Course Specification

(Postgraduate Programs)

Course Title:	**Incident Response Technologies**
Course Code:	**CYS 27121**
Program:	**Master of Science in Cyber Security**
Department:	**Information System**
College:	**Computing and Information Technology**
Institution:	**University of Bisha**
Version:	*Course Specification Version Number*
Last Revision Date:	*Pick Revision Date.*

Table of Contents

A. General information about the course:

1. Course Identification:

1. Credit hours: (4.5)				
2. Course type				
A.	☐University	☐College	☐Department	☐Track
B.	☐Required		☒Elective	
3. Level/year at which this course is offered: (2 Level/ 1st Year)				
4. Course General Description:				
This course provides comprehensive knowledge of security incidents, intrusions, and response technologies. This course includes identifying and categorizing incidents, responding to .incidents, log analysis, network traffic analysis, and tools				