الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

# The Saudi Cybersecurity Higher Education Framework

## SCyber-Edu–2: 2026

TLP: Clear

Document Classification: Public

**Disclaimer:** Please refer to the National Cybersecurity Authority's website (https://nca.gov.sa), to obtain the latest version of this document

In The Name Of Allah,
The Most Gracious,
The Most Merciful

**Disclaimer: The following framework will be governed by and implemented in accordance with the laws of the Kingdom of Saudi Arabia, and must be subject to the exclusive jurisdiction of the courts of the Kingdom of Saudi Arabia. Therefore, the Arabic version will be the binding language for all matters relating to the meaning or interpretation of this document.**

## Traffic Light Protocol (TLP):

This marking protocol is widely used around the world. It has four colors (traffic lights):

**Red (Personal, Confidential, and for the Intended Recipient Only)**

The recipient has no right to share the information classified in red with any person outside the defined range of recipients, either inside or outside the entity, beyond the scope specified for receipt.

**Amber+ Strict (Sharing within the entity)**

The recipient may share the information only with the intended recipients inside the entity.

**Amber (Restricted Sharing)**

The recipient may share the information only with the intended recipients inside the entity or with recipients who are required to take action related to the shared information.

**Green (Sharing within the Same Community)**

The recipient may share information with other recipients inside the entity or outside it within the same sector or with a related entity. However, it is not allowed to exchange or publish this information on public channels.

**Clear (No Restrictions)**

# Updates to Document

| Version | Date | Changes |
|---|---|---|
| 1.0 | October 2020 | Initial version |
| 2.0 | November 2026 | Major revision of Knowledge Units (KUs), addition of specialized program tracks, and alignment with updated national and international cybersecurity frameworks. Please refer to Appendix (B) for the details of the updates. |

# Table of Contents


1. Introduction ..... 10

1.1 Scope ..... 11

1.2 Methodology ..... 12

1.3 Prerequisites and Mathematics Requirements ..... 15

1.4 Structure of the Document ..... 15

2. Programs ..... 16

2.1 Intermediate Diploma ..... 16

2.2 Bachelor (Cybersecurity Track) ..... 18

2.3 Bachelor (Cybersecurity Major) ..... 20

2.4 Higher Diploma for IT Background ..... 22

2.5 Higher Diploma for Non-IT Background ..... 24

2.6 Master (Cybersecurity Track) ..... 26

2.7 Master (Cybersecurity Major) ..... 28

2.8 Doctoral ..... 31

3 Knowledge Units (KUs) ..... 35

Cybersecurity Fundamentals (CSF) ..... 35

Cybersecurity Design Principles (CDP) ..... 36

IT Systems Components (ISC) ..... 37

Basic Cryptography (BCY) ..... 39

Basic Networking (BNW) ..... 40

Basic Scripting and Programming (BSP) ..... 41

Network Defense (NDF) ..... 42

Operating Systems Concepts (OSC) ..... 43

Cyber Threats (CTH) ..... 44

Cybersecurity Planning and Management (CPM) ..... 45

Policy, Legal, Ethics and Compliance (PLE) ..... 46

Security Program Management (SPM) ..... 47

Security Risk Analysis (SRA) ..... 48

Advanced Algorithms (AAL) ..... 49

Access Control (ACC) ..... 50
Advanced Cryptography (ACR) ..... 51
Algorithms (ALG) ..... 53
Advanced Network Technology and Protocols (ANT) ..... 54
Analog Telecommunications (ATC) ..... 55
Analytical Tools (ATT) ..... 56
Awareness and Understanding (AUU) ..... 57
Business Continuity, Disaster Recovery and Incident Management (BDR) ..... 58
Cloud Computing (CCO) ..... 59
Cryptography (CRY) ..... 60
Cryptography Engineering (CRE) ..... 62
Cyber Crime (CCR) ..... 63
Cybersecurity Ethics (CSE) ..... 64
Cyber-Physical System (CPS) ..... 65
Databases (DAT) ..... 66
Data Administration (DBA) ..... 67
Digital Communications (DCO) ..... 68
Digital Forensics (DFS) ..... 69
Data Integrity and Authentication (DIA) ..... 70
Deep Learning (DLL) ..... 71
Database Management Systems (DMS) ..... 72
Distributed Systems Architecture (DSA) ..... 73
Data Structures (DST) ..... 74
Device Forensics (DVF) ..... 75
Embedded Systems (ESY) ..... 76
Forensic Accounting (FAC) ..... 77
Formal Methods (FMD) ..... 78
Mathematical Foundations of Cryptography (FCY) ..... 79
Fraud Prevention and Management (FPM) ..... 81
Hardware Architecture (HAA) ..... 82
Hardware/Firmware Security (HFS) ..... 83
Host Forensics (HOF) ..... 84

Hardware Reverse Engineering (HRE) ..... 85
Information Assurance Architectures (IAA) ..... 86
Information Assurance Compliance (IAC) ..... 87
Information Assurance Standards (IAS) ..... 88
Industrial Control Systems (ICS) ..... 89
Independent/Directed Study/Research (IDR) ..... 91
Intrusion Detection/Prevention Systems (IDS) ..... 92
Identity Management (IMM) ..... 93
Internet of Things (IoT) ..... 94
Information Storage Security (ISS) ..... 95
Introduction to the Theory of Computation (ITC) ..... 96
Life-Cycle Security (LCS) ..... 97
Low Level Programming (LLP) ..... 98
Media Forensics (MEF) ..... 99
Machine Learning (MLL) ..... 100
Mobile Technologies (MOT) ..... 101
Network Security Administration (NSA) ..... 102
Network Technology and Protocols (NTP) ..... 103
Network Forensics (NWF) ..... 104
Operating Systems Administration (OSA) ..... 105
Operating Systems Hardening (OSH) ..... 106
Operating Systems Theory (OST) ..... 107
Penetration Testing (PTT) ..... 108
QA/Functional Testing (QAT) ..... 109
Radio Frequency Principles (RFP) ..... 110
Software Assurance (SAS) ..... 111
System Control (SCC) ..... 112
Secure Communication Protocols (SCP) ..... 113
Supply Chain Security (SCS) ..... 114
Systems Programming (SPG) ..... 115
Secure Programming Practices (SPP) ..... 116
Software Reverse Engineering (SRE) ..... 117

Software Security Analysis (SSA) ..... 118
Systems Security Engineering (SSE) ..... 119
Vulnerability Analysis (VLA) ..... 120
Virtualization Technologies (VTT) ..... 121
Web Application Security (WAS) ..... 122
Wireless Sensor Networks (WSN) ..... 123

**4. Appendix (A): Examples of Specialized Cybersecurity Programs. 124**

A1. Bachelor of AI in Cybersecurity ..... 124
A2. Master of Cryptography ..... 125
A3. Master of ICS/OT Cybersecurity ..... 126
A4. Master of Cybersecurity Management ..... 127

**5. Appendix (B): Summary of Version Updates ..... 128**

**6. References ..... 129**

# 1. Introduction

As per the mandate of the National Cybersecurity Authority (NCA) that was issued by the Royal Order number 6801, dated October 31, 2017, the NCA is mandated to build the national cybersecurity workforce; to participate in developing education and training programs; to prepare professional standards and frameworks; and to develop and run professional assessment tests related to cybersecurity. Therefore, due to the importance of developing national high-quality academic programs in cybersecurity, the NCA has developed the "Saudi Cybersecurity Higher Education Framework (SCyber-Edu)" to serve as a guide for developing, evaluating, and accrediting cybersecurity higher education programs. This framework was developed by the NCA in cooperation and coordination with the Ministry of Education and the Education and Training Evaluation Commission.

This framework contributes to setting the minimum curriculum requirements of cybersecurity higher education programs to assure their academic quality. The goal of this framework is to ensure that higher education programs in Saudi Arabia develop highly qualified cybersecurity professionals who can join and enrich the national cybersecurity workforce and contribute to the national efforts towards "A resilient, secure and trusted Saudi cyberspace that enables growth and prosperity".

SCyber-Edu is designed in alignment with the Unified Saudi Classification for Educational Levels and Specializations, the National Qualifications Framework (NQF), and the guidelines of the National Center for Academic Accreditation and Evaluation.

## 1.1 Scope

This framework covers the following higher education degree programs in cybersecurity:

1. Intermediate Diploma
2. Bachelor
3. Higher Diploma
4. Master
5. Doctoral

The framework can be used and applied to cybersecurity degree programs offered by public and private post-secondary educational institutions in Saudi Arabia.

It is important to note that the Associate Diploma is not covered in this framework. This exclusion is based on the requirements of the Saudi Cybersecurity Workforce Framework- Career Progression (SCyWF-CP 1.0), which establishes the Intermediate Diploma as the minimum educational requirement for any cybersecurity job roles. By this alignment, the NCA ensures that graduates possess the necessary depth of technical competency and knowledge to effectively secure the national cyberspace.

Since cybersecurity is a highly dynamic discipline, the curriculum requirements in this framework will be reviewed and updated periodically to maintain relevance with emerging threats and international standards.

## 1.2 Methodology

Even though the field of cybersecurity is still evolving as compared to other well-established fields such as computer science, several international frameworks for cybersecurity education have been recently developed to ensure the quality of cybersecurity education programs. These include the framework of the National Centers of Academic Excellence in Cyber Defense (CAE-CD) Program [1], ABET Criteria for Accrediting Cybersecurity and Similarly Named Computing Programs, IEEE/ACM Cybersecurity Curricula, and the framework of the NCSC-certified Higher Education Program[2]. These frameworks have major commonalities. These international frameworks have been studied to define the methodology for preparing the Saudi Cybersecurity Higher Education Framework by setting the minimum curriculum requirements for each degree program in cybersecurity in terms of Program Descriptors (PD), through which Program Learning Outcomes can be derived, and Knowledge Units (KUs) that students need to study in the program. As mentioned earlier, the SCyber-Edu is compatible with the Unified Saudi Classification for Educational Levels and Specializations, the National Qualifications Framework (NQF) and the guidelines of the National Center for Academic Accreditation and Evaluation.

The PDs correspond to NQF Level Descriptors which help academic organizations design the Program Learning Outcomes (PLOs) that comprise a set of knowledge, skills and values which graduates are expected to obtain upon completion of the program. The SCyber-Edu is intended to contribute to setting the minimum PDs that need to be considered in writing the PLOs for each degree program. However, an educational institution can add additional PLOs to its cybersecurity programs.

The KUs are thematic groupings that encompass multiple related topics; where the topics cover the required curricular content for each KU. Each KU contains a set of learning outcomes. The KU-specific learning outcomes specify the minimum of what students should know or be able to do after successfully completing the KU. It is important for educational institutions to take into account the depth, expansion and progression of these learning

[1] The CAE-CD program is an initiative sponsored by the National Security Agency and the Department of Homeland Security in the United States of America.

[2] The NCSC-certified higher education program is developed by the National Cyber Security Center in the United Kingdom.

outcomes to suit the level of the program; and to include learning outcomes related to communication skills and values in the curricula.

The SCyber-Edu sets the minimum core KUs that must be covered by the program and provides a list of elective KUs. Educational institutions can offer the desired elective KUs that are relevant to their programs and students can choose from them to complete their graduation requirements. It is important to note that a KU is not necessarily a credit course. A KU may be covered by one or more credit courses and a credit course may cover one or more KUs partially or completely.

For the bachelor's and master's degrees, this framework differentiates between a cybersecurity major degree program and an IT related major degree program with a cybersecurity track within the program.

The KUs are derived from the following sources:

- National Centers of Academic Excellence in Cybersecurity (NCAE-C) – Cyber Defense (CAE-CD) Knowledge Units (KUs) 2024.
- CyBOK, The Cyber Security Body of Knowledge (Version 1.1.0), 2021.
- The IEEE/ACM Cybersecurity Curricula 2017.
- The IEEE/ACM Computer Science Curricula 2023.

The necessary additions and modifications were made to meet the national needs in this field; and to comply with the relevant frameworks in the Kingdom.

For each degree program, SCyber-Edu sets three types of requirements:

1. Admission Requirements: A list of requirements that need to be met prior to admitting a student into the program.

2. Core KUs: Mandatory KUs that a student must complete as part of the graduation requirements. They are categorized as follows:

   - Cybersecurity Core KUs: These represent the minimum common knowledge and skills in cybersecurity and are required in all programs within the framework.
   - Technical Core KUs: These focus primarily on the fundamentals, concepts, and technical skills related to systems architecture, network concepts, software development, and cryptography. These units develop the hands-on capabilities needed to design, implement, and protect technology.

- Non-Technical Core KUs: Focus on the organizational, administrative, and legislative dimensions of cybersecurity, including risk and threat management, governance, compliance, and policy. Although labeled "non-technical," they may still incorporate technical examples to illustrate how management decisions impact security controls.

The classification of each KU is based on its predominant area of focus; labeling a KU as non-technical does not mean it excludes technical content.

3. Elective KUs: A list of elective KUs that an educational institution and/or a student can choose from. A minimum number of these elective KUs must be completed as part of the graduation requirements. In specialized cybersecurity programs, the elective KUs must be directly related to the program's name or title.

## 1.3 Prerequisites and Mathematics Requirements

Some KUs are considered to be prerequisites for other KUs. It is requested that such dependencies are reflected properly in the program of study.

Furthermore, there is a foundational connection between mathematics and many cybersecurity areas; and most undergraduate cybersecurity programs require some foundational mathematics knowledge units. However, the mathematics knowledge units required for a particular program depend heavily on the nature and focus of that program. Therefore, post-secondary educational institutions offering undergraduate programs in cybersecurity are requested to include mathematics knowledge units that are relevant to their programs and that properly meet the prerequisites of the cybersecurity knowledge units in their programs.

## 1.4 Structure of the Document

The rest of this document is organized as follows. Section 2 presents the covered cybersecurity programs along with their targeted PDs and KUs requirements. Section 3 describes the details of all KUs. Furthermore, Appendix (A) presents examples of specialized cybersecurity programs, and Appendix (B) summarizes the update of this version.

# 2. Programs[3]

## 2.1 Intermediate Diploma[4]

| 2.1.1 Program Descriptors | | |
|---|---|---|
| Knowledge | Skills | Values |
| • General and interrelated knowledge and understanding of the foundations, theories, principles and technical concepts in the field of cybersecurity.<br>• Knowledge and understanding of the analytical methodologies used in cybersecurity topics and the interpretation of information related to them. | • Use a range of theoretical and technical knowledge in related sciences; and adapt them to reflect theoretical understanding in specific and unfamiliar contexts in cybersecurity.<br>• Apply critical thinking and creativity, for providing innovative practical solutions in moderately complex and unfamiliar contexts related to the field of cybersecurity.<br>• Use study and investigation methodologies to benefit from their results to solve problems of moderate complexity in cybersecurity.<br>• Select and use a variety of practices and technical tools; and adapt them to carry out practical moderately complex activities in the field of cybersecurity.<br>• Communicate in appropriate forms to demonstrate understanding and knowledge transfer to the beneficiaries in the field of cybersecurity.<br>• Manage specialized cybersecurity teams, take the initiative to build positive professional relationships, contribute to development of others, and work independently toward achieving shared objectives. | • Adhere to the professional ethics of cybersecurity, and the professional and humanitarian values and ethics associated with its practice.<br>• Demonstrate responsible citizenship by actively participating in national cybersecurity initiatives, even in moderately complex or unfamiliar contexts, while complying with national regulations, legislation, and cybersecurity controls under indirect supervision.<br>• Manage learning and work independently; set goals and work towards achieving them; and take decisions regarding learning with moderate degree of autonomy.<br>• Manage tasks and activities related to cybersecurity; and work under indirect supervision.<br>• Promote health, psycho-logical and social aspects related to the field of cybersecurity. |

[3] The following references were used to prepare the content of the requirements for the programs: [1], [2].

[4] This program corresponds to the Diploma program at the fifth level in the Unified Saudi Classification for Educational Levels and Specializations; and the National Qualifications Framework (NQF).

### 2.1.2 Admission Requirements

- High school diploma or equivalent.

### 2.1.3 Core Knowledge Units

**The students must complete the following:**

- **3 Cybersecurity Foundational KUs:**
  - Cybersecurity Fundamentals (CSF)
  - Cybersecurity Design Principles (CDP)
  - IT Systems Components (ISC)
- **5 Technical Core KUs:**
  - Basic Cryptography (BCY)
  - Basic Networking (BNW)
  - Basic Scripting and Programming (BSP)
  - Network Defense (NDF)
  - Operating Systems Concepts (OSC)

### 2.1.4 Elective Knowledge Units

- Elective KUs are all remaining KUs. Students must complete at least 5 elective KUs before graduation.

