Mandatory Knowledge Units

1.0 Core2Y

1.1 Basic Data Analysis
The intent of this Knowledge Unit is to provide students with basic abilities to manipulate data into meaningful information.

1.1.1 Topics
- Summary Statistics
- Graphing / Charts
- Spreadsheet Functions
- Problem solving

1.1.2 Outcomes
Students will be able to:
- Apply standard statistical inference procedures to draw conclusions from data.

1.2 Basic Scripting or Introductory Programming
The intent of this Knowledge Unit is to provide students with the ability to create simple scripts/programs to automate and perform simple operations. This knowledge should include basic security practices in developing scripts/programs (e.g., bounds checking, input validation).

1.2.1 Topics
- *Basic Security
  - Bounds checking, input validation
- Program Commands
- Program Control Structures
- Variable Declaration
- Debugging
- Scripting Language (e.g. PERL, Python, BASH, VB Scripting, Powershell)
- *Basic Boolean logic/operations
  - AND / OR / XOR / NOT

1.2.2 Outcomes
Students will be able to:
- Demonstrate their proficiency in the use of scripting languages to write simple scripts (e.g., to automate system administration tasks).
- Write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL).
- Write simple linear and looping scripts.

1.3 Cyber Defense
The intent of this Knowledge Unit is to provide students with a basic awareness of the options available to mitigate threats within a system.

1.3.1 Topics:
- Network mapping (enumeration and identification of network components)
- *Network security techniques and components
  - Access controls, flow control, cryptography, firewalls, intrusion detection systems, etc.
- Applications of Cryptography

* = Can include a summary justification for that section.
2014 Mandatory Knowledge Unit Checklist – 4 Year\(^{+}\) Programs

**1.3.2 Outcomes:**
Students will be able to:
- Describe potential system attacks and the actors that might perform them
- Describe cyber defense tools, methods and components
- Apply cyber defense methods to prepare a system to repel attacks
- Describe appropriate measures to be taken should a system compromise occur.

### 1.4 Cyber Threats
The intent of this Knowledge Unit is to provide students with basic information about the threats that may be present in the cyber realm.

**1.4.1 Topics:**
- Adversaries and targets
- Motivations and Techniques
- The Adversary Model (resources, capabilities, intent, motivation, risk aversion, access)
- *Types of Attacks
  - Password guessing / cracking
  - Backdoors / trojans / viruses / wireless attacks
  - Sniffing / spoofing / session hijacking
  - Denial of service / distributed DOS / BOTs
  - MAC spoofing / web app attacks / 0-day exploits
- Vulnerabilities that enable attacks
- Attack Timing (within x minutes of being attached to the net)
- Social Engineering
- Events that indicate an attack is/has happened
- Legal Issues
- Attack surfaces / vectors
- Attack trees
- Insider problem
- Covert Channels
- Threat Information Sources (e.g., CERT)

**1.4.2 Outcomes:**
Students will be able to:
- Identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations, aversion to risk
- Describe different types of attacks and their characteristics

\* = Can include a summary justification for that section.
1.5 Fundamental Security Design Principles

The intent of this Knowledge Unit is to provide students with basic security design fundamentals that help create systems that are worthy of being trusted.

1.5.1 Topics:

___ Separation (of domains)
___ Isolation
___ Encapsulation
___ Least Privilege
___ Simplicity (of design)
___ Minimization (of implementation)
___ Fail Safe Defaults / Fail Secure
___ Modularity
___ Layering
___ Least Astonishment
___ Open Design
___ Usability

1.5.1 Outcomes:

Students will be able to:

___ List the first principles of security
___ Describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies
___ Analyze common security failures and identify specific design principles that have been violated
___ Identify the needed design principle when given a specific scenario
___ Describe why good human machine interfaces are important to system use
___ Understand the interaction between security and system usability and the importance for minimizing the affects of security mechanisms

1.6 Information Assurance Fundamentals

The intent of this Knowledge Unit is to provide students with basic concepts of information assurance fundamentals.

