history; enforce by using group policies; and common attack methods; avoid common passwords or phrases.

Standard 5 - Encryption (9%)

Objective 1 Understand encryption

1. Understand the history of encryption - Caesar, Enigma, Vigenere ciphers.
2. Understand public key and private keys and how they are implemented.
3. Understand the implementation and recognize the following encryption algorithms - MD5, SHA-256, AES, RSA.
4. Understand certificate properties; certificate services; PKI/ certificate services infrastructure; and token devices.

Optional: Standard performance evaluations on the final page of this document

Standard 6 - Malware (11%)

Objective 1 Understand malware

1. Understand the major malware attacks throughout history - WannaCry, Stuxnet, Code Red, Morris worm, iloveyou.
2. Understand the difference between common pieces of malware - viruses, worms, Trojans, ransomware, spyware, adware, and rogue security software.

Objective 2 Understand vulnerabilities

1. Understand the following vulnerabilities: buffer overflow, backdoors, Spectre, Meltdown, log4j.

Objective 3 Understand how to protect against malware & vulnerabilities

1. Understand how vulnerabilities are prevented.
2. Understand how and why you should keep your software and devices up to date.
3. Understand antivirus software and how to remove a virus when a machine is infected and verify that the virus is removed.

Standard 7 - Network Security (14%)

Objective 1 Understand dedicated firewalls.

1. Understand the types of hardware firewalls and their characteristics.
2. Understand when to use a hardware firewall instead of a software firewall.
3. Understand the difference between stateful vs. stateless inspection.

Objective 2 Understand Network Access Protection (NAP).

1. Understand the purpose of NAP and when to use NAP.

Objective 3 Understand network isolation.

1. Understand network isolation: VLANs; routing; NAT; VPN; IPsec;
2. Understand device isolation: DMZ(Demilitarized zone); Server and Domain Isolation.
3. Understand the purpose of a honeypot.

Objective 4 Understand protocol security.

1. Understand the following: protocol spoofing; IPsec; tunneling; DNSsec;
2. Understand how a network sniffer works and how to use one on a network.

Objective 5 Understand wireless security.

1. Understand advantages and disadvantages of specific security types; network keys, SSID, and MAC filters.

Workplace Skills

1. Problem Solving
2. Critical Thinking
3. Legal Requirements/Expectations

Performance Skills Evaluation

Exam name: Principles of Cyber Defense and Ethics

Candidate Name: _____

Performance assessments may be completed and evaluated any time before the certification is issued. The following performance skills can be used in connection with the associated standards and exam. The evaluator will function as the subject matter expert to determine if the candidate meets the skills requirements with a Yes/No for passing.

Standard 1 – Self Awareness and Careers	**Pass:**
• Identify four personal values and explain how these values affect behavior and choices. • Research a Human Services career that includes educational requirements, skill development, and income potential. • Will practice communication skills through public speaking using one or more of the following activities: memorized speech, prepared speech, extemporaneous speech, parliamentary practice, group presentation, or serving in a leadership capacity.	

Evaluator Name: _____ **Date:** _____