## 2.2 Bachelor (Cybersecurity Track)[5]

| 2.2.1 Program Descriptors | | |
|---|---|---|
| **Knowledge** | **Skills** | **Values** |
| • Knowledge of a broad and in-depth range of basic foundations, theories, principles and concepts in the field of cybersecurity.<br>• In-depth knowledge and understanding of the processes, tools, techniques, policies and practices used in cybersecurity.<br>• A broad range of specialized knowledge related to current and emerging developments and advanced topics in the field of cybersecurity. | • Apply integrated theories, principles, and concepts in various cybersecurity contexts.<br>• Analyze and evaluate various complex information in the field of cybersecurity.<br>• Critically evaluate, select and use cybersecurity techniques, methodologies and tools to solve problems, and perform cybersecurity work.<br>• Use study, investigation and research methodologies in cybersecurity projects and activities.<br>• Perform a wide range of tasks and procedures using cybersecurity tools in various complex operations.<br>• Communicate in appropriate forms to demonstrate knowledge, specialized skills and advanced concepts.<br>• Execute specialized collaborative projects in cybersecurity, embrace diverse perspectives, value diversity, analyze stakeholders' viewpoints, resolve conflicts with flexibility, and demonstrate leadership, entrepreneurship, and responsible task performance.<br>• Select AI tools and applications related to cybersecurity responsibly and adapt them, evaluate their results, document and improve them through the design of prompts and instructions, and comply with ethical AI-governance standards and advanced protection requirements | • Adhere to the professional ethics of cybersecurity, and the professional and humanitarian values and ethics associated with its practice.<br>• Demonstrate responsible citizenship and actively participate in national initiatives, particularly those related to cybersecurity, in diverse and unfamiliar contexts while complying with national regulations, including national cybersecurity legislation and controls.<br>• Take constructive decisions in situations that require self-reliance to work, learn and innovate with autonomy.<br>• Manage cybersecurity related tasks with autonomy.<br>• Participate actively in developing the field of cybersecurity and community service. |
| **2.2.2 Admission Requirements** | | |
| • High school diploma or equivalent. | | |

[5] This program corresponds to the Bachelor programs at the sixth level in the Unified Saudi Classification for Educational Levels and Specializations; and the National Qualifications Framework (NQF).

### 2.2.3 Core Knowledge Units

**The students must complete the following:**

- **3 Cybersecurity Foundational KUs:**
  - Cybersecurity Fundamentals (CSF)
  - Cybersecurity Design Principles (CDP)
  - IT Systems Components (ISC)
- **5 Program-Specific Core either:**
  - **Technical Core KUs**
    - Basic Cryptography (BCY)
    - Basic Networking (BNW)
    - Basic Scripting and Programming (BSP)
    - Network Defense (NDF)
    - Operating Systems Concepts (OSC)
  - **Non-Technical Core KUs**
    - Cyber Threats (CTH)
    - Policy, Legal, Ethics and Compliance (PLE)
    - Security Risk Analysis (SRA)
    - Cybersecurity Planning and Management (CPM)
    - Security Program Management (SPM)

### 2.2.4 Elective Knowledge Units

- Elective KUs are all remaining KUs. Students must complete at least 4 elective KUs before graduation.

## 2.3 Bachelor (Cybersecurity Major) [6]

| 2.3.1 Program Descriptors | | |
|---|---|---|
| Knowledge | Skills | Values |
| • Knowledge of a broad and in-depth range of basic foundations, theories, principles and concepts in the field of cybersecurity.<br>• In-depth knowledge and understanding of the processes, tools, techniques, policies and practices used in cybersecurity.<br>• A broad range of specialized knowledge related to current and emerging developments and advanced topics in the field of cybersecurity. | • Apply integrated theories, principles, and concepts in various cybersecurity contexts.<br>• Analyze and evaluate various complex information in the field of cybersecurity.<br>• Critically evaluate, select and use cybersecurity techniques, methodologies and tools to solve problems, and perform cybersecurity work.<br>• Use study, investigation and research methodologies in cybersecurity projects and activities.<br>• Perform a wide range of tasks and procedures using cybersecurity tools in various complex operations.<br>• Communicate in appropriate forms to demonstrate knowledge, specialized skills and advanced concepts.<br>• Execute specialized collaborative projects in cybersecurity, embrace diverse perspectives, value divesity, analyze stakeholders' viewpoints, resolve conflicts with flexibility and demonstrate leadership, entrepreneurship and responsible task performance.<br>• Select AI tools and applications related to cybersecurity responsibly and adapt them, evaluate their results, document and improve them through the design of prompts and instructions, and comply with ethical AI-governance standards and advanced protection requirements | • Adhere to the professional ethics of cybersecurity, and the professional and humanitarian values and ethics associated with its practice.<br>• Demonstrate responsible citizenship and actively participate in national initiatives, particularly those related to cybersecurity, in diverse and unfamiliar contexts while complying with national regulations, including national cybersecurity legislation and controls.<br>• Take constructive decisions in situations that require self-reliance to work, learn and innovate with autonomy.<br>• Manage cybersecurity related tasks with autonomy.<br>• Participate actively in developing the field of cybersecurity and community service. |
| **2.3.2 Admission Requirements** | | |
| • High school diploma or equivalent. | | |

[6] This program corresponds to the Bachelor programs at the sixth level in the Unified Saudi Classification for Educational Levels and Specializations; and the National Qualifications Framework (NQF).

### 2.3.3 Core Knowledge Units

**The students must complete the following:**

- **3 Cybersecurity Foundational KUs:**
  - Cybersecurity Fundamentals (CSF)
  - Cybersecurity Design Principles (CDP)
  - IT Systems Components (ISC)
- **7 Technical Core KUs:**
  - Basic Cryptography (BCY)
  - Basic Networking (BNW)
  - Basic Scripting and Programming (BSP)
  - Network Defense (NDF)
  - Operating Systems Concepts (OSC)
  - Data Structures (DST)
  - Databases (DAT)
- **5 Non-Technical Core KUs**
  - Cyber Threats (CTH)
  - Policy, Legal, Ethics and Compliance (PLE)
  - Security Risk Analysis (SRA)
  - Cybersecurity Planning and Management (CPM)
  - Security Program Management (SPM)

### 2.3.4 Elective Knowledge Units

• Elective KUs are all remaining KUs. Students must complete at least 10 elective KUs before graduation.

## 2.4 Higher Diploma for IT Background[7]

| 2.4.1 Program Descriptors | | |
|---|---|---|
| Knowledge | Skills | Values |
| • In-depth and specialized range of theoretical and technical knowledge and understanding of key issues in cybersecurity.<br>• Rigorous knowledge and understanding of processes, techniques, policies and practices used in cybersecurity.<br>• Deep understanding of new developments and advanced topics in cybersecurity. | • Select theoretical concepts, methodologies, techniques and tools for conducting cybersecurity work; assess and use them in complex and advanced contexts.<br>• Evaluate the main concepts, principles and theories in cybersecurity; critically review them; and express opinion on them.<br>• Provide and design innovative solutions in complex and advanced contexts for cybersecurity problems.<br>• Communicate in various forms to demonstrate specialized knowledge and skills with different categories of beneficiaries.<br>• Execute specialized collaborative projects in cybersecurity, embrace diverse perspectives, value diversity, analyze stakeholders' viewpoints, resolve conflicts with flexibility and demonstrate leadership, entrepreneurship and responsible task performance.<br>• Select AI tools and applications related to cybersecurity responsibly and adapt them, evaluate their results, document and improve them through the design of prompts and instructions, and comply with | • Adhere to the professional ethics of cybersecurity, and the professional and humanitarian values and ethics associated with its practice.<br>• Demonstrate responsible citizenship and actively participate in national initiatives, particularly those related to cybersecurity, in diverse and unfamiliar contexts while complying with national regulations, including national cybersecurity legislation and controls.<br>• Initiate professional planning for learning, work and professional development; and participate in making strategic professional decisions with high autonomy.<br>• Manage tasks effectively and with high autonomy in the field of cybersecurity.<br>• Participate effectively in developing the field of cybersecurity and community service. |

[7] This program corresponds to the Higher Diploma program at the sixth level in the Unified Saudi Classification for Educational Levels and Specializations.

| | | |
|---|---|---|
| | ethical AI-governance standards and advanced protection requirements | |

### 2.4.2 Admission Requirements

- Bachelor's degree in cybersecurity, computer science or related fields.
- English proficiency.

### 2.4.3 Core Knowledge Units

- If one or more of the required KUs of the Bachelor (Cybersecurity Track) program (which are listed in Section 2.2.3) are not completed by the student prior to admission, they must be completed in the program of study of this degree program.

### 2.4.4 Elective Knowledge Units

Elective KUs are all remaining KUs. Students must complete at least 8 elective KUs before graduation.

## 2.5 Higher Diploma for Non-IT Background[8]

| 2.5.1 Program Descriptors | | |
|---|---|---|
| Knowledge | Skills | Values |
| • A range of specialized theoretical knowledge and understanding of fundamental topics in cybersecurity.<br>• Rigorous knowledge and understanding of the regulatory and ethical aspects, processes, policies, practices, governance, risk management and monitoring compliance with controls and standards in the field of cybersecurity.<br>• Deep understanding of new developments in cybersecurity. | • Apply special principles, methodologies, concepts and tools in advanced cybersecurity contexts.<br>• Analyze, build and update policies, organizational and ethical aspects, compliance, risk management and governance in the field of cybersecurity.<br>• Evaluate and critically review the main concepts, principles and methodologies; express opinions on them; and provide creative solutions in complex and advanced contexts for problems in cybersecurity.<br>• Perform a range of tasks and procedures using tools for assessing cyber risks.<br>• Communicate in various forms to demonstrate specialized knowledge and skills with different categories of beneficiaries.<br>• Execute specialized collaborative projects in cybersecurity, embrace diverse perspectives, value diversity, analyze stakeholders' viewpoints, resolve conflicts with flexibility and demonstrate leadership, entrepreneurship and responsible task performance.<br>• Responsibly of using AI tools and applications related to cybersecurity responsibly and adapt them, evaluate their results, document and improve | • Adhere to the professional ethics of cybersecurity, and the professional and humanitarian values and ethics associated with its practice.<br>• Demonstrate responsible citizenship and actively participate in national initiatives, particularly those related to cybersecurity, in diverse and unfamiliar contexts while complying with national regulations, including national cybersecurity legislation and controls.<br>• Initiate professional planning for learning, work and professional development; and participate in making strategic professional decisions with high autonomy.<br>• Manage tasks effectively and with high autonomy in the field of cybersecurity.<br>• Participate effectively in developing the field of cybersecurity and community service. |

[8] This program corresponds to the Higher Diploma program at the sixth level in the Unified Saudi Classification for Educational Levels and Specializations.

| | | |
|---|---|---|
| | them through the design of prompts and instructions, and comply with ethical<br>AI-governance standards and advanced protection requirements | |

### 2.5.2 Admission Requirements

- Bachelor's degree.
- English proficiency.

### 2.5.3 Core Knowledge Units

**The students must complete the following:**

- **3 Cybersecurity Foundational KUs:**
  - Cybersecurity Fundamentals (CSF)
  - Cybersecurity Design Principles (CDP)
  - IT Systems Components (ISC)
- **3 Non-Technical Core KUs**
  - Cyber Threats (CTH)
  - Policy, Legal, Ethics and Compliance (PLE)
  - Security Risk Analysis (SRA)

### 2.5.4 Elective Knowledge Units

Elective KUs are all remaining KUs. Students must complete at least 2 elective KUs before graduation.

## 2.6 Master (Cybersecurity Track)[9]

| 2.6.1 Program Descriptors | | |
|---|---|---|
| Knowledge | Skills | Values |
| • Knowledge of a broad and in-depth range of theoretical and technical topics in the field of cybersecurity.<br>• Deep understanding of the processes and practices in cybersecurity.<br>• Deep understanding of modern and advanced developments and theories in cybersecurity.<br>• Knowing a set of specialized techniques for research and investigation in the field of cybersecurity | • Use a wide range of specialized tools, methods and practices based on knowledge of the latest developments in the field of cybersecurity.<br>• Plan and implement advanced cybersecurity research and innovative projects to develop cybersecurity products and services.<br>• Use advanced and specialized processes, techniques and tools to perform complex work in cybersecurity.<br>• Communicate in various forms to demonstrate specialized knowledge and skills with different categories of beneficiaries.<br>• Effectively employ AI tools to accomplish highly complex tasks and address intricate issues in cybersecurity, assess their effectiveness and outputs, improve and document them, using advanced prompting and command-engineering techniques, and adhere to ethical AI-governance standards and advanced protection requirements.<br>• Communicate in various forms to demonstrate specialized knowledge and | Adhere to the professional ethics and standards of cybersecurity, and demonstrate integrity along with professional and humanitarian values when handling the various issues and challenges in the cybersecurity field.<br>Demonstrate responsible citizenship and actively participate in national initiatives, particularly those related to cybersecurity, in diverse and unfamiliar contexts while complying with national regulations, including national cybersecurity legislation and controls.<br>Initiate professional planning for learning, work and professional development; and participate in making strategic professional decisions with high autonomy.<br>Effectively manage tasks and complete them with discipline and a high degree of autonomy in the field of cybersecurity.<br>Participate effectively in developing the field of cybersecurity and community service. |

[9] This program corresponds to the Master program at the seventh level in the Unified Saudi Classification for Educational Levels and Specializations; and the National Qualifications Framework (NQF).

| | | |
|---|---|---|
| | skills with different categories of beneficiaries.<br>• Implement advanced collaborative projects and initiatives in cybersecurity, interact with colleagues from multiple cultures, exchange ideas and resources to develop team performance, assume a leadership role, and take on multiple responsibilities. | |

### 2.6.2 Admission Requirements

- Bachelor's degree in cybersecurity, computer science or related fields.
- English proficiency.

### 2.6.3 Core Knowledge Units

- If one or more of the required KUs of the Bachelor (Cybersecurity Track) program (which are listed in Section 2.2.3) are not completed by the student prior to admission, they must be completed in the program of study of this degree program.
- Completion of a thesis or a project in a cybersecurity topic.

### 2.6.4 Elective Knowledge Units

Students must complete at least 4 elective KUs before graduation. Elective KUs for this program include all KUs except the required KUs of the Bachelor (Cybersecurity Track) program (listed in Section 2.2.3).

## 2.7 Master (Cybersecurity Major) [10]

| 2.7.1 Program Descriptors | | |
|---|---|---|
| Knowledge | Skills | Values |
| • Knowledge of a broad and in-depth range of theoretical and technical topics in the field of cybersecurity.<br>• Deep understanding of the processes and practices in cybersecurity.<br>• Deep understanding of modern and advanced developments and theories in cybersecurity.<br>• Knowing a set of specialized techniques for research and investigation in the field of cybersecurity. | • Use a wide range of specialized tools, methods and practices based on knowledge of the latest developments in the field of cybersecurity.<br>• Plan and implement advanced cybersecurity research and innovative projects to develop cybersecurity products and services.<br>• Apply specialized theories, principles and concepts, and use a broad set of methodologies, techniques and practices in complex, advanced cybersecurity contexts; evaluate them, conduct critical reviews, and deliver creative solutions to their issues and challenges.<br>• Use advanced and specialized processes, techniques and tools to perform complex work in cybersecurity.<br>• Effectively employ AI tools to accomplish highly complex tasks and address intricate issues in cybersecurity, assess their effectiveness and outputs, improve and document them, using advanced prompting and command-engineering techniques, and adhere to ethical AI-governance standards and advanced protection requirements.<br>• Communicate in various forms to demonstrate specialized knowledge and skills | • Adhere to the professional ethics and standards of cybersecurity, and demonstrate integrity along with professional and humanitarian values when handling the various issues and challenges in the cybersecurity field.<br>• Demonstrate responsible citizenship and actively participate in national initiatives, particularly those related to cybersecurity, in diverse and unfamiliar contexts while complying with national regulations, including national cybersecurity legislation and controls.<br>• Initiate professional planning for learning, work and professional development; and participate in making strategic professional decisions with high autonomy.<br>Effectively manage tasks and complete them with discipline and a high degree of autonomy in the field of cybersecurity<br>Participate effectively in developing the field of cybersecurity and community service. |

[10] This program corresponds to the Master program at the seventh level in the Unified Saudi Classification for Educational Levels and Specializations; and the National Qualifications Framework (NQF).

| | | |
|---|---|---|
| | with different categories of beneficiaries.<br>• Implement advanced collaborative projects and initiatives in cybersecurity, interact with colleagues from multiple cultures, exchange ideas and resources to develop team performance, assume a leadership role, and take on multiple responsibilities. | |

### 2.7.2 Admission Requirements

- Bachelor's degree in cybersecurity, computer science or related fields.
- English proficiency.

### 2.7.3 Core Knowledge Units

- If one or more of the required KUs of the Bachelor (Cybersecurity Track) program (which are listed in Section 2.2.3) are not completed by the student prior to admission, they must be completed in the program of study of this degree program.
- Completion of a thesis or a project in a cybersecurity topic.

### 2.7.4 Elective Knowledge Units

Students must complete at least 7 elective KUs before graduation. Elective KUs for this program include all KUs except the required KUs of the Bachelor (Cybersecurity Track) program (listed in Section 2.2.3).