1.6.1 Topics

___ Threats and Adversaries
___ Vulnerabilities and Risks
___ Basic Risk Assessment
___ Security Life-Cycle
___ Intrusion Detection and Prevention Systems
___ Cryptography
___ Data Security (in transmission, at rest, in processing)
___ Security Models
___ Access Control Models (MAC, DAC, RBAC)
___ Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy
___ Security Mechanisms (e.g., Identification/Authentication, Audit)

* = Can include a summary justification for that section.
1.6.2 Outcomes
Students will be able to:
- List the fundamental concepts of the Information Assurance / Cyber Defense discipline
- Describe how the fundamental concepts of cyber defense can be used to provide system security
- Examine the architecture of a typical, complex system and identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed

1.7 Introduction to Cryptography
The intent of this Knowledge Unit is to provide students with a basic ability to understand where and how cryptography is used.

1.7.1 Topics
- Symmetric Cryptography (DES, Twofish)
- *Public Key Cryptography
  - Public Key Infrastructure
  - Certificates
- *Hash Functions (MD4, MD5, SHA-1, SHA-2, SHA-3)
  - For integrity
  - For protecting authentication data
  - Collision resistance
- Digital Signatures (Authentication)
- Key Management (creation, exchange/distribution)
- Cryptographic Modes (and their strengths and weaknesses)
- Types of Attacks (brute force, chosen plaintext, known plaintext, differential and linear cryptanalysis, etc.)
- Common Cryptographic Protocols
- DES -> AES (evolution from DES to AES)
- Security Functions (data protection, data integrity, authentication)

1.7.2 Outcomes
Students will be able to:
- Identify the elements of a cryptographic system
- Describe the differences between symmetric and asymmetric algorithms
- Describe which cryptographic protocols, tools and techniques are appropriate for a given situation
- Describe how crypto can be used, strengths and weaknesses, modes, and the issues that must be addressed in an implementation (e.g., key management), etc

1.8 Information Technology System Components
The intent of this Knowledge Unit is to provide students with an understanding of the basic components in an information technology system and their roles in system operation.

1.8.1 Topics
- Workstations
- Servers
- Network Storage Devices
- Routers / Switches / Gateways

* = Can include a summary justification for that section.
1.8.2 Outcomes
Students will be able to:
___ Describe the hardware components of modern computing environments and their individual functions

1.9 Networking Concepts
The intent of this Knowledge Unit is to provide students with basic understanding of network components and how they interact.

1.9.1 Topics
___ Overview of Networking (OSI Model)
___ Network Media
___ Network architectures (LANs, WANs)
___ Network Devices (Routers, Switches, VPNs, Firewalls)
___ Network Services
___ Network Protocols (TCP/IP, HTTP, DNS, SMTP, UDP)
___ Network Topologies
___ Overview of Network Security Issues

1.9.2 Outcomes
Students will be able to:
___ Describe the fundamental concepts, technologies, components and issues related to communications and data networks.
___ Describe a basic network architecture given a specific need and set of hosts/clients.
___ Track and identify the packets involved in a simple TCP connection (or a trace of such a connection).
___ Use a network monitoring tool (e.g., WireShark).
___ Use a network mapping tool (e.g., Nmap).

1.10 Policy, Legal, Ethics and Compliance
The intent of this Knowledge Unit is to provide students with and understanding of information assurance in context and the rules and guidelines that control them.

1.10.1 Topics
___ HIPAA / FERPA
___ Computer Security Act
___ Sarbanes – Oxley
___ Gramm – Leach – Bliley
___ Privacy (COPPA)
___ Payment Card Industry Data Security Standard (PCI DSS)
___ State, US and international standards / jurisdictions
___ Laws and Authorities
___ US Patriot Act
___ BYOD issues

* = Can include a summary justification for that section.
1.10.2 Outcomes

Students will be able to:

- List the applicable laws and policies related to cyber defense and describe the major components of each pertaining to the storage and transmission of data
- Describe their responsibilities related to the handling of information about vulnerabilities
- Describe how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it

1.11 Systems Administration

The intent of this Knowledge Unit is to provide students with skill to perform basic operations involved in system administration.

1.11.1 Topics

- OS Installation
- User accounts management
- Password policies
- Authentication Methods
- Command Line Interfaces
- Configuration Management
- Updates and patches
- Access Controls
- Logging and Auditing (for performance and security)
- Managing System Services
- Virtualization
- Backup and Restoring Data
- File System Security
- Network Configuration (port security)
- Host (Workstation/Server) Intrusion Detection
- Security Policy Development

1.11.2 Outcomes

Students will be able to:

- Apply the knowledge gained to successfully install and securely configure, operate and maintain a commodity OS, to include: setting up user accounts, configuring appropriate authentication policies, configuring audit capabilities, performing back-ups, installing patches and updates, reviewing security logs, and restoring the system from a backup

2.0 Core to 4 year+ only

2.1 Database Management Systems

The intent of this Knowledge Unit is to provide students with the skills to utilize database management system to solve specific problems.

