Cybersecurity Incident Response and Resilience Planning (CIRRP) for Government Leaders

UWF Florida Cybersecurity Training Program
Offered by the University of West Florida Center for Cybersecurity

Course Overview

Cyber Skills Exercise Date: October 21, 2024

Cyber Skills Exercise Times: 8 am – 4 pm CT with a break from 11:30 am – 12:30 pm CT

Duration: 1 day

Estimated Time Commitment: 7 hours total

Instructional Hours: 7 contact hours

Delivery Format: Synchronous online / one-day session / 2 Hours expected of active participation and independent study

Target Audience: Elected and appointed officials, governmental leaders, administrators, emergency management personnel, IT and cybersecurity personnel, non-technical personnel

Required Prerequisites / Background: None

Course Credits

CEUs: 0.7, **CPEs:** 8.4

Course Instructor(s):

Lead Instructor	Email
Dr. Haris Alibašić, Associate Professors, UWF, College of Business, Public Administration Program	halibasic@uwf.edu

Course Description

Course Overview
The "Cybersecurity Incident Response and Resilience Planning (CIRRP) for Government Leaders" training is designed to equip appointed and elected officials with the knowledge and skills to respond to cybersecurity incidents effectively. This comprehensive course integrates change management principles and organizational resilience to ensure robust and effective incident response strategies.

Learning Outcomes
By the end of this course, participants will be able to:

1. Understand the fundamentals of cybersecurity threats and incident response.

2. Apply change management principles to improve the efficiency of incident response plans.
3. Develop and implement strategies to enhance organizational resilience.
4. Tailor incident response plans to meet the specific needs of their respective offices.
5. Analyze real-world case studies to derive practical insights and best practices.

Hands-On Exercises

- **Case Study Discussions:** Analyze and discuss notable cybersecurity incidents to understand effective response and resilience strategies.

Certifications Prepared For

This course prepares participants for certifications in cybersecurity and incident response, including:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified in Risk and Information Systems Control (CRISC)

Course Materials

Participants will have access to a comprehensive set of materials, including:

- Detailed reading materials and case studies
- Templates and checklists for incident response planning
- Access to online documents and potential for further educational opportunities.

Join us for this essential training to enhance your organization's preparedness and resilience against cybersecurity threats.

NIST NICE Cybersecurity Workforce Framework Mapping

The course prepares for the following cybersecurity roles defined by the NICE Cybersecurity Workforce Framework.

Cybersecurity Work Roles and Categories:

- **Cyber Defense Analyst (Protect and Defend, PR-CDA-001):** Analyzes data from multiple sources to identify, respond to, and recover from cybersecurity threats.
- **Incident Responder (Protect and Defend, PR-IR-001):** Manages and coordinates responses to cybersecurity incidents, ensuring proper documentation and reporting.
- **Risk Manager (Oversee and Govern, OV-RM-001):** Identifies, assesses, and prioritizes risks to organizational operations and assets and develops strategies to mitigate those risks.