## 2.8 Doctoral[11]

| 2.8.1 Program Descriptors | | |
|---|---|---|
| Knowledge | Skills | Values |
| • A substantial body of knowledge and thorough understanding of a broad range of topics in the field of cybersecurity, integrating advanced topics, specialized theories, pioneering principles and concepts necessary to create new and original knowledge, including the integration between disciplines.<br>• Detailed critical knowledge and understanding of cybersecurity processes, technologies, policies and practices for protecting data, systems and networks.<br>• Comprehensive knowledge and understanding of recent developments, emerging issues and challenges in cybersecurity.<br>• Advanced knowledge of methodologies for conducting original research and scientific activities that contribute to the development of the cybersecurity field. | • Evaluate, combine and critically review modern concepts, principles and theories; and develop innovative, creative and pioneering solutions to highly complex issues, problems, products and services of most advanced frontier in the field of cybersecurity.<br>• Apply leading theories, principles and concepts, and use a broad range of methodologies, techniques, policies and practices in highly complex cybersecurity contexts.<br>• Develop, adapt and implement highly advanced research and investigation methodologies to create original knowledge that contribute significantly to cybersecurity.<br>• Use highly advanced and new processes, technologies, tools and devices in the field of cybersecurity to carry out new, difficult and highly complex practical activities.<br>• Communicate in numerous forms to disseminate and promote original knowledge and new insights; and conduct scientific and professional dialogue with peers, specialized groups and the society at large. | • Demonstrate high level of academic integrity and values in the field of cybersecurity when dealing with emerging ethical and professional issues, research and knowledge; and promote them.<br>• Develop professional experience continuously; and take academic and professional strategic decisions with substantial autonomy.<br>• Foster professional relationships and community service in the field of cybersecurity. |

[11] This program corresponds to the Doctoral program at the eighth level in the Unified Saudi Classification for Educational Levels and Specializations; and the National Qualifications Framework (NQF).

| | | |
|---|---|---|
| | • Build multidisciplinary research and professional teams in the field of cybersecurity, engage at both institutional and community levels, take the initiative and lead them, and assume responsibility for their scientific activities with a high degree of autonomy<br>• Process and interpret quantitative and qualitative data; and use it in highly complex research, projects or innovations of most advanced frontier related to the field of cybersecurity. while complying with data-protection and privacy requirements in scientific research and professional practice<br>• Effectively employ AI tools to accomplish highly complex tasks and address intricate issues in cybersecurity, assess their effectiveness and outputs, improve and document them, using advanced prompting and command-engineering techniques, and adhere to ethical AI-governance standards and advanced protection requirements. | |

### 2.8.2 Admission Requirements

- Master's degree in cybersecurity, computer science or related fields[12].
- English proficiency.

[12] is permissible to admit candidates who hold a Bachelor's degree in cybersecurity, computer science, or any related field directly into Ph-D programs after the bachelor's degree, in accordance with the National Qualifications Framework.

### 2.8.3 Core Knowledge Units

- If one or more required KUs of the Bachelor (Cybersecurity Track) program (which are listed in Section 2.2.3) are not completed by the student prior to admission, they must be completed in the program of study of this degree program.
- Completion of a dissertation in a cybersecurity topic.

### 2.8.4 Elective Knowledge Units

Students must complete at least 3 elective KUs before graduation. Elective KUs for this program include all KUs except the required KUs of the Bachelor (Cybersecurity Track) program (listed in Section 2.2.3).

<table>
<tr><th></th><th>Intermediate Diploma</th><th>Bachelor (Cybersecurity Track)</th><th>Bachelor (Cybersecurity Major)</th><th>Higher Diploma for Non-IT Background</th><th>Higher Diploma for IT Background</th><th>Master (Cybersecurity Track)</th><th>Master (Cybersecurity Major)</th><th>Doctoral</th></tr>
<tr><td>Admission Requirements</td><td>High school diploma or equivalent</td><td>High school diploma or equivalent</td><td>High school diploma or equivalent</td><td>Bachelor's degree</td><td colspan="3">Bachelor's degree in cybersecurity, computer science or related fields</td><td>Master's degree in cybersecurity, computer science or related fields</td></tr>
<tr><td rowspan="2">Core Knowledge Units</td><td rowspan="2">CSF, CDP, ISC, BCY, BNW, BSP, NDF, OSC</td><td rowspan="2">CSF, CDP, ISC, and either:<br>• BCY, BNW, BSP, NDF, OSC<br>• CTH, PLE, SRA, CPM, SPM</td><td rowspan="2">CSF, CDP, ISC, BCY, BNW, BSP, NDF, OSC, DST, DAT, CTH, PLE, SRA, CPM, SPM</td><td rowspan="2">CSF, CDP, ISC, CTH, PLE, SRA</td><td colspan="4">Complete missing core KUs from Bachelor (Cybersecurity Track) if not completed before admission</td></tr>
<tr><td></td><td colspan="2">Completion of a thesis or project in a cybersecurity topic</td><td>Completion of a dissertation in a cybersecurity topic</td></tr>
<tr><td>Elective Knowledge Units</td><td>At least 5 elective KUs</td><td>At least 4 elective KUs</td><td>At least 10 elective KUs</td><td>At least 2 elective KUs</td><td>At least 8 elective KUs</td><td>At least 4 elective KUs</td><td>At least 7 elective KUs</td><td>At least 3 elective KUs</td></tr>
</table>

FIGURE 1: SUMMARY OF ADMISSION REQUIREMENTS, CORE KUS AND ELECTIVE KUS FOR ALL PROGRAMS.

# 3 Knowledge Units (KUs)

## Cybersecurity Fundamentals (CSF)

| | |
|---|---|
| Description | This KU provides general knowledge of basic concepts in cybersecurity. |
| Topics | The following topics must be included in this KU:<br>1. The Importance of Cybersecurity<br>2. Cybersecurity principles<br>3. Cyber Risks, Threats and Vulnerabilities<br>4. Confidentiality, Integrity, and Availability (CIA) Triad<br>5. Access Control, Authentication, Authorization and Non-Repudiation<br>6. Encryption and Its Uses<br>7. Governance and Cyber Risk Management<br>8. Protecting Data, Systems and Networks<br>9. Detecting and Responding to Cyber Incidents<br>10. Technologies and Solutions Used in Cybersecurity<br>11. Social Engineering and the Role of the Human Element in Cybersecurity |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Define the fundamental principles and goals of cybersecurity.<br>2. Identify common cyber risks, threats, and vulnerabilities.<br>3. Describe various types of cyber attacks, including social engineering attacks.<br>4. Explain the methodologies and techniques used to protect data, systems, and networks,<br>5. Recognize basic measures to be taken when a system compromise occurs.<br>6. Explain the role of governance and cyber risk management in supporting cybersecurity practices. |

## Cybersecurity Design Principles (CDP)

| | |
|---|---|
| Description | This KU includes the knowledge and skills of the fundamentals of secure-by-design for designing secure and reliable cyber systems. |
| Topics | The following topics must be included in this KU:<br>1. Principles of system and software design<br>2. Separation of domain and duties<br>3. Adequate Security<br>4. Isolation<br>5. Encapsulation<br>6. Modularity<br>7. Organizational and system resilience<br>8. Security by design<br>9. Accountability.<br>10. Simplicity of Design<br>11. Minimization of Implementation<br>12. Open Design<br>13. Complete Mediation<br>14. Layering and Defense-in-Depth<br>15. Least Privilege<br>16. Leverage Existing Components<br>17. Models of Systems Security Levels and Access Privileges<br>18. Fail Safe Defaults and Fail Secure<br>19. Least Astonishment<br>20. Minimize Trust Surface<br>21. Secure Design and Usability<br>22. Trust Relationships<br>23. Secure Coding Patterns<br>24. Ethics in Cybersecurity |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Express the secure-by-design principles.<br>2. Explain the importance of cybersecurity design principles and how each principle is useful to design trusted systems.<br>3. Distinguish the violated design principle for common system security weaknesses.<br>4. Analyze the required cybersecurity design principles needed for a given setup.<br>5. Apply cybersecurity design principles to complex programs and / or systems. |

## IT Systems Components (ISC)

| | |
|---|---|
| Description | This KU provides general introduction to common information technology systems components and general cybersecurity implications associated with them. |
| Topics | The following topics must be included in this KU:<br>1. Endpoint protection (e.g., Workstations, laptops, tablets, servers, appliances, mobile devices, peripheral devices (Printers, scanners, external storage), wearable devices)<br>2. Storage Devices (e.g., external storage drives, filesystems, shared file servers, databases)<br>3. System Architectures (e.g., enterprise, cloud, SaaS/PaaS/IaaS, etc.) and enabling technologies (e.g., containers, virtualization)<br>4. Managed services alternative environments (e.g., Supervisory Control and Data Acquisition (SCADA), real-time systems, critical infrastructures)<br>5. Configuration Management<br>6. Networks (Internet, LANs, wireless, WANs, CANs, Internet of Things, Automotive, and Smart cities)<br>7. Networking Equipment (e.g., routers, switches, firewalls, and network cables)<br>8. Network mapping (identification and enumeration of network components)<br>9. Network Security Components (Data Loss Prevention, VPNs, Firewalls, monitors, intrusion detection systems)<br>10. Intrusion Detection and Prevention Systems, Incident Response<br>11. Managed Services<br>12. IT Management and Monitoring (e.g., system monitoring tools, configuration management tools, and backup/recovery tools)<br>13. Software (e.g., operating systems, applications, and virtualization software)<br>14. Software Security (secure coding principles, software issues by type)<br>15. Configuration Management |

| | |
|---|---|
| | 16. System and application software updates patching (e.g., patch management)<br>17. Vulnerability Scanning (e.g., Vulnerability Windows, zero-day to patch availability)<br>18. Physical and environmental Security<br>19. Internet of Things (IoT)<br>20. IT organizational structure |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Identify common IT system components (both hardware and software) and illustrate their main functions.<br>2. Explain main cybersecurity implications of the current and future IT environments.<br>3. Express common cybersecurity systems, components, activities and their values to cybersecurity.<br>4. Understand system and software architectures.<br>5. Describe how software is managed within an organization. |

## Basic Cryptography (BCY)

| | |
|---|---|
| Description | This KU provides introduction to basic cryptographic algorithms and applications. |
| Topics | The following topics must be included in this KU:<br>1. Security Functions of Cryptography<br>2. History of cryptography and Classical ciphers<br>3. Symmetric Cryptography<br>4. Block vs. Stream Data<br>5. Block Cipher Modes of Operation<br>6. Public Key Cryptography<br>7. Key Generation, Management, Exchange and Distribution<br>8. Digital Certificates and PKI<br>9. Hash Functions<br>10. Cryptographic hash function properties<br>11. Digital Signatures<br>12. Common Cryptographic Protocols and Standards<br>13. Types of Cryptographic Attacks |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Describe the main security functions that cryptography can provide.<br>2. Explain the main components of any cryptographic system.<br>3. Differentiate between symmetric and asymmetric cryptography.<br>4. Demonstrate the use of Cryptographic Hash Functions to ensure data authenticity and verify message integrity<br>5. Illustrate the use of PKI to digitally sign and encrypt data. |

## Basic Networking (BNW)

| | |
|---|---|
| Description | This KU provides introduction to networks operations, components, layers, protocols, services, applications, tools and network security. |
| Topics | The following topics must be included in this KU:<br>1. Networking models: OSI, and TCP/IP<br>2. Network Media: Wired, Optical and Wireless<br>3. Network Topologies: bus, star, partial and full mesh<br>4. Network Architectures and Topologies: PAN, LAN, WAN, DMZ, VLAN, NAT, Subnetting, and supernetting<br>5. Network service model: peer-to-peer, and client-server<br>6. Common Network Devices: Routers, Switches, clients and servers, Wireless Access Points and Firewalls<br>7. Network and Transport Layers Protocols: IP, TCP, UDP, and ICMP<br>8. Network Services Protocols: DNS, NTP, DHCP, etc.<br>9. Network Applications Protocols: SMTP, HTTP, VoIP, SSH, etc.<br>10. Basic network administration tools: PING, and Traceroute<br>11. Overview of Network Security concepts: Zero Trust, and Defense-in-depth |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Explain foundational concepts of data networks including components, layers, protocols, services, applications and tools.<br>2. Design a basic network architecture given a setup scenario.<br>3. Identify packets trace for simple connections.<br>4. Apply network tools to recognize packet flows.<br>5. Illustrate common network threats and vulnerabilities. |

## Basic Scripting and Programming (BSP)

| | |
|---|---|
| Description | This KU focuses on enabling writing simple scripts/programs to automate and perform simple operations, and to provide the skills necessary to implement scripts and use programming languages to solve problems. This knowledge includes basic security practices in developing scripts/programs. |
| Topics | The following topics must be included in this KU:<br>1. Fundamental concepts and basic implementation of regular expressions<br>2. Fundamental data structures and algorithms<br>3. Boolean logic/operations<br>4. Scripting on Windows and Linux<br>5. Integrated Development Environment (IDE), Compilers/Interpreters<br>6. Basic programming constructs and concepts: Variables and Data Types, Strings, Arrays and Structures, Sequential and Parallel Execution, Statements and Expressions. Decisions and Branching, Loops in Programming and Their Types, Functions, Procedures and Calls, Debugging Techniques Console and file I/O, and Libraries<br>7. Basic Concepts of Secure Coding: Permissions, Bounds Checking, Input Validation, Type Checking, Parameter Validation and Error Handling |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Develop and execute programs in a high-level language using basic programming constructs and concepts<br>2. Write simple scripts to automate system administration tasks.<br>3. Develop and implement secure and reliable programs considering the characteristics of operating systems and environments.<br>4. Implement basic security practices in scripting, including bounds checking and input validation. |

## Network Defense (NDF)

| | |
|---|---|
| Description | This KU provides necessary concepts, skills, knowledge and tools to defend and protect a network against cyber threats. |
| Topics | The following topics must be included in this KU:<br>1. Concepts of network defense: Defense-in-Depth, Network attacks and exploitation, Network Hardening, Minimizing Exposure (e.g., Attack Surface and Vectors)<br>2. Network defense/monitoring tools: Firewalls, DMZs / Proxy Servers, VPNs, Decoys (e.g., Honeypots and Honeynets), Implementing IDS/IPS, Traffic signature analysis, Network anomaly detection<br>3. Network Operations: Network Security Monitoring (e.g., NOCs, SOCs), Network Traffic Analysis<br>4. Network security policies as they relate to network defense/security: Network Access Control (internal and external), Network Policy Development and Enforcement<br>5. Security Incident and Event Management (SIEM): Log analysis, Visualization of anomalies |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Illustrate main network defense concepts.<br>2. Demonstrate the use of network defense tools to defend against attacks and mitigate vulnerabilities.<br>3. Analyze the security policies implementations to protect a network.<br>4. Examine network operations relevant to network defense. |

## Operating Systems Concepts (OSC)

| | |
|---|---|
| Description | This KU provides a general introduction to the basic roles, functions and services of operating systems. |
| Topics | The following topics must be included in this KU:<br>1. Privileged and Non-Privileged States<br>2. Processes and Process Management<br>3. Threads and Concurrency<br>4. Scheduling<br>5. Memory Management<br>6. I/O Management<br>7. File systems<br>8. Virtualization and Hypervisors<br>9. Security Design in Operating Systems<br>10. Access controls (e.g., models and mechanisms)<br>11. Domain Separation, Process Isolation, Resource Encapsulation and Least Privilege<br>12. Event Management |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Illustrate the basic roles, functions and services of operating systems.<br>2. Demonstrate operating systems interactions with hardware components and other software applications.<br>3. Explain main cybersecurity issues related to operating systems.<br>4. Harden operating systems in a virtual environment. |

## Cyber Threats (CTH)

| | |
|---|---|
| Description | This KU includes knowledge and skills about cyber threats and attacks. |
| Topics | The following topics must be included in this KU:<br>1. Models and Types of Cyber Threats<br>2. Cyber Adversary Model: Resources, Capabilities, Intent, Motivation, Risk Aversion and Access<br>3. Attack Techniques: Backdoors, Trojans, Viruses, Ransomware, Wireless Attacks, Social Engineering and Covert Channels<br>4. Password Guessing and Cracking<br>5. Data Interception, Sniffing, spoofing, session hijacking, MiTM<br>6. Data Disclosure, Alteration and Sabotage Threats<br>7. Repudiation Threats<br>8. Denial of Service Attacks, Distributed Denial of Service Attacks, BOTs, and Botnets<br>9. Web Application Attacks, and Cloud Computing Attacks<br>10. Buffer Overflow<br>11. Persistence<br>12. Zero-Day Exploits<br>13. Indicators of compromise<br>14. Attack Indication Events and Attack Timing<br>15. Threat actors: Insider Threats, Script kiddies, Advanced Persistent Threats (APT)<br>16. Attack Surfaces, Attack Vectors and Attack Trees<br>17. Threat Information Sources<br>18. Cryptographic Threats<br>19. Social Engineering<br>20. Tactics, Techniques, and Procedures (TTPs) |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Categorize adversary resources, capabilities, techniques and motivations.<br>2. Describe different types of cyberattacks and their characteristics.<br>3. Distinguish and identify attack indication events.<br>4. Determine if a given attack is a threat to a given organization. |