2.1.1 Topics

- Overview of database types (e.g., flat, relational, network, object-oriented)
- SQL (for queries)
- Advanced SQL (for DBMS administration – e.g., user creation/deletion, permissions and access controls)

* = Can include a summary justification for that section.
2.1.2 Outcomes
Students will be able to:

- List the most common structures for storing data in a database management system
- Configure a commodity DBMS for secure access
- Describe alternatives to relational DBMSs and their unique security issues
- Describe the role of a database, a DBMS, and a database server within a complex system supporting multiple applications
- Demonstrate basic SQL proficiency for table creation, data insertion and data query
- Describe DBMS access controls and privilege levels and apply them to a simple database
- Develop a DB structure for a specific system/problem.

2.2 Network Defense
The intent of this Knowledge Unit is to teach students the techniques that can be taken to protect a network and communication assets from cyber threats.

2.2.1 Topics
- Implementing IDS/IPS
- Implementing Firewalls and VPNs
- Defense in Depth
- Honeypots and Honeynets
- Network Monitoring
- Network Traffic Analysis
- Minimizing Exposure (Attack Surface and Vectors)
- Network Access Control (internal and external)
- DMZs / Proxy Servers
- Network Hardening
- Mission Assurance
- Network Policy Development and Enforcement
- Network Operational Procedures
- Network Attacks (e.g., session hijacking, Man-in-the-Middle)

2.2.2 Outcomes
Students will be able to:

- Describe the various concepts in network defense.
- Apply their knowledge to implement network defense measures.
- Use a network monitoring tool (e.g., WireShark).
- Use a network mapping tool (e.g., Nmap).

2.3 Network Technology and Protocols
The intent of this Knowledge Unit is to provide students with an understanding of the components in a network environment, their roles, and communication methods.

2.3.1 Topics
- Network Architectures
- Networks Infrastructure

* = Can include a summary justification for that section.
2.3.2 Outcomes
Students will be able to:

- Apply their knowledge of network technologies to design and construct a working network
- Analyze a trace of packets to identify the establishment of a TCP connection
- Demonstrate the use of a network monitor to display packets

2.4 Operating Systems Concepts
The intent of this Knowledge Unit is to provide students with an understanding of the roles of an operating system, its basic functions, and the services provided by the operating system.

2.4.1 Topics

- Privileged and non-privileged states
- Processes and Threads (and their management)
- Memory (real, virtual, and management)
- Files Systems
- Access Controls (Models and Mechanisms)
  - Access control lists
  - Virtualization / Hypervisors
- How does the an OS protect itself from attack?
- *Fundamental Security Design Principles as applied to an OS
  - Domain separation, process isolation, resource encapsulation, least privilege

2.4.2 Outcomes
Students will be able to:

- Identify the major concepts in modern operating systems and the basic security issues in OS design and implementation (how the first principles of security apply to operating systems)

2.5 Probability and Statistics
The intent of this Knowledge Unit is to provide students with the ability to use basic statistics to analyze and attach meaning to datasets.

2.5.1 Topics

- Probability as a concept
- Random variables/events
- Odds of an event happening
- Data Interpretation
- Statistical Problem Solving
- Probability Distributions

2.5.2 Outcomes
Students will be able to:

- Evaluate probabilities to solve applied problems
- Describe how basic statistics and statistical methods can be applied in a given situation

* = Can include a summary justification for that section.
2.6 Programming

The intent of this Knowledge Unit is to provide students with the skills necessary to implement algorithms using programming languages to solve problems.

2.6.1 Topics

- Programming Language, such as: C
- Programming constructs and concepts variables, strings, assignments, sequential execution, loops, functions
- Security issues, such as type checking and parameter validation
- *Basic Boolean logic/operations
  - AND / OR / XOR / NOT

2.6.2 Outcomes

Students will be able to:

- Demonstrate proficiency in the use of a programming language to solve complex problems in a secure and robust manner
- Write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL)
- Demonstrate the ability to design and develop basic programs for modern computing platforms (e.g., PC, cloud, mobile, web)