



## Data Security

### Course Overview

**Course Dates:** March 31 - April 11, 2025

**Duration:** 2 weeks

**Instructional Hours:** 15 contact hours

**Delivery Format:** Asynchronous online

**Target Audience:** IT and Cybersecurity practitioners

**Recommended Background:** Learners should have basic familiarity with computer concepts and operations.

**CEUs:** 1.5, **CPEs:** 1

**Course Instructor:**

Instructor	Email Address
Dr. Elizabeth Rasnick	erasnick@uwf.edu
Mrs. Sajida Shabanali	sshabanali@uwf.edu

### Course Outline

Module	Topic	Lab
Module 1	Access Control	Data Classification
Module 2	Encryption	Encryption
Module 3	Database Security	Database Security
Module 4	Data Privacy	Data Privacy
Module 5	Data Security Policies	Data Security Policies

### NIST NICE Cybersecurity Workforce Framework Mapping

#### Work Roles

The course addresses cybersecurity work roles as identified in NIST’s Special Publication 800-181 rev 1, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework available at

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>

**The course is mapped to the following work roles:**

- Systems Security Analyst (Operate and Maintain, OPM ID: 461)



# CENTER FOR CYBERSECURITY

---

## AT THE UNIVERSITY OF WEST FLORIDA

- Privacy Officer/Privacy Compliance Manager (Oversee and Govern, OPM ID: 732)
- Cyber Defense Analyst (Protect and Defend, OPM ID: 511)

**Abilities, Tasks, Knowledge, and Skills required to fulfill tasks corresponding to the above work roles:**

- Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (A0123)
- Assess adequate access controls based on principles of least privilege and need-to-know (T0475)
- Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources (T0261)
- Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure (T0348)
- Knowledge of cybersecurity and privacy principles (K0004)
- Knowledge of cyber threats and vulnerabilities (K0005)
- Knowledge of host/network access control mechanisms (K0033)
- Knowledge of basic system, network, and OS hardening (K0205)
- Skill in applying host/network access controls (e.g., access control list) (S0007)
- Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation) (S0367)