## Cybersecurity Planning and Management (CPM)

| | |
|---|---|
| Description | This KU provides necessary skills and abilities to strategically develop, implement, effectively communicate, and oversee cybersecurity policies, procedures, processes and plans for an organization, while aligning cybersecurity initiatives with the organization's goals and regulatory requirements. |
| Topics | The following topics must be included in this KU:<br>1. Cybersecurity Common Body of Knowledge (CBK) with Relation to Planning and Management<br>2. Operational, Tactical and Strategic Planning and Management<br>3. Cybersecurity Related C-Level Functions<br>4. Cybersecurity in the core organizational strategy<br>5. Risk Assessment and Management<br>6. Cybersecurity Policies and Procedures<br>7. Cybersecurity Best Practices and Frameworks<br>8. Compliance and Regulatory Requirements<br>9. Overview of Security Architecture and Design<br>10. Vendor and Third-Party Risk Management<br>11. Overview of Threat Intelligence and Analysis |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Analyze system security functions and their strengths and weaknesses.<br>2. Identify and illustrate all roles, financial implication and responsibilities in cybersecurity planning and management.<br>3. Develop policies, processes, and procedures in relation to regulations, internationally recognized standards, and/or business requirements. |

## Policy, Legal, Ethics and Compliance (PLE)

| | |
|---|---|
| Description | This KU provides knowledge related to cybersecurity laws, standards, regulations, guidelines, policies and ethics. |
| Topics | The following topics must be included in this KU:<br>1. Best Practices of Work Ethics in the Field of Cybersecurity for Organizations and Individuals<br>2. Issues Related to the Ethics and Practices of Using Social Media Platforms<br>3. National and International Legislation to Combat Cybercrimes<br>4. Judicial Authorities, Agreements, Treaties and International Organizations Related to Cybersecurity<br>5. National and International Cybersecurity Standards and Controls (e.g. Essential Cybersecurity Controls (ECC) issued by the National Cybersecurity Authority, ISO 27001, PCI DSS)<br>6. Privacy and Data Protection Legislation and Regulations<br>7. Intellectual Property Protection Legislation and Regulations<br>8. Guidelines and Best Practices in Recent Trends (e.g. BYOD, Cybersecurity Guidelines for Internet of Things)<br>9. Best Practices for Aligning with Cybersecurity Legislation, Controls and Standards |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Discuss issues related to ethics and practices of using technology and cybersecurity.<br>2. Discussing legislation, regulations, guidelines and major policies in the field of cybersecurity.<br>3. Recognize important legislative and ethical issues when dealing with data.<br>4. Explain correct practices in alignment with cybersecurity legislation, controls and standards<br>5. Explain the challenges and dilemmas that cybersecurity professionals face in both legal and ethical situations |

## Security Program Management (SPM)

| | |
|---|---|
| Description | This KU provides necessary knowledge to implement, run and manage cybersecurity programs to protect and defend the organization in the cyberspace. |
| Topics | The following topics must be included in this KU:<br>1. Security Programs Goals and Objectives<br>2. Roles and Responsibilities<br>3. Cybersecurity Baselining<br>4. Program Monitoring and Control<br>5. Cybersecurity Awareness, Training and Education<br>6. Measuring Effectiveness<br>7. Cybersecurity Metrics and Reporting<br>8. Automation<br>9. Cybersecurity program address: Physical Security, Personnel Security, System and Data Identification, System Security Plans, Configuration and Patch management, System Documentation, Incident Response Program Management, Disaster Recovery Program Management, Certification and Accreditation, Business Continuity and Crisis Management<br>10. Security Education, Training, and Awareness (SETA)<br>11. Intellectual Property Protection Plan<br>12. Access Controls requirements and Implementation Management |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Design, prepare and manage a security program with goals, objectives and metrics for a given organization.<br>2. Measure the effectiveness of a cybersecurity program.<br>3. Design and prepare contingency plans including business continuity, disaster recovery and incident response.<br>4. Design patch and change management plan, intellectual property protection plan and access controls implementation plan. |

## Security Risk Analysis (SRA)

| | |
|---|---|
| Description | This KU includes the knowledge and skills of the models, methodologies and processes for assessing, managing and dealing with cyber risks. |
| Topics | The following topics must be included in this KU:<br>1. Principles and Concepts of Cybersecurity Risk Assessment, Analysis and Management<br>2. Risk Management Lifecycle and Steps<br>3. Cyber Risk Models<br>4. Methodologies for Measuring and Evaluating Cyber Risks<br>5. Cybersecurity Controls<br>6. Cyber Risks Mitigation Economics<br>7. Transference, Acceptance, Termination and Mitigation of Cyber Risks<br>8. Communication, documentation, and logging of Cyber Risks<br>9. Cyber Risk Management Standards and Frameworks |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Relate risk to a cybersecurity policy.<br>2. Demonstrate the main risk management methodologies.<br>3. Evaluate and categorize risk with respect to technology, individuals and entities.<br>4. Choosing the appropriate methodology for dealing with cyber risks taking into consideration the advantages and disadvantages.<br>5. Apply standards, frameworks, legal requirements, regulatory and institutional policy when conducting a risk assessment. |

## Advanced Algorithms (AAL)

| | |
|---|---|
| Description | This KU focuses on the ability to select and apply advanced algorithms to solve specific problems and to analyze the effectiveness of algorithms in context. |
| Topics | The following topics must be included in this KU:<br>1. Bloom filters<br>2. Naive Bayes<br>3. Map-Reduce<br>4. Linear Programming algorithms<br>5. Dynamic Programming algorithms<br>6. Markov Chain Monte Carlo<br>7. Coding and Compression<br>8. Graph algorithms<br>9. Stable Matching<br>10. NP-hardness<br>11. Approximation algorithms<br>12. Randomized algorithms<br>13. Artificial Intelligence Algorithms |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Design advanced algorithms to optimally and efficiently solve real problems.<br>2. Apply advanced algorithms to solve relevant problems in an effective and efficient way.<br>3. Analyze advanced algorithms and evaluate their complexity. |



Document Classification: Public

TLP: Clear

## Access Control (ACC)

| | |
|---|---|
| Description | This KU provides knowledge of data access control techniques. |
| Topics | The following topics must be included in this KU:<br>1. Physical Data Security: Data Center Security, Keyed Access, Key Cards, Video Surveillance, Rack-Level Security and Data Destruction.<br>2. Logical Data Access Control: Access Control Lists, Group Policies, Passwords, Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Rule-Based Access Control (RAC), History-Based Access Control (HBAC), Identity-Based Access Control (IBAC), Organization-Based Access Control (OrBAC), Federated Identities and Access Control<br>3. Secure Architecture Design: Principles of a Security Architecture and Protection of Information in Computer Systems<br>4. Data Leak Prevention Techniques: Controlling Authorized Boundaries, Channels, Destinations and Methods of Data Sharing |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Discuss the main physical security controls to ensure data integrity.<br>2. Explain logical access control concepts.<br>3. Differentiate among the different types of identities, such as federated identities<br>4. Investigate access control models, such as role-based, rule-based, and attribute-based. |



Document Classification: Public

TLP: Clear

## Advanced Cryptography (ACR)

| | |
|---|---|
| Description | This KU provides advanced knowledge of modern and emerging cryptographic algorithms, protocols, and secure implementation methodologies. |
| Topics | The following topics must be included in this KU:<br>1. Modern Symmetric Cryptography: Authenticated Encryption AEAD, Lightweight cryptography, Sponge and duplex constructions.<br>2. Post-Quantum Cryptography (PQC)<br>3. Evaluation methodologies for PQ modules.<br>4. Cryptanalysis of PQC.<br>5. Quantum attack models and Grover/Shor implications.<br>6. PQ transition and hybrid implementation.<br>7. Quantum Cryptography (QC)<br>8. Quantum Key Distribution<br>9. QKD protocols (e.g. BB84, E91, BBM92, B92, KMB09, AWEM-QKD)<br>10. Implementation limitation and Hybrid implementation.<br>11. Pairing-based cryptography.<br>12. Identity-based encryption (IBE), and attribute-based encryption (ABE)<br>13. Functional encryption<br>14. Forward security, key-evolving cryptography<br>15. Threshold cryptography and distributed key generation (DKG)<br>16. Zero-Knowledge Proofs cryptography.<br>17. Secure Multiparty computation (SMPC) cryptography.<br>18. Homomorphic Encryption (Partially and fully homomorphic schemes)<br>19. Secure messaging (e.g. Double Ratchet)<br>20. Anonymous credential systems and voting protocols.<br>21. Blockchain & Cryptographic Ledgers: Cryptographic accumulators, Merkle trees and vector commitments, Consensus cryptography, cryptography for decentralized networks.<br>22. Cryptographic attack models<br>23. Advanced side-channel analysis and countermeasures. |



Document Classification: Public

TLP: Clear

| | |
|---|---|
| | 24. Fault attacks and countermeasures.<br>25. Formal verification of cryptographic implementations.<br>26. Secure hardware implementations.<br>27. Key management in advanced systems.<br>28. Cryptographic Governance, Standards & Evaluation<br>29. FIPS 140-3 module requirements and testing for validation (ISO/IEC 19790, ISO/IEC 24759).<br>30. Common Criteria requirements (ISO/IEC 15408).<br>31. Cryptographic Module Validation Program (CMVP), Cryptographic Algorithm Validation Program (CAVP), Automated Cryptographic Validation Testing System (ACVTS), Automated Cryptographic Module Validation Project (ACMVP), Automated Cryptographic Validation Testing (ACVT) |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Analyze modern symmetric constructions<br>2. Evaluate and implement Post-Quantum Cryptography (PQC) and hybrid schemes to mitigate quantum attack models.<br>3. Design systems using Homomorphic Encryption and Secure Multi-Party Computation (SMPC) to process sensitive data without decryption.<br>4. Apply Zero-Knowledge Proofs and Threshold Cryptography to create anonymous credential systems and distributed trust environments.<br>5. Assess cryptographic mechanisms used in decentralized systems.<br>6. Evaluate cryptographic governance and validation frameworks, |



Document Classification: Public

TLP: Clear

## Algorithms (ALG)

| | |
|---|---|
| Description | This KU focuses on the ability to select and apply algorithms to solve specific problems and to analyze the effectiveness of algorithms in context. |
| Topics | The following topics must be included in this KU:<br>1. Algorithm Analysis<br>2. Computational Complexity<br>3. Best/Worst/Average Case Behavior<br>4. Optimization<br>5. Searching / Sorting<br>6. String matching algorithms<br>7. Iterative algorithms<br>8. Recursion<br>9. Greedy Algorithms<br>10. Hill Climbing |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Analyze algorithms and evaluate their effectiveness.<br>2. Design algorithms to solve problems in a correct and efficient way. |



Document Classification: Public

TLP: Clear

## Advanced Network Technology and Protocols (ANT)

| | |
|---|---|
| Description | This KU provides knowledge of advanced networking concepts and complex network security issues. |
| Topics | The following topics must be included in this KU:<br>1. Advanced Routing algorithms and protocols: BGP, OSPF, MPLS, Static and dynamic routing, Distance vector and link state.<br>2. Ethernet Switching: Spanning Tree Protocol, VLANs, Trunks, Link Aggregation, POE, port mirroring<br>3. Wireless (e.g., WLAN topology, antennas, frequencies, channels, standards, security issues)<br>4. Remote Access: VPN, site-to-site vs client-to-site, standards, protocols, RDP<br>5. Principles, protocols, and implications of software-defined networking<br>6. IPv6 Networking Suite including IPv6 security issues.<br>7. Quality of Service<br>8. Network Services<br>9. Social Network implementation and security issues.<br>10. Voice over IP (VoIP).<br>11. Multicasting.<br>12. Advanced Network Security Topics: Secure DNS, NAT, Deep Packet Inspection, and Transport Layer Security.<br>13. Troubleshooting |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Demonstrate the work of common advanced network protocols.<br>2. Analyze the security of advanced network protocols.<br>3. Operate network tools to examine an advance network protocol behavior. |



Document Classification: Public

TLP: Clear

## Analog Telecommunications (ATC)

| | |
|---|---|
| Description | This KU provides a general introduction to analog communications systems. |
| Topics | The following topics must be included in this KU:<br>1. Analog communication system components.<br>2. Signaling Methods<br>3. Architecture<br>4. Trunks, Switching<br>5. Grade of Service<br>6. Blocking<br>7. Call Arrival Models<br>8. Interference Issues |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Illustrate the main components and architecture of analog communications systems.<br>2. Differentiate between types of modulation in terms of their advantages and applications. |



Document Classification: Public

TLP: Clear

## Analytical Tools (ATT)

| | |
|---|---|
| Description | This KU provides knowledge, skills and ability to recognize, monitor, block, divert and respond to cyberattacks. |
| Topics | The following topics must be included in this KU:<br>1. Performance Measurements<br>2. Data Analytics<br>3. Cybersecurity Threat Intelligence |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Design, implement and manage the use of specific measurements to determine the effectiveness of the overall security program.<br>2. Use approaches and techniques to define and evaluate the utility of performance measurements.<br>3. Use techniques to manipulate large volumes of data to recognize, block, divert and respond to cyberattacks.<br>4. Collection, analysis and dissemination of cybersecurity threat intelligence information including threats and adversary capabilities. |



Document Classification: Public

TLP: Clear

## Awareness and Understanding (AUU)

| | |
|---|---|
| Description | This KU provides knowledge of risk, cyber hygiene, user education and vulnerabilities and threat awareness. |
| Topics | The following topics must be included in this KU:<br>1. Risk Perception and Communication<br>2. Cyber Hygiene<br>3. Cybersecurity User Education<br>4. Cyber Vulnerabilities and Threat Awareness |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Illustrate cyber hygiene, cybersecurity user education and cyber vulnerabilities and threat awareness.<br>2. Demonstrate Security Education, Training and Awareness (SETA) programs.<br>3. Explain risk perception and communication in cybersecurity. |



Document Classification: Public

TLP: Clear

## Business Continuity, Disaster Recovery and Incident Management (BDR)

| | |
|---|---|
| Description | This KU provides knowledge of business continuity, disaster recovery and incident management techniques that support organizational resilience. |
| Topics | The following topics must be included in this KU:<br>1. Introduction to BCDR: Definition and Importance, Key Concepts, Business Continuity vs. Disaster Recovery<br>2. Risk Assessment and Business Impact Analysis (BIA): Identifying Potential Risks, Assessing Impact on Business, Prioritizing Critical Business Functions<br>3. Business Continuity Planning (BCP): Developing a Business Continuity Plan, Strategies for Maintaining Operations, Communication Plans and Stakeholder Roles<br>4. Disaster Recovery Planning (DRP): Developing a Disaster Recovery Plan, IT Systems and Data Recovery, Recovery Time Objective (RTO) and Recovery Point Objective (RPO), Communication Plans and Stakeholder Roles<br>5. Implementation and Testing: Plan Implementation, Regular Testing and Drills |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Explain what resilience is and identify the environments in which resilience is important.<br>2. Discuss the basics of a disaster recovery plan and business continuity plan and the difference between them.<br>3. Analyze potential risks and vulnerabilities in an organization's current BC and DR plans, and suggest improvements to enhance its effectiveness.<br>4. Write case-based or actual plans for disaster recovery and business continuity.<br>5. Evaluate the effectiveness of a BC and DR plan through testing and simulation exercises, and recommend improvement. |



Document Classification: Public

TLP: Clear

## Cloud Computing (CCO)

| | |
|---|---|
| Description | This KU provides a general introduction to cloud computing technologies, services, models and security. |
| Topics | The following topics must be included in this KU:<br>1. Virtualization Platforms<br>2. Cloud Services: SaaS, PaaS, DaaS, IaaS, FaaS.<br>3. Scalability<br>4. Hypervisors and Cloud Computing Implementations<br>5. Service Oriented Architectures<br>6. Service Level Agreements (SLAs)<br>7. Deployment Models: Private, Public, Community and Hybrid<br>8. Cloud Security<br>9. Common cloud security tools and services<br>10. Best practices in cloud computing cybersecurity<br>11. Storage<br>12. Identity and Access Management (IAM) in cloud systems<br>13. Resilience and Disaster recovery<br>14. Forensics/IR Implications of cloud use<br>15. Legal, Regulatory, and Compliance Issues |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Explain cloud computing services.<br>2. Discuss the advantages and disadvantages of virtualization.<br>3. Deploy a cloud-based application.<br>4. Efficiently allocate resources to users and applications.<br>5. Discuss the importance of resource management in cloud computing.<br>6. Explain the requirements for a secure cloud environment. |



