## **CYBR 475: Cyber Incident Handling and Response (3 credits)**

This course provides an in-depth examination of Incident Response and Management, focusing on key areas such as Incident Response Theory, Pre-incident Preparation, and Remediation. It covers the dynamics of Incident Investigation, Scope Determination, and the strategic use of Tools and Technologies in incident response. The course includes essential elements like Incident Report Writing, Post-Incident Analysis, and Crisis Communication, along with effective management strategies for Cybersecurity Incident Response Teams (CIRT). Additionally, students will explore the latest Emerging Trends and Future Challenges in incident response across various environments.  ***(****Prerequisite****:*** *CYBR 310****)***

**Course Learning Outcomes:**

By the end of the course, students will be able to:

A1. Demonstrate critical knowledge in diverse cyber incident response areas.

A2. Adapt appropriate methods, practices, techniques, and tools related to incident response.

B1. Critically evaluate and synthesize information and concepts within complex scenarios to develop appropriate incident response plans.

B2. Effectively communicate findings in incidents and incident response plans through comprehensive reports and presentations.

**Course Learning Materials:**

* "Digital Forensics and Incident Response: Incident Response Tools and Techniques for Effective Cyber Threat Response," 3rd ed., Packt Publishing, 2022. ISBN-13: 978-1803238678, ISBN-10: 1803238674.
* Computer Security Incident Handling Guide by National Institute of Standards and Technology (NIST) (2012).
* Incident Response & Computer Forensics by Jason T. Luttgens and Matthew Pepe (2014).
* Blue Team Handbook: SOC, SIEM, and Threat Hunting by Don Murdoch GSE (2019).

**Course Content:**

1. Incident Response Theory
2. Pre-incident Preparation
3. Incident Investigation
4. Initial Development of Leads
5. Incident Scope
6. Incident Report Writing
7. Remediation
8. Tools and Technologies for Incident Response
9. Post-Incident Analysis and Review
10. Crisis Communication and Stakeholder Management
11. Cybersecurity Incident Response Team (CIRT) Management
12. Incident Response in Different Environments
13. Emerging Trends and Future Challenges in Incident Response