Document Classification: Public

TLP: Clear

## Cryptography (CRY)

| | |
|---|---|
| Description | This KU provides the knowledge and skills related to standard cryptographic algorithms and protocols. It focuses on the functional design, security properties, and analysis of symmetric and asymmetric encryption, hash functions, and digital signatures, serving as the core technical foundation for securing information and communications. |
| Topics | The following topics must be included in this KU:<br>1. Stream ciphers: design principles, Table based such as RC4, LFSR such as Salsa, ChaCha Trivium, Grain, ZUC and Snow<br>2. Block ciphers: Feistel cipher, AES, Camellia and Serpent, Algorithm structure<br>3. Standards and new modes of operation<br>4. Message Authentication Codes (HMAC, CMAC and KMAC)<br>5. Authenticated encryption (GCM and CCM)<br>6. Symmetric cryptanalysis: Known attacks of block and stream ciphers<br>7. RSA: encryption, DSA, security assumptions<br>8. Diffie - Hellman key exchange<br>9. ElGamal Encryption and DSA<br>10. Elliptic Curve Cryptography (ECDH, ECDSA)<br>11. Signature schemes<br>12. Introduction to Quantum cryptography (PQC, QKD and QRNG)<br>13. Asymmetric cryptanalysis<br>14. Hash Functions: SHA-2, SHA-3 (Keccak)<br>15. Hash-based message authentication<br>16. Merkle trees and commitment schemes<br>17. Hash functions cryptanalysis<br>18. Certificates and certificate authorities: root, intermediate, subordinate and user certificates<br>19. X.509 certificate structure<br>20. Certificate validation, revocation protocols<br>21. Certificateless Public Key Cryptography<br>22. Trust models: hierarchical, web-of-trust |



Document Classification: Public

TLP: Clear

| | |
|---|---|
| | 23. Hardware security modules (HSM), Trusted Platform Modules (TPM) and smart cards<br>24. Key Generation: Random number generator (PRNG, TRNG and QRNG), Hybrid random number generator, Statistical tests for RNG<br>25. Key Wrap Functions<br>26. Key Derivation Functions<br>27. Side-channel attacks: timing, power analysis, fault injection<br>28. Real-world vulnerabilities and implementation issues: e.g. padding Oracle |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Analyze the operations of block and stream ciphers to determine the most secure implementation for a given scenario.<br>2. Apply public-key cryptographic techniques to achieve secure key exchange and digital signatures.<br>3. Evaluate the security properties of cryptographic hash functions to ensure data authenticity and verify message integrity<br>4. Design and assess secure key generation and key management processes.<br>5. Apply cryptoanalysis techniques to break encrypted data. |



Document Classification: Public

TLP: Clear

## Cryptography Engineering (CRE)

| | |
|---|---|
| Description | This KU provides an introduction to cryptographic engineering principles and practices, focusing on the secure design, implementation, evaluation, and governance of cryptographic systems. |
| Topics | The following topics must be included in this KU:<br>1. Cryptographic Engineering Principals: Secure cryptographic implementation and security by design, Secure key storage and authentication, Secure booting, Side-channel resistant design<br>2. Cryptographic Governance, Standards and Policy Aspects: NCA's publication (NCS, ECC, CSCC, DCC and CCC), NIST SP 800-series, Compliance with national cryptographic regulations, Key escrow requirements, Cryptography and digital rights, Ethical use of encryption tools<br>3. Cryptographic Protocols: Secure key exchange and Authentication protocols, Secure messaging, voting protocols and secure multiparty mechanisms, Zero-knowledge protocols<br>4. Applied Cryptography: Disk encryption, Network encryption, Secure email, End-to-end encryption, Password security and authentication systems<br>5. Cryptographic Engineering & Implementation Security: Fault attacks and countermeasures, Formal verification of cryptographic implementations, Secure hardware, Constant-time programming and leakage-resilient coding, Key management in advanced systems, Hardware cryptographic implementation (FPGA, ARM, RISC-V and ASIC)<br>6. Cryptography assessment, evaluation, and implementation validation: KAT, Invasive and Non-Invasive evaluation, Red-Black architecture validation, Emanation assessment |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Design and integrate cryptographic modules into systems.<br>2. Align cryptographic implementations with national and international standards and policies. |



Document Classification: Public

TLP: Clear

| | |
|---|---|
| | 3. Analyze the security and efficiency of a given cryptographic protocol.<br>4. Apply cryptography protocol to secure software and hardware systems. |

## Cyber Crime (CCR)

| | |
|---|---|
| Description | This KU provides general information about cybercrimes and abuses in the cyberspace. |
| Topics | The following topics must be included in this KU:<br>1. Cyber Crime Types: Social Engineering, Hacking, Intrusions, Malware, Espionage, Intellectual Property Theft, Fraud, Extortion, Services Disruption, Data Leakage, Data Destruction, Data Falsification.<br>2. Cyber Stalking and Predators<br>3. Cyber Bullying<br>4. Identity Theft<br>5. Cyber Assisted Crimes<br>6. Cyber Terrorism<br>7. Cyber Crime Laws: National Laws, International Laws, Treaties.<br>8. Ethical codes and societal norms: Rights of others, Respect and principles of community, Resource use, allocation, and abuse, Cybersecurity and social responsibility.<br>9. Common tactics used in cyber crime<br>10. Impact of cyber crime (e.g., financial loss, reputation damage, legal consequences, operational disruption) |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Explain potential cybercrimes, cyber-stalking, cyberbullying and other abusive behaviors in the internet.<br>2. Demonstrate the use of cybersecurity applications for defense against crime and abuse.<br>3. Examine case studies of Internet cybercrime methods and potential protections. |



Document Classification: Public

TLP: Clear

## Cybersecurity Ethics (CSE)

| | |
|---|---|
| Description | This KU provides knowledge of ethical issues in cybersecurity. |
| Topics | The following topics must be included in this KU:<br>1. Maintaining Privacy and Confidentiality of Information in Cybersecurity<br>2. Protecting User Rights in Cybersecurity<br>3. Ethical Codes and Frameworks related to Cybersecurity Ethics<br>4. Ethical Aspects in Protecting Sensitive Systems and Networks That Has High Impact on Society and Individuals<br>5. The Balance between Protecting and Enabling Systems and Networks<br>6. National and Social Responsibility in Cybersecurity<br>7. Ethical Foundations in Cybersecurity<br>8. Common Ethical Dilemmas in Cybersecurity<br>9. Ethical Decision-Making Tools<br>10. Role of Cybersecurity in Promoting Ethics<br>11. Impact of Cybersecurity Practices on Society |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Explain basic topics in cybersecurity ethics.<br>2. Practicing cybersecurity work while adhering to the ethical aspects related to it. |



Document Classification: Public

TLP: Clear

## Cyber-Physical System (CPS)

| | |
|---|---|
| Description | This KU provides knowledge of fundamental concepts, principles, and practices in designing, developing, and deploying CPS. |
| Topics | The following topics must be included in this KU:<br>1. Architecture and Design: system design, modeling, and simulation<br>2. Cybersecurity of CPSs including threats, vulnerabilities, risk assessment, and mitigation strategies<br>3. Real-time Systems: scheduling, synchronization, and timing analysis<br>4. Networked Systems: communication protocols, network architecture, and distributed systems<br>5. Embedded Systems: microcontrollers, embedded software, and hardware and software integration<br>6. Sensor and Actuator Systems: sensor fusion, actuator control, and feedback mechanisms<br>7. Control Systems: control theory, stability analysis, and optimization techniques<br>8. Human-Machine Interface: user interface design, human factors, and usability<br>9. Safety and Reliability: hazard analysis, fault tolerance, and system reliability<br>10. Standards and Regulations: industry standards, regulatory requirements, and compliance<br>11. Physical Security Information Management (PSIM) Systems<br>12. Security of Unmanned Aerial Vehicle (UAV)/drones including security of drone platforms, communications, evidence artifacts, and supply chain in the design and construction |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Describe the integration of computational and physical processes, including the role of sensors, actuators, and control systems in CPS.<br>2. Implement strategies for ensuring the safety, security, and reliability of CPS, particularly in critical applications such as healthcare, transportation, and industrial automation. |



Document Classification: Public

TLP: Clear

| | |
|---|---|
| | 3. Analyze and evaluate CPS applications in various industries, such as smart grids, autonomous vehicles, and smart cities. |

## Databases (DAT)

| | |
|---|---|
| Description | This KU provides knowledge, skills and abilities to manage, use and protect database systems. |
| Topics | The following topics must be included in this KU:<br>1. Database Management Systems (DBMS) Types: Relational, Hierarchical, NoSQL Databases, Object-Based, Object Oriented and Distributed.<br>2. Database Security Models: Inference, Aggregation, Injection, Hashing, Encryption, Data Corruption, Unauthorized Access, Database Access Controls (DAC, MAC, RBAC, Clark-Wilson) |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Differentiate between different types of database management systems (DBMS) in terms of its structure and applications.<br>2. Illustrate security aspects related to databases and DBMS. |



Document Classification: Public

TLP: Clear

## Data Administration (DBA)

| | |
|---|---|
| Description | This KU provides students with knowledge about data life cycle, data quality and data security. |
| Topics | The following topics must be included in this KU:<br>1. Data Lifecycle: Capture, Maintenance, Transformation, Usage, Distribution, Archival and Purging<br>2. Data Quality: Accuracy, Completeness, Relevance, Consistency, Integrity, Cleansing, Verification and Validation<br>3. Data Accessibility<br>4. Data Utility<br>5. Data Storage and Archiving: Data Warehousing, Long Term Archival and Big Data<br>6. Hadoop, MongoDB and HBASE<br>7. Data Control: Ownership, Stewardship, Management, Possession, Governance<br>8. Data Policies: Internal and External<br>9. Data Security: Access Control, Data Classification and Encryption |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Explain data lifecycle stages and discuss related security issues.<br>2. Analyze data quality, accessibility and utility.<br>3. Manage the creation, change, distribution, storage and termination of data in a secure way.<br>4. Discuss and explain data ownership, stewardship, management, possession and governance.<br>5. Illustrate the importance of data classification in cybersecurity. |



Document Classification: Public

TLP: Clear

## Digital Communications (DCO)

| | |
|---|---|
| Description | This KU provides knowledge of digital communications systems and related protocols. |
| Topics | The following topics must be included in this KU:<br>1. Digital Communications System Components<br>2. Coding Schemes<br>3. Digital Signaling and modulation<br>4. Spread Spectrum Signals<br>5. Multi-User Communication Access (e.g. CDMA, TDMA, FDMA, SDMA, PDMA) |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Describe digital communications systems in terms of subsystems and modulation techniques<br>2. Explain the principles and advantages of spread spectrum signals regarding interference/jamming resistance.<br>3. Differentiate between multi-user communication access methods. |

## Digital Forensics (DFS)

| | |
|---|---|
| Description | This KU provides knowledge of forensics techniques and skills to apply them for investigation activities in a way that complies with the legal requirements. |
| Topics | The following topics must be included in this KU:<br>1. Digital Forensics Terminologies<br>2. Legal Compliance: Applicable Laws, Affidavits, Testimony, Testifying, Case Law and Chain of Custody<br>3. Digital Investigation: E-Discovery, Authentication of evidence, Chain of Custody Procedures, and Root Cause Analysis<br>4. Acquisition and Preservation of Evidence: Write-blocking, Imaging Procedures, Live Forensics, Analysis and Authentication of Evidence (Hashing)<br>5. Analysis of Evidence: Root Cause Analysis, Metadata and File Carving<br>6. Usage of Tools and Techniques for forensics investigation<br>7. Reporting and Presentation of Results: Timeline and Attribution |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Conduct a digital forensics investigation across the full digital investigation lifecycle.<br>2. Illustrate legal and regulation issues related to digital forensics in the Kingdom. |



Document Classification: Public

TLP: Clear

## Data Integrity and Authentication (DIA)

| | |
|---|---|
| Description | This KU provides knowledge of data integrity and authentication techniques. |
| Topics | The following topics must be included in this KU:<br>1. Authentication Strength: Multi-Factor Authentication, Cryptographic Tokens, Cryptographic Devices, Biometric Authentication, One-Time Passwords and Knowledge Based Authentication<br>2. Password Attack Techniques: Dictionary Attack, Brute Force Attack, Rainbow Table Attack, Phishing, Social Engineering, Malware-Based Attack, Spidering, Off-line Analysis and Password Cracking Tools<br>3. Password Storage Techniques: Cryptographic Hash Functions, Collision Resistance, Salting, Iteration Count and Password-Based Key Derivation<br>4. Data integrity: Message Authentication Codes (HMAC, CBC-MAC), Digital Signatures, Authenticated Encryption and Hash Trees |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Explain the main concepts in authentication, authorization, access control and data integrity.<br>2. Illustrate strengths and weaknesses of authentication techniques.<br>3. Demonstrate common attacks on passwords. |



Document Classification: Public

TLP: Clear

## Deep Learning (DLL)

| | |
|---|---|
| Description | This KU provides knowledge and skills for the development and application of modern neural networks. |
| Topics | The following topics must be included in this KU:<br>1. Neural Networks: Binary Classification, Logistic Regression, Logistic Regression Cost Function, Gradient Descent, Derivatives, Computation Graph, Vectorization<br>2. Shallow Neural Networks: Neural Network Representation, Activation Functions, non-linear Activation Functions, Derivatives of Activation Functions, Gradient descent, Forward Propagation, Backward Propagation and Computational Graphs<br>3. Convolutional Neural Networks: Classic Networks, Recurrent Neural Networks and Loss Functions and Optimization<br>4. Unsupervised Deep Learning<br>5. Deep Reinforcement Learning<br>6. Adversarial training and generative adversarial networks |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Explain the key fundamentals of deep learning and deep network architectures.<br>2. Use deep learning networks to solve problems related to cybersecurity.<br>3. Enhance the security of deep learning models using adversarial training. |

## Database Management Systems (DMS)

| | |
|---|---|
| Description | This KU provides students with knowledge about main concepts of database management systems in addition to skills and abilities to utilize database management systems. |
| Topics | The following topics must be included in this KU:<br>1. Database Types: Flat, Relational, Network, Hierarchical, Object-Oriented, Object-based, Key-Value and Distributed<br>2. SQL Data Manipulation Language: SELECT, INSERT, DELETE and UPDATE<br>3. SQL Data Definition Language<br>4. SQL Database Administration: User Creation and Deletion, Permissions and Access Controls<br>5. Database concepts: Indexing, Inference, Aggregation and Polyinstantiation<br>6. Database Security and Protection |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Explain the main database concepts.<br>2. Differentiate between the roles of a database, a DBMS and a database server within a complex system supporting multiple applications.<br>3. Apply SQL to create, administer and operate databases.<br>4. Manage DBMS access controls, privilege levels.<br>5. Sketch structures for storing data in DBMS.<br>6. Design and implement a database for a given application. |



Document Classification: Public

TLP: Clear

## Distributed Systems Architecture (DSA)

| | |
|---|---|
| Description | This KU provides knowledge of distributed systems and how they are connected. |
| Topics | The following topics must be included in this KU:<br>1. Distributed Systems General Concepts<br>2. Examples of Distributed Systems<br>3. Protocols and Layering<br>4. High Performance Computing<br>5. Hypervisors and Cloud Computing Implementation<br>6. Vulnerabilities and Exploit Examples |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Describe the components and interfaces of a networking standard provided.<br>2. Explain a process in an operating system and introduce various architectures for running processes and enabling their communication.<br>3. Describe HPC and use cases that distinguish HPC from the standard Internet.<br>4. Examine the attack surfaces of the various distributed computing models emphasizing the fact that every interface introduces potential vulnerabilities. |



Document Classification: Public

TLP: Clear

## Data Structures (DST)

| | |
|---|---|
| Description | This KU focuses on understanding the basic abstract data types, associated operations and applying them to solve problems. |
| Topics | The following topics must be included in this KU:<br>1. Numerical<br>2. Strings<br>3. Arrays and Vectors<br>4. Lists: Linked List, Double Linked List<br>5. Heaps<br>6. Queues and Stacks<br>7. Objects, Maps, Hash maps, Hash tables and dictionaries<br>8. Sets<br>9. Buffers<br>10. Trees<br>11. Graphs<br>12. Language-specific native data structures |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Implement common abstract data types.<br>2. Use given abstract data types and their operations to implement solutions to given problems.<br>3. Differentiate between different data structures and their uses, benefits and drawbacks.<br>4. Design specifications of a required data structure based on given needs.<br>5. Illustrate the abstraction concept and recognize abstract violations for given data structure specifications. |



Document Classification: Public

TLP: Clear

## Device Forensics (DVF)

| | |
|---|---|
| Description | This KU provides skills and abilities to apply forensics techniques to investigate devices. |
| Topics | The following topics must be included in this KU:<br>1. Device acquisition and evidence extraction: Mobile devices, Embedded Systems (GPS, Games Consoles and Smart TVs), and Internet of Things Devices<br>2. Device analysis<br>3. Legal considerations of device forensics<br>4. Devices forensics tools |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Illustrate methods of acquiring and extracting data from embedded systems, mobile and IoT devices.<br>2. Perform analysis on embedded systems, mobile and IoT devices.<br>3. Discuss legal aspects linked to forensic analysis on embedded systems, mobile and IoT devices. |

## Embedded Systems (ESY)

| | |
|---|---|
| Description | This KU provides knowledge about embedded systems, and related security issues, as well as the skills and abilities needed to design and implement components of embedded systems. |
| Topics | The following topics must be included in this KU:<br>1. Introduction to Embedded Systems: Definition and Characteristics, Examples and Applications, Differences between Embedded Systems and General-Purpose Computers<br>2. Embedded System Components (e.g., Hardware and Software)<br>3. Embedded System Design and Development<br>4. Microcontroller/embedded processor architectures<br>5. PLC's, Gate Arrays, and other common programmable logic devices<br>6. I/O, A/D, registers, sensors, actuators, and embedded hardware components<br>7. Memory (e.g., RAM, ROM, Flash)<br>8. Embedded devices communications<br>9. Interrupt handling and timing issues<br>10. Resource management in real time systems<br>11. Operating Systems for Embedded Systems: Devices without operating systems, Real-Time Operating Systems (RTOS)<br>12. Security in Embedded Systems: Security issues imposed by limited resources<br>13. Programming languages and environments for embedded systems: Tool chains, Target operating systems and devices, Cross compilers |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Describe the fundamental components and architecture of embedded systems, including microcontrollers, sensors, and actuators.<br>2. Explain the constraints and challenges associated with developing applications for embedded devices.<br>3. Design, develop and prototype embedded system solutions that address specific real world problems, integrating hardware and software components effectively. |



Document Classification: Public

TLP: Clear

## Forensic Accounting (FAC)

| | |
|---|---|
| Description | This KU provides knowledge about forensic techniques for financial investigations, in addition to the skills and abilities to apply them. |
| Topics | The following topics must be included in this KU:<br>1. Investigative Accounting<br>2. Fraudulent Financial Reporting<br>3. Misappropriation of Assets<br>4. Indirect Methods of Reconstructing Income<br>5. Money Laundering<br>6. Transnational Financial Flows<br>7. Litigation Services<br>8. Evidence Management<br>9. Economic Damages and Business Valuations |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Describe common financial statement fraud and their detection techniques.<br>2. Estimate concealed revenue and income.<br>3. Illustrate money laundering methods and their detection and prevention techniques.<br>4. Evaluate fraud and theft loss and damages. |



Document Classification: Public

TLP: Clear

## Formal Methods (FMD)

| | |
|---|---|
| Description | This KU provides knowledge about the mathematical logic and skills needed to apply it in the design of secure systems. |
| Topics | The following topics must be included in this KU:<br>1. Concept of Formal Methods<br>2. Mathematical Logic<br>3. Formal Method application in System Design and Software Engineering<br>4. Limitations of Formal Methods<br>5. Bell-LaPadula<br>6. Automated Reasoning Tools<br>7. System Modeling and Specification<br>8. Proofs<br>9. Model Checkers and Model Finders<br>10. Comparison to other tools and techniques for defect detection (e.g. Testing, Fuzzing)<br>11. Formal approaches to software modeling and analysis: Model checkers, Model finders |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Apply formal methods to real situations.<br>2. Describe the use of mathematical logic in the design of securing systems.<br>3. Illustrate the value of formal methods and analysis techniques over testing as software validation and verification techniques.<br>4. Apply formal methods to software designs.<br>5. Explain formal specification languages advantages and disadvantages. |

## Mathematical Foundations of Cryptography (FCY)

| | |
|---|---|
| Description | This KU provides the theoretical and mathematical foundations of modern cryptography. |
| Topics | The following topics must be included in this KU:<br>1. Number Theory<br>2. Finite Fields<br>3. Discrete Logarithms<br>4. Factoring<br>5. Probabilities<br>6. Information theory<br>7. Truly entropy source generator.<br>8. Random number generator (PRNG, TRNG and QRNG)<br>9. Hybrid random number generator<br>10. Advanced Random Number Generation<br>11. Elliptic Curves<br>12. Lattices in cryptography<br>13. Perfect security and computational complexity<br>14. Adversarial models and threat assumptions<br>15. Kerckhoffs' principle of Cryptography and Claude Shannon information theory<br>16. Complexity-theoretic security definitions<br>17. Simulation-based security (IND-CPA, IND-CCA1, IND-CCA2 …)<br>18. Universal composability framework<br>19. Hardness assumptions (LWE, RSA, CDH, DDH…) |



Document Classification: Public

TLP: Clear

| Learning Outcomes | By completing this KU, students should be able to:<br>1. Explain fundamental mathematical hardness assumptions underlying modern cryptography<br>2. Differentiate between perfect security and computational security.<br>3. Illustrate the mathematical requirements for cryptographic-strength random number generation.<br>4. Differentiate between cryptographic hardness assumptions, including number-theoretic, group-theoretic, and lattice-based assumptions. |
|---|---|

## Fraud Prevention and Management (FPM)

| | |
|---|---|
| Description | This KU provides knowledge and abilities to design plans and processes to prevent and mitigate fraud. |
| Topics | The following topics must be included in this KU:<br>1. Fraud Introduction and Terminologies<br>2. Fraud Prevention and Auditing: Scientific Method and Benford's Law<br>3. Dealing with Data: Collecting, Cleaning, Verifying and Normalizing<br>4. Understanding Data: Analysis, Visualization, Sorting, Indexing, Summarizing and Stratifying<br>5. Numeric Tests for Fraud: Frequently Used Values, Even Amounts, Rounding, Ratio/Variance Analysis, Testing for Outliers, Statistical Tests and Randomization Testing<br>6. Modeling Fraud: Machine Learning Techniques for Fraud Detection<br>7. Advanced Fraud Detection and Prevention |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Evaluate cost and effectiveness of fraud detection and prevention methods.<br>2. Explain legal and ethical issues related to fraud detection and prevention.<br>3. Apply fraud tools and techniques for detection and prevention. |



Document Classification: Public

TLP: Clear

## Hardware Architecture (HAA)

| | |
|---|---|
| Description | This KU provides introduction to the advantages of hardware architectures standards and potential vulnerabilities. |
| Topics | The following topics must be included in this KU:<br>1. Standard Architectures<br>2. Hardware Interface Standards (e.g. ISA, PCI)<br>3. Common Architectures (e.g. CPU chips, PC motherboard, Ethernet standards) |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Understand the idea of standard architectures and the advantages of standardization.<br>2. Describe various hardware interface standards for network connectors. |

## Hardware/Firmware Security (HFS)

| | |
|---|---|
| Description | This KU provides knowledge of hardware/firmware components and the related security issues. |
| Topics | The following topics must be included in this KU:<br>1. Physical Vulnerabilities: Unused/Unsecured Communications Channels, Test Pads, Test Paths, Back Doors, Trojans, Hidden Circuits, Doping, Induced Faults, Reverse Engineering, Unauthorized Memory Access<br>2. Hardware Side Channel Attacks: Timing, Power Analysis, Electromagnetic, RF analysis, Hardware Insertion and Out-of-Band Channels<br>3. Sourcing Attacks: Pirated, Fake, Counterfeit Parts and Supply Chain Disruption<br>4. Equipment Destruction Attacks<br>5. Hardware Security Components: Verifiable Device IDs, Random Number Generators, Boot ROM Digital Signatures, Hardware-Base Encryption Modules, Security Controllers/Co-Processors and Encryption Accelerators, Trusted Platform Module (TPM), UEFI Secure Boot<br>6. Physical Security Attributes: Device Validation, Open/ Accepted Security Algorithms, Strong Random Number Generation, Secure Time Source, Standardized Developer Interface, Clear Documentation, Key Backup/Protection, Tamper-Resistance and Scalability<br>7. Bootloader Vulnerabilities: Boot Sector Attacks, Single User Mode, Boot to Non-Secure OS's and Boot Loader Reconfiguration, UEFI Secure Boot bypasses<br>8. Microcode Vulnerabilities<br>9. Firmware Vulnerabilities: Reflashing BIOS/PROMs<br>10. Security Role of Intermediate Layers: Hardware Abstraction Layer and Virtualization Layers |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Illustrate main hardware and firmware vulnerabilities.<br>2. Utilize hardware security capabilities.<br>3. Explain systems initialization and software loading and validation.<br>4. Discuss the security role of hardware abstraction layers. |



Document Classification: Public

TLP: Clear

## Host Forensics (HOF)

| | |
|---|---|
| Description | This KU provides skills and ability to investigate a network host using forensics techniques. |
| Topics | The following topics must be included in this KU:<br>1. File Systems and File System Forensics<br>2. Hypervisor Analysis<br>3. Cryptanalysis<br>4. Rainbow Tables<br>5. Known File Filters (KFF)<br>6. Steganography<br>7. File Carving<br>8. Live System Investigations<br>9. Timeline Analysis<br>10. Host application forensic analysis |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Identify retrievable data from multiple operating system environments.<br>2. Demonstrate host forensics methodologies.<br>3. Perform live system investigation and forensic report |

## Hardware Reverse Engineering (HRE)

| | |
|---|---|
| Description | This KU provides knowledge, abilities and skills to determine the functionality, input, output and stored data of given hardware components using reverse engineering procedures and techniques. |
| Topics | The following topics must be included in this KU:<br>1. Reverse Engineering Principles<br>2. Stimulus, Data Collection and Data Analysis<br>3. Specification Development<br>4. Capability Enhancement and Modification Techniques<br>5. Detecting Modification<br>6. Stimulation Methods and Instrumentation<br>7. JTAG IEEE 1149.1 Standards<br>8. Defining and Enumerating Interfaces<br>9. Functional Decomposition |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Demonstrate hardware reverse engineering techniques.<br>2. Apply probing, measuring and data collection to identify the functionality of a given hardware component.<br>3. Describe a technique for reverse engineering the functionality of an integrated circuit. |

## Information Assurance Architectures (IAA)

| | |
|---|---|
| Description | This KU provides knowledge of cybersecurity architectures used for protecting information systems and data. |
| Topics | The following topics must be included in this KU:<br>1. Defense in Depth<br>2. DMZs<br>3. Proxy Servers<br>4. Composition and Security<br>5. Cascading<br>6. Emergent Properties<br>7. Dependencies<br>8. Trusted Computing Base Subsets<br>9. Enterprise Architectures and Security Architectures<br>10. Secure Network Design |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Differentiate and relate between Information Assurance (IA) architecture stages and components.<br>2. Demonstrate knowledge of the capabilities and limitations of current methods for evaluating, planning, implementing and maintaining IA Architectures solutions.<br>3. Examine potential vulnerabilities for a given architecture.<br>4. Design secure architectures for given applications. |



Document Classification: Public

TLP: Clear

## Information Assurance Compliance (IAC)

| | |
|---|---|
| Description | This KU provides knowledge of rules, regulations and issues related to the audit and compliance with applicable laws and regulations related to cybersecurity. |
| Topics | The following topics must be included in this KU:<br>1. Relationship Between Compliance and Audit<br>2. Audit Types: Internal and External<br>3. Audit Purposes: Requirements, Specifications, Policy, Standards, Laws, Regulatory and Internal Controls<br>4. Audit Process: Charter, Baseline, Activities, Reporting, Results, Recommendations, Response and Mitigation Strategy<br>5. Compliance Monitoring<br>6. Compliance Training |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Differentiate between mandatory and optional compliance requirements.<br>2. Design, plan and perform audits to examine compliance. |

## Information Assurance Standards (IAS)

| | |
|---|---|
| Description | This KU provides knowledge of the common information national and international information assurance standards. |
| Topics | The following topics must be included in this KU:<br>1. National standards related to cybersecurity<br>2. International regulations and standards related to cybersecurity (e.g. NIST)<br>3. Commercial Standards (e.g. PCI/DSS)<br>4. Open Standards (e.g. OWASP) |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Compare different types of national and international laws, regulations, policies, frameworks and standards.<br>2. Explain the impact of standards or regulation on given systems.<br>3. Illustrate standards implications on sub-contractors and customers.<br>4. List and explain main standards provisions. |



Document Classification: Public

TLP: Clear

## Industrial Control Systems (ICS)

| | |
|---|---|
| Description | This KU provides knowledge of industrial control systems and their potential vulnerabilities. |
| Topics | The following topics must be included in this KU:<br>1. Industrial operations ecosystem: Industry sectors, Professional roles and responsibilities, Process types, Industrial lifecycles, Workplace safety<br>2. Instrumentation and control systems: Supervisory Control and Data Acquisition (SCADA) Systems, Types of ICSs (e.g., power distribution systems, manufacturing), Models of ICS systems (e.g., time-driven vs. event-driven), Sensors and actuators, Controllers (Programmable Logic Controllers (PLC), Remote Terminal Units (RTUs), Distributed Control Systems (DCS)), Controller programming (ladder diagram, function block, structured text, sequential function chart), Human-Machine Interfaces (HMIs) in ICS and SCADA systems<br>3. Process equipment: Hardware components of ICS and SCADA systems<br>4. Industrial control networking and communications: ICS and SCADA systems protocols and networking (e.g., Ethernet/IP, MODBUS, PROFINET, DNP3, OPC, ICCP, HART), Other ICS communications technologies (e.g. serial, RS232/485, ZIGBEE, 900MHz, Bluetooth, X.25)<br>5. Process safety and reliability: causes of safety risk, hazards assessment, impact analysis<br>6. Industrial cybersecurity guidance and regulations: Regulatory, compliance, and industry standards and guidelines requirements for ICS and SCADA systems, ICS Network Security Architectures<br>7. Common weaknesses affecting ICS environments: ICS and SCADA security challenges, Common vulnerabilities in critical infrastructure, ICS, and SCADA systems, Threats and attack vectors affecting ICS environments<br>8. ICS events and incidents response/recovery |

| | |
|---|---|
| | 9. ICS cybersecurity defensive techniques: network segmentation, anomaly detection, device hardening, engineered controls |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Describe the components of a SCADA industrial control system.<br>2. Describe the use and application of Programmable Logic Controllers (PLCs) in automation.<br>3. Describe approaches to address common weaknesses while considering unique ICS characteristics and requirements.<br>4. Apply knowledge of ICS and SCADA systems to identify potential vulnerabilities and threats.<br>5. Explain how ICS environments differ from traditional information system environments.<br>6. Explain how cybersecurity models are being used to guide ICS and SCADA systems security. |



Document Classification: Public

TLP: Clear

## Independent/Directed Study/Research (IDR)

| | |
|---|---|
| Description | This KU provides knowledge of emerging issues related to cybersecurity. |
| Topics | The following topics must be included in this KU:<br>1. Emerging Technologies with Relevant Security Issues<br>2. Emerging Tools, Techniques and Methods Related to Cybersecurity |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Discuss advanced and emerging technologies related to cybersecurity.<br>2. Apply, demonstrate and discuss the use of emerging and advanced cybersecurity tools, methods and techniques. |

## Intrusion Detection/Prevention Systems (IDS)

| | |
|---|---|
| Description | This KU provides knowledge about methods and techniques to detect and analyze vulnerabilities and threats, as well as the skills to utilize them to mitigated associated risks. |
| Topics | The following topics must be included in this KU:<br>1. Deep Packet Inspection<br>2. Log File Analysis<br>3. Telemetry data<br>4. Log Aggregation<br>5. Cross Log Comparison and Analysis<br>6. Anomaly Detection: Establishing Profiles<br>7. Anomaly Algorithms: Statistical Techniques, Correlation Techniques, Fuzzy Logic Approaches, Artificial Intelligence, Filtering Algorithms and Neural Networks<br>8. Misuse Detection: Signature Detection<br>9. Specification-Based Detection<br>10. Host-Based Intrusion Detection and Prevention: Behavioral Detection (file and process)<br>11. Network-Based Intrusion Detection and Prevention: Stealth mode<br>12. Distributed Intrusion Detection<br>13. Hierarchical IDS's<br>14. Honeynets/Honeypots<br>15. Intrusion Response: Device Reconfiguration, Notifications, Trace Recording, Opening Application, Session Interruption and Reach Back |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Detect and respond to host and network intrusions.<br>2. Apply tools to analyze logs and detect various anomalous activity on a network.<br>3. Design corrective procedures to respond to discovered intrusions.<br>4. Configure IDS/IPS to optimize their performance and accuracy. |

## Identity Management (IMM)

| | |
|---|---|
| Description | This KU provides knowledge of identity management techniques. |
| Topics | The following topics must be included in this KU:<br>1. Identification and Authentication: People and Devices, Network Access Control (NAC), Identity Access Management (IAM), Roles, Multi-Method Identification and Authentication Systems, Biometric Authentication Systems, Accuracy/FAR/FRR, Resistance, Privacy, Usability and Tolerability of the Methods<br>2. Physical and Logical Assets Control: System Hardware, Network Assets, Backup/Storage Devices, Rules-Based Access Control (RAC), Role based Access Control (RBAC), Inventory Tracking Methods, Identity Creation Methods<br>3. Identity as a Service (IaaS)<br>4. Third-Party Identity Services<br>5. Access Control Attacks and Mitigation Measures: Password, Dictionary, Brute Force, Spoofing Attacks, Multi-Factor Authentication, Strong Password Policy, Secure Password Files and Restrict Access to Systems |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Differentiate between identification, authentication and access authorization.<br>2. Discuss the audit trails and logging importance in identification and authentication.<br>3. Apply least privilege and segregation of duties concepts.<br>4. Explain access control attacks and discuss mitigation measures. |

## Internet of Things (IoT)

| | |
|---|---|
| Description | This KU provides knowledge of IoT and their potential vulnerabilities. |
| Topics | The following topics must be included in this KU:<br>1. IoT Architecture (e.g., system design, modeling, and simulation)<br>2. IoT Applications<br>3. IoT Communication Protocols<br>4. IoT operating Systems<br>5. IoT threats and attacks<br>6. Secure Software Lifecycle for IoT<br>7. Security Evaluation Standard for IoT Platforms<br>8. Radio-Frequency Identification (RFID) tags<br>9. The Manufacturer Usage Description (MUD) specification<br>10. Secure Upgrade Process |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Describe the IoT Architecture and applications.<br>2. Describe best cybersecurity measures to secure IoT devices<br>3. Identify the security evaluation standard for IoT platforms. |

## Information Storage Security (ISS)

| | |
|---|---|
| Description | This KU provides knowledge of information storage security techniques. |
| Topics | The following topics must be included in this KU:<br>1. Disk and File Encryption: Hardware vs. Software Encryption<br>2. Data Erasure: Overwriting, Degaussing, Physical Destruction Methods and Memory Remanence<br>3. Data Masking: for Testing, for Obfuscation and for Privacy<br>4. Database Security: Access, Authentication, Auditing and Application Integration Paradigms |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Discuss storage device encryption implemented at the hardware and software levels.<br>2. Contrast techniques for data erasure and their limitations in implementation.<br>3. Explain data masking applications.<br>4. Discuss database access, authentication, auditing and application integration. |

## Introduction to the Theory of Computation (ITC)

| | |
|---|---|
| Description | This KU provides knowledge of finite automata and their role and use in computation. It also provides the skills and abilities to analyze the complexity of computation problems. |
| Topics | The following topics must be included in this KU:<br>1. Automata<br>2. Turing Machines<br>3. Deterministic and Non-Deterministic Finite Automata<br>4. Formal Language Theory<br>5. Computability and Non-Computability<br>6. Turing Computability<br>7. Analysis of Algorithms<br>8. Complexity Measures: Time, Storage, Communications and Numbers of Processors<br>9. Big O Notation<br>10. Best, Worst and Average Complexity<br>11. Upper and Lower Bounds on Complexity<br>12. Classes of Complexity: P, NP and Intractability |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Explain abstract machines theory and automata.<br>2. Differentiate between computable and incomputable functions.<br>3. Explain complexity and quantify resources requirements for problems computation.<br>4. Analyze given problems using deterministic and non-deterministic finite automata. |



Document Classification: Public

TLP: Clear

## Life-Cycle Security (LCS)

| | |
|---|---|
| Description | This KU provides knowledge of security principles and skills to apply them to improve security throughout the system or product lifecycle. |
| Topics | The following topics must be included in this KU:<br>1. System Life-Cycle Phases and Issues: Initiation, Requirements, Design, Development, Testing, Deployment, Operations, Maintenance and Disposal<br>2. Vulnerability Mapping, Management and Tractability<br>3. Threat Modeling<br>4. Software Assurance Maturity Model<br>5. Role of Project/Program Management<br>6. Role of Process Management<br>7. Importance of Culture and Training<br>8. Development Processes and Paradigms<br>9. Configuration Management<br>10. Developmental Threats |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Describe the importance of secure software, programming best-practices, and the development processes and methodologies that lead to secure software.<br>2. Explain system life-cycle stages along with their security related issues.<br>3. Identify maturity model elements. |

## Low Level Programming (LLP)

| | |
|---|---|
| Description | This KU provides skills to securely perform low level operations using low level programing languages. |
| Topics | The following topics must be included in this KU:<br>1. Higher level languages which allow low level access, such as C<br>2. Programing in Assembly<br>3. Library Functions Security<br>4. Pointers and Pointer Manipulation<br>5. Modularization in Low Level Programs<br>6. Defensive Programming Techniques<br>7. Compile, Assemble and Link Object Files<br>8. Calls in Assembly |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Apply low level programming to implement OS components and hardware drivers.<br>2. Discuss the benefits and the risks of using low level programming. |

## Media Forensics (MEF)

| | |
|---|---|
| Description | This KU provides skills and ability to investigate media using forensics techniques. |
| Topics | The following topics must be included in this KU:<br>1. Drive Acquisition<br>2. Evidence Authentication: Verification, Validation and Hashing<br>3. Metadata: Modification, Access or Change (MAC) Timestamps<br>4. Live vs. Static Acquisition<br>5. Sparse vs. Full Imaging<br>6. Slack Space<br>7. Hidden Files, Clusters and Partitions |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Demonstrate forensic analysis techniques and acquisition methods on given media.<br>2. Apply forensic investigation techniques on specified media. |

## Machine Learning (MLL)

| | |
|---|---|
| Description | This KU provides knowledge of machine learning algorithms and mathematical and statistical models. It also provides the skills to use these algorithms and models in machine learning applications. |
| Topics | The following topics must be included in this KU:<br>1. Linear Regression<br>2. Linear Classification<br>3. Logistic Regression<br>4. K-Nearest Neighbors<br>5. Evaluation Metrics: AUC, Precision, Recall, Specificity, MSE, MAPE and RMSE<br>6. Hypothesis Testing<br>7. Gradient Descent<br>8. Decision Trees<br>9. Random Forest<br>10. Support Vector Machines<br>11. Probabilistic Classifiers<br>12. Artificial Neural Networks<br>13. Clustering<br>14. Singular Value Decomposition (SVD), Principal Component Analysis (PCA) and Autoencoders<br>15. Reinforcement Learning<br>16. Ethics for Machine Learning<br>17. Application of machine learning algorithms related to cybersecurity |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Apply machine learning algorithms and models to classification, regression and clustering problems.<br>2. Evaluate and interpret the results of the algorithms.<br>3. Analyze and handle large data sets.<br>4. Compare and contrast several learning techniques.<br>5. Given a cybersecurity application of machine learning, describe ethical issues regarding the choices of data, preprocessing steps, algorithm selection, and visualization/presentation of results. |



Document Classification: Public

TLP: Clear

## Mobile Technologies (MOT)

| | |
|---|---|
| Description | This KU provides knowledge of mobile technologies including their hardware, communications, management and programing environments. |
| Topics | The following topics must be included in this KU:<br>1. Cellular Networks (e.g. 4G/LTE, 5G, and 6G): Standards Heritage and Core Architecture Evolution<br>2. Design Choices<br>3. Encryption<br>4. Mobility Management<br>5. Radio Resource Control (RRC) Signaling<br>6. Billing/Charging<br>7. Mobile Security |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Demonstrate how mobile systems function to secure voice and data access.<br>2. Explain how network connectivity is maintained during motion.<br>3. Compare among different cellular network standards in terms of architecture and security. |



Document Classification: Public

TLP: Clear

## Network Security Administration (NSA)

| | |
|---|---|
| Description | This KU provides knowledge related to the administration and maintenance of enterprise security infrastructures. |
| Topics | The following topics must be included in this KU:<br>1. Mapping Business Objectives to Technology Objectives<br>2. Main Security Solutions and Product Categories and Features<br>3. Information Security Conflicts with Potential Solutions<br>4. Cybersecurity Best Practices<br>5. Applying Network Security Policies<br>6. Risk Posture and Risk Appetite<br>7. Network and Systems Monitoring Tools<br>8. Issue Evaluation, Response and Management<br>9. Incident Identification<br>10. Incident Response Processes and Management<br>11. Deployment and Upgrade Processes<br>12. User Acceptance Testing<br>13. Blackout Plans<br>14. Maintenance Windows and Management |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Analyze network requirements and recommend solutions, products and technologies.<br>2. Identify best security practices to satisfy business objectives according to risk assumptions.<br>3. Protect IT assets and infrastructure from potential threats.<br>4. Perform systems monitoring for anomalies and periodically perform system updating and patching.<br>5. Practice incident response activities to breaches, intrusions and theft.<br>6. Plan, test, implement and evaluate software and hardware deployment. |



Document Classification: Public

TLP: Clear

## Network Technology and Protocols (NTP)

| | |
|---|---|
| Description | This KU provides knowledge of network protocols and components. It also provides skills to use tools to monitor and analyze a network. |
| Topics | The following topics must be included in this KU:<br>1. Network Switching: Ethernet, ARP, and RARP<br>2. Network layer 2 Security Issues<br>3. IPv4 Suite: IPv4 Addressing<br>4. IPv6 Suite: IPv6 Addressing<br>5. Routing in IPv4 and IPv6: Routing Algorithms, Routing Tables and Metrics<br>6. Network Layer 3 Security Issues<br>7. Network Naming: DNS and NetBIOS<br>8. Network Analysis and Troubleshooting: Netflow<br>9. Protocol and packet analysis tools: Wireshark |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Explain layer 2 networking.<br>2. Illustrate IPv4 and IPv6 structure.<br>3. Detect and mitigate layer 2 and layer 3 security issues.<br>4. Apply networks and packet analysis tools for troubleshooting. |



Document Classification: Public

TLP: Clear

## Network Forensics (NWF)

| | |
|---|---|
| Description | This KU provides skills and ability to investigate and analyze network traffic using forensic techniques. |
| Topics | The following topics must be included in this KU:<br>1. Packet Capture and Analysis<br>2. Network security incident investigation<br>3. Intrusion Detection and Prevention<br>4. Interlacing of Device and Network Forensics<br>5. Log File Analysis<br>6. Yara and Sigma Detection rules<br>7. MITRE ATT&CK/ATLAS frameworks<br>8. Cyber Threat Intelligence |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Demonstrate network forensic methodologies.<br>2. Analyze network traffic.<br>3. Detect malicious and anomalous activities and their effects. |



Document Classification: Public

TLP: Clear

## Operating Systems Administration (OSA)

| | |
|---|---|
| Description | This KU provides knowledge and skills to perform basic operations in operating systems administration. |
| Topics | The following topics must be included in this KU:<br>1. OS Installation<br>2. User Accounts Management: Access Control, Password Policies, Authentications Methods and Group Policies<br>3. Command Line Interfaces<br>4. Configuration Management<br>5. Updates and Patches<br>6. Event Logging and Auditing<br>7. Managing System Services<br>8. Virtualization<br>9. Backup and Restoring Data<br>10. File System Security<br>11. Network Configuration<br>12. Host Intrusion Detection<br>13. Security Policy Development<br>14. Host firewall and endpoint protection configuration |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Setup user accounts, develop authentication policies and implement them.<br>2. Design and implement audit configurations.<br>3. Perform backup and restore operations.<br>4. Review security and system logs.<br>5. Install patches and updates.<br>6. Configure basic security settings on the operating system. |



Document Classification: Public

TLP: Clear

## Operating Systems Hardening (OSH)

| | |
|---|---|
| **Description** | This KU provides knowledge, skills and abilities to improve the security and robustness of operating systems. |
| **Topics** | The following topics must be included in this KU:<br>1. Secure Installation<br>2. Removing Unnecessary Components<br>3. File System Maintenance: Isolation of Sensitive Data<br>4. User Restrictions: Access and Authorizations<br>5. User, Group and File Management<br>6. Password Standards and Requirements<br>7. Shutting Down Unnecessary and Unneeded Services<br>8. Closing Unnecessary and Unneeded Ports<br>9. Patch Management and Software Updates<br>10. Virtualization<br>11. Vulnerability Scanning<br>12. Host Firewall Configuration<br>13. Secure Boot<br>14. Drive Encryption |
| **Learning Outcomes** | By completing this KU, students should be able to:<br>1. Demonstrate hardening steps for a given OS to reduce the attack surface area.<br>2. Perform secure OS installation and disable unneeded components, services and ports.<br>3. Perform OS patching and updating periodically.<br>4. Leverage built-in OS capabilities and/or third-party applications to increase defensive posture. |

## Operating Systems Theory (OST)

| | |
|---|---|
| Description | This KU provides knowledge of operating system concepts, components and interfaces. |
| Topics | The following topics must be included in this KU:<br>1. Privilege States<br>2. Processes, Threads and Process/Thread Management<br>3. Memory Management and Virtual Memory<br>4. Inter-Process Communications<br>5. Concurrency, Synchronization and Deadlocks<br>6. File Systems<br>7. Input and Output<br>8. Real-time Operating Systems and Security Issues<br>9. Distributed OS Architectures and Security Issues<br>10. Race Conditions<br>11. Buffer Overflows<br>12. Virtualization<br>13. Clear Interface Semantics<br>14. Zero-trust architecture<br>15. Micro segmentation and isolated environments |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Illustrate and demonstrate operating systems theory and implementation.<br>2. Design and implement OS architectural changes. |



Document Classification: Public

TLP: Clear

## Penetration Testing (PTT)

| | |
|---|---|
| Description | This KU provides knowledge of methods to exploit vulnerabilities to gain control or access to systems and networks. It also provides skills and ability to utilize and apply these methods. |
| Topics | The following topics must be included in this KU:<br>1. Flaw Hypothesis Methodology<br>2. Other Methodologies (e.g., OSSTMM)<br>3. Identifying Flaws from Documentation<br>4. Identifying Flaws from Source Code Analysis<br>5. Vulnerability Scanning<br>6. Families of Attacks<br>7. Flaws that Lead to Vulnerabilities<br>8. Enumeration and Footprinting<br>9. Attack Surface Discovery<br>10. Attack Vectors<br>11. Attack Frameworks (e.g., MITRE ATT&CK/ATLAS)<br>12. Exploitation and post-exploitation techniques<br>13. Ethical usage of penetration testing<br>14. Professional penetration testing reports<br>15. Penetration Testing Tools and Scripts (e.g., Metasploit, Kali Linux, etc.)<br>16. Open Source Intelligence (OSINT)<br>17. Passive/Active Reconnaissance |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Plan and perform penetration testing on a system or a network.<br>2. Discuss and compare families of attacks.<br>3. Analyze security vulnerabilities of systems and networks.<br>4. Discuss post-exploitation techniques.<br>5. Identify attack surfaces for penetration testing<br>6. Create a professional penetration testing report with results and findings.<br>7. Assess ethical and legal requirements of security assessment and penetration testing. |



Document Classification: Public

TLP: Clear

## QA/Functional Testing (QAT)

| | |
|---|---|
| Description | This KU provides knowledge of methods used to assess the extent to which a requirement is met by a functional unit. |
| Topics | The following topics must be included in this KU:<br>1. Testing Methodologies: White, Grey and Black Box Testing<br>2. Testing Types and Levels: unit testing, integration testing, system testing, acceptance testing, performance testing, and security testing<br>3. Test Coverage Analysis<br>4. Automatic and Manual Generation of Test Inputs<br>5. Test Execution<br>6. Validation of Results<br>7. Documentation of test results |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Design and develop effective, structured and organized tests.<br>2. Perform cybersecurity functional testing to demonstrate that security policies and mechanisms are completely and correctly implemented. |

## Radio Frequency Principles (RFP)

| | |
|---|---|
| Description | This KU provides knowledge about radio frequency communications. |
| Topics | The following topics must be included in this KU:<br>1. Basics of Electromagnetic Radiation<br>2. Antennas<br>3. Information Modulation<br>4. Digital Modulation<br>5. Spectral Representation<br>6. Bandwidth<br>7. BER<br>8. Eb/No vs. S/N<br>9. Limiting Access in RF<br>10. Propagation Principles |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Explain isolating RF emissions methods.<br>2. Identify techniques for obfuscating RF transmissions.<br>3. Demonstrate the tradeoffs related to bandwidth data rate, modulation, complexity, acceptable BER and signal spreading. |



Document Classification: Public

TLP: Clear

## Software Assurance (SAS)

| | |
|---|---|
| Description | This KU provides knowledge of methods and techniques that lead to secure software. |
| Topics | The following topics must be included in this KU:<br>1. Security Principles: Segregation, Isolation, Encapsulation, Least Privilege, Simplicity, Minimization, Fail Safe Defaults, Fail Secure, Modularity, Layering, Least Astonishment, Open Design, Usability and Reduce Attack Surfaces<br>2. Security of Alternative Designs<br>3. Secure Design Patterns<br>4. Security requirements for system data<br>5. Audit Trail<br>6. Security Modeling Techniques and Vulnerability Mapping<br>7. Resiliency<br>8. Design Reviews |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Apply secure-by-design principles.<br>2. Illustrate the effects of system design and architecture on security.<br>3. Create a system design optimized to meet appropriate security requirements.<br>4. Construct a secure design using modeling and vulnerability assessment.<br>5. Discuss how Design Reviews can significantly help improving security. |



Document Classification: Public

TLP: Clear

## System Control (SCC)

| | |
|---|---|
| Description | This KU provides knowledge of system control techniques including detecting, compensating for, defending against and preventing attacks. |
| Topics | The following topics must be included in this KU:<br>1. Resources access control<br>2. Authorization Models<br>3. Intrusion Detection: Anomaly, Misuse [Rule-Based, Signature-Based] and Specification-Based Techniques<br>4. Attack models: Attack Trees and Graphs<br>5. Defenses: ASLR, IP Hopping and Intrusion Tolerance<br>6. Audit: Logging, Log Analysis and Relationship to Intrusion Detection<br>7. Malware: Viruses, Worms and Ransomware<br>8. Vulnerabilities Models: RISOS and PA, CVE and CWE<br>9. Penetration Testing: Flaw Hypothesis Methodology, ISSAF, OSSTMM, GISTA, PTES<br>10. System Requirements for Forensics<br>11. Recovery and Resilience |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Contrast various system-related methods for authentication, authorization, and access control.<br>2. Describe how malicious activity can be detected, including the use of intrusion detection systems.<br>3. Differentiate among types of malware.<br>4. Discuss recovery and resilience mechanisms that help ensure system availability. |



Document Classification: Public

TLP: Clear

## Secure Communication Protocols (SCP)

| | |
|---|---|
| Description | This KU provides knowledge of secure communication protocols. |
| Topics | The following topics must be included in this KU:<br>1. Application and transport layer protocols: HTTP, HTTPS, SSH, SMTP and SSL/TLS<br>2. Attacks on TLS: Downgrade Attacks, Certificate Forgery, Implications of Stolen Root Certificates and Certificate Transparency<br>3. Internet/Network Layer security protocols: IPsec and VPN<br>4. Wireless network security protocols: WEP, WPA, WPA2, and WPA3<br>5. Data Link Layer security protocols: L2TP, PPP and RADIUS |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Explain main secure communication protocols at different network layers.<br>2. Illustrate attacks and countermeasures on transport layer security protocol. |

## Supply Chain Security (SCS)

| | |
|---|---|
| Description | This KU provides knowledge of risk and cybersecurity issues related to third party components used in building complex systems. |
| Topics | The following topics must be included in this KU:<br>1. Supply Chain Risks: Cybersecurity Risks Related to Third Party in the Supply Chain and Best Practices to manage them<br>2. Global Development Trends<br>3. Offshore Production<br>4. Transport and Logistics of IT Components<br>5. Evaluation of 3rd Party Development Practices<br>6. Capabilities and limitations of Software and Hardware Reverse Engineering<br>7. Procurement Process: Physical Security, Split Manufacturing, Traceability, Cargo Screening and Validation, Supplier Vetting |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Discuss cybersecurity issues related to outsourcing hardware, software development and integration.<br>2. Describe hardware and software security threats and risks in component procurement.<br>3. Demonstrate methods to mitigate supply chain cybersecurity risks and explain the challenges of these mitigation methods. |

## Systems Programming (SPG)

| | |
|---|---|
| Description | This KU provides knowledge, skills and ability to develop complex and low-level software, which is designed to provide services to other software. |
| Topics | The following topics must be included in this KU:<br>1. Hardware and Software Interfaces and Interactions<br>2. Types of Systems Programs: Development Environments, Operating Systems, Utilities, Networking Functions, Device Drivers, Storage Frameworks and Gaming Engines<br>3. Layered Services Design<br>4. Application Programming Interfaces (API's)<br>5. Programming Operating Systems Internal Interfaces<br>6. Low Level Programming: Assembly, C<br>7. Resource Optimization<br>8. Resource Management<br>9. Runtime Overhead Minimization<br>10. Direct Control of Memory Access and Flow Control<br>11. Memory Management in Systems Software<br>12. Security Concerns in Systems Software<br>13. Monitoring and Logging Systems Software |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Develop programs that can correctly operate under limited resources.<br>2. Apply a layered approach for API's access.<br>3. Implement new functions that can be embedded into an OS kernel.<br>4. Implement systems functions without using external libraries. |



Document Classification: Public

TLP: Clear

## Secure Programming Practices (SPP)

| | |
|---|---|
| Description | This KU provides knowledge skills and abilities needed to develop and implement secure software. |
| Topics | The following topics must be included in this KU:<br>1. Interpretation and realization of Security Requirements<br>2. Principles of Secure Programming<br>3. Robust Programming<br>4. Defensive Programming: Input Validation, Type checking, Bounds checking, Coverage of all traces, handle exceptions, Avoidance of risky coding constructs, and information leakage prevention<br>5. Security practices of classes: Prevention of external interfaces data changes by reference, Using Context for data access, Data update verification, and Authentication<br>6. Programming Flaws: Buffer Overflows, Integer Errors, Input Validation, API Abuse, Security Features, Time and State, Errors, Code Quality, Encapsulation, and Environment<br>7. Software Static and Dynamic Analysis<br>8. Data Obfuscation<br>9. Data Protection<br>10. Web Application Threats<br>11. Secure Programming paradigms: Pair programming, Code reviews, and Test-driven development<br>12. Uses of Cryptography in Programming |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Design and develop secure software that meets its functional requirements.<br>2. Describe the characteristics of secure programming.<br>3. Understand the vulnerabilities inherent in different programming languages.<br>4. Examine vulnerabilities introduced through the use of libraries and how to mitigate those vulnerabilities. |



Document Classification: Public

TLP: Clear

## Software Reverse Engineering (SRE)

| | |
|---|---|
| Description | This KU provides skills and ability to perform reverse engineering of executable code to determine its function, effect and implementation details. |
| Topics | The following topics must be included in this KU:<br>1. Malware Analysis<br>2. Reverse Engineering Tools & Techniques<br>3. Static vs Dynamic Analysis<br>4. Sandboxing<br>5. Anti-Reverse Engineering Techniques<br>6. Commercial software packers<br>7. Code disassembly<br>8. Memory Analysis tools |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Apply software reverse engineering tools to discover functionality and implementation details of software or malware.<br>2. Analyze malware using static, dynamic, code, and/or memory analysis techniques. |



Document Classification: Public

TLP: Clear

## Software Security Analysis (SSA)

| | |
|---|---|
| Description | This KU provides knowledge and skill of using tools and methods to analyze the security of software in binary or source code form. |
| Topics | The following topics must be included in this KU:<br>1. Testing Methodologies<br>2. Source and Binary Code Analysis<br>3. Static and Dynamic Analysis Techniques<br>4. Sandboxing<br>5. Common Analysis Tools and Methods |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Describe tools and techniques used for software security analysis.<br>2. Apply software security analysis tools to analyze unknown software components. |

## Systems Security Engineering (SSE)

| | |
|---|---|
| Description | This KU provides skills to participate in the development of large-scale secure systems using related techniques and methods throughout the entire system life-cycle. |
| Topics | The following topics must be included in this KU:<br>1. Testing Design<br>2. Testing methodologies<br>3. Emergent Properties<br>4. Systems Engineering<br>5. System Integration<br>6. Make or Buy Analysis<br>7. Systems Security Analysis<br>8. Enterprise System Components |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Participate in the development of system components by collecting and analyzing requirements along with designing, implementing, testing and maintaining components.<br>2. Analyze system components in a composed system and how they interact.<br>3. Analyze a given system design and assess its compliance with the system security requirements. |



Document Classification: Public

TLP: Clear

## Vulnerability Analysis (VLA)

| | |
|---|---|
| Description | This KU provides knowledge and skills related to detection, identification, root cause determination and mitigation of system and network vulnerabilities. |
| Topics | The following topics must be included in this KU:<br>1. Vulnerability Definition<br>2. System Modeling Techniques<br>3. Vulnerability Mapping<br>4. Vulnerability Characteristics and Classification.<br>5. Taxonomy: Buffer Overflows, Privilege Escalation, Rootkits, Trojans, Backdoors, Viruses, Return Oriented Programming, Social Engineering Vulnerabilities and Administrative Privileges Effect on Vulnerabilities<br>6. Vulnerabilities Root Causes<br>7. Mitigation Strategies<br>8. Countermeasure Analysis<br>9. Vulnerability Disclosure<br>10. Vulnerabilities Detection Tools and Techniques |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Apply vulnerabilities detection tools and techniques.<br>2. Construct vulnerability map of a given system.<br>3. Trace vulnerabilities to identify their root causes.<br>4. Analyze countermeasures for vulnerabilities mitigation.<br>5. Discuss scenarios when vulnerabilities must be disclosed. |

## Virtualization Technologies (VTT)

| | |
|---|---|
| Description | This KU provides knowledge of modern host virtualization and its implementation, deployment, use, system components and security. |
| Topics | The following topics must be included in this KU:<br>1. Virtualization Architectures<br>2. Virtualization Techniques for Code Execution<br>3. Memory Management in Virtual Environments<br>4. Networking in Virtual Environments<br>5. Storage in Virtual Environments<br>6. Scheduling of Virtual Machines<br>7. Migration and Snapshots<br>8. Virtual Management Layers<br>9. Digital Forensics in Virtual Environments<br>10. Security Risks and Considerations (e.g., VM Sprawl, Malware, VM Sandbox Escape) |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Explain virtualization concepts.<br>2. Compare and contrast various virtualization architectures<br>3. Design, construct, implement and configure virtualization environments.<br>4. Discuss potential virtualization security risks and mitigation strategies. |



Document Classification: Public

TLP: Clear

## Web Application Security (WAS)

| | |
|---|---|
| Description | This KU provides knowledge of technology, tools and practices related to web applications. It also provides skills to apply these tools and practices to develop and deploy secure web applications. |
| Topics | The following topics must be included in this KU:<br>1. Web Application Technologies: HTTP Protocol, Encoding Schemes, Web Application Architectures, AJAX, XML and JSON<br>2. Server-Side Controls<br>3. Authentication<br>4. Session Management<br>5. Access Controls<br>6. Client-Side Controls<br>7. Input-Based Vulnerabilities: SQL Injection, Blind SQL Injection, Cross-Site Scripting and Cross-Site Request Forgery<br>8. JavaScript and Cookies Attack<br>9. Function-Specific Input Vulnerabilities<br>10. Attacking Application Logic<br>11. Recent Attack Trends<br>12. Shared Hosting Vulnerabilities<br>13. Application Server Vulnerabilities |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Demonstrate common web application technologies and explain security issues related to them.<br>2. Develop and deploy secure web applications.<br>3. Illustrate web applications security principles. |



Document Classification: Public

TLP: Clear

## Wireless Sensor Networks (WSN)

| | |
|---|---|
| Description | This KU provides knowledge of wireless sensor networks principles, the challenges and cybersecurity aspects related to them. |
| Topics | The following topics must be included in this KU:<br>1. Wireless Sensor Devices<br>2. Wireless Sensor Networks Applications<br>3. Deploying Wireless Sensor Networks: Structured, Randomized, Topology, Signal Strength Control, Coverage, Mobility<br>4. Localization<br>5. Synchronization<br>6. Wireless Transmission Characteristics<br>7. Channel Access<br>8. Sleep Scheduling<br>9. Effective Energy Consumption<br>10. Data-Centric Network Services<br>11. Congestion Control and Transport Reliability<br>12. Security Aspects Associated with Wireless Sensor Networks |
| Learning Outcomes | By completing this KU, students should be able to:<br>1. Perform simulations of wireless sensor networks for given scenarios.<br>2. Apply appropriate security measures for wireless sensor networks.<br>3. Describe the challenges associated with wireless sensor networks, including localization, synchronization and power consumption. |



Document Classification: Public

TLP: Clear

# 4. Appendix (A): Examples of Specialized Cybersecurity Programs.

## A1. Bachelor of AI in Cybersecurity

| | |
|---|---|
| Required KU | 1. Cybersecurity Fundamentals (CSF)<br>2. Cybersecurity Design Principles (CDP)<br>3. IT Systems Components (ISC)<br>4. Basic Cryptography (BCY)<br>5. Basic Networking (BNW)<br>6. Basic Scripting and Programming (BSP)<br>7. Network Defense (NDF)<br>8. Operating Systems Concepts (OSC)<br>9. Data Structures (DST)<br>10. Databases (DAT)<br>11. Cyber Threats (CTH)<br>12. Policy, Legal, Ethics and Compliance (PLE)<br>13. Security Risk Analysis (SRA)<br>14. Cybersecurity Planning and Management (CPM)<br>15. Security Program Management (SPM) |
| Elective KUs | 1. Deep Learning (DLL)<br>2. Machine Learning (MLL)<br>3. Analytical Tools (ATT)<br>4. Data Administration (DBA)<br>5. Algorithms (ALG)<br>6. Advanced Algorithms (AAL)<br>7. Cloud Computing (CCO)<br>8. Secure Programming Practices (SPP)<br>9. Intrusion Detection/Prevention Systems (IDS)<br>10. Vulnerability Analysis (VLA) |



Document Classification: Public

TLP: Clear

## A2. Master of Cryptography

| | |
|---|---|
| Required KU | 1. Cybersecurity Fundamentals (CSF)<br>2. Cybersecurity Design Principles (CDP)<br>3. IT Systems Components (ISC)<br>4. Basic Cryptography (BCY)<br>5. Basic Networking (BNW)<br>6. Basic Scripting and Programming (BSP)<br>7. Network Defense (NDF)<br>8. Operating Systems Concepts (OSC) |
| Elective KUs | 1. Mathematical Foundations of Cryptography (FCY)<br>2. Introduction to the Theory of Computation (ITC)<br>3. Cryptography (CRY)<br>4. Data Integrity and Authentication (DIA)<br>5. Algorithms (ALG)<br>6. Cryptography Engineering (CRE)<br>7. Advanced Cryptography (ACR) |



Document Classification: Public

TLP: Clear

## A3. Master of ICS/OT Cybersecurity

| | |
|---|---|
| Required KU | 1. Cybersecurity Fundamentals (CSF)<br>2. Cybersecurity Design Principles (CDP)<br>3. IT Systems Components (ISC)<br>4. Basic Cryptography (BCY)<br>5. Basic Networking (BNW)<br>6. Basic Scripting and Programming (BSP)<br>7. Network Defense (NDF)<br>8. Operating Systems Concepts (OSC) |
| Elective KUs | 1. Industrial Control Systems (ICS)<br>2. Cyber-Physical System (CPS)<br>3. Embedded Systems (ESY)<br>4. Hardware/Firmware Security (HFS)<br>5. Internet of Things (IoT)<br>6. Wireless Sensor Networks (WSN)<br>7. Business Continuity, Disaster Recovery and Incident Management (BDR) |



Document Classification: Public

TLP: Clear

## A4. Master of Cybersecurity Management

| | |
|---|---|
| Required KU | 1. Cybersecurity Fundamentals (CSF)<br>2. Cybersecurity Design Principles (CDP)<br>3. IT Systems Components (ISC)<br>4. Cyber Threats (CTH)<br>5. Policy, Legal, Ethics and Compliance (PLE)<br>6. Security Risk Analysis (SRA)<br>7. Cybersecurity Planning and Management (CPM)<br>8. Security Program Management (SPM) |
| Elective KUs | 1. Business Continuity, Disaster Recovery and Incident Management (BDR)<br>2. Information Assurance Standards (IAS)<br>3. Information Assurance Compliance (IAC)<br>4. Supply Chain Security (SCS)<br>5. Information Assurance Architectures (IAA)<br>6. Life-Cycle Security (LCS)<br>7. Cyber Crime (CCR) |



Document Classification: Public

TLP: Clear

# 5. Appendix (B): Summary of Version Updates

This version (SCyber-Edu – 2: 2026) represents a significant update of the Saudi Cybersecurity Higher Education Framework to address the highly dynamic nature of the cybersecurity discipline. Key updates include:

1. **Comprehensive KU Revision:** All topics and learning outcomes of Knowledge Units (KUs) have been revised to reflect current technological trends and threat landscapes.
2. Knowledge Unit Expansion: New KUs have been introduced, and redundant KUs have been removed to ensure the framework remains streamlined and relevant.
3. Programs Updates: The programs descriptors and KUs requirements have been revised to align with latest benchmark standards and frameworks.
4. New Program Tracks: A Master's degree (Cybersecurity Track) has been introduced to accommodate existing master's programs in related disciplines that include a cybersecurity track at higher education institutions.
5. Specialization Appendix: A new appendix has been added specifically for cybersecurity specializations, providing guidance for institutions moving beyond general cybersecurity programs.



Document Classification: Public

TLP: Clear

# 6. References


[1] National Qualifications Framework (NQF), Education and Training Evaluation Commission, 2026.

[2] The National Centers of Academic Excellence in Cyber Defense (CAE-CD) Designation Program Guidance and Knowledge Units, 2024.

[3] The IEEE/ACM Cybersecurity Curricula, 2017.

[4] The IEEE/ACM Computer Science Curricula, 2023.

[5] E. Fernandez-Buglioni, Security Patterns in Practice: Designing Secure Architectures Using Software Patterns, Wiley, 2013.

[6] S. McConnell, Code Complete: A Practical Handbook of Software Construction, 2nd ed., Microsoft Press, 2004.

[7] Shostack, Threat Modeling: Designing for Security, John Wiley & Sons Inc., 2014.

[8] Reynolds, Ethics in Information Technology, 5th ed., Cengage Learning, 2014.

[9] J Martin and M Talabis, Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis, 2013.

[10] T. H. Cormen, C. E. Leiserson and R. L. Rivest, Introduction to Algorithms, The MIT Press, 2009.

[11] Anti-Cyber Crime Law in the Kingdom of Saudi Arabia.

[12] B. Krishnamachari, Networking Wireless Sensors, Cambridge University Press, 2009

[13] CyBOK, The Cyber Security Body of Knowledge (Version 1.1.0), 2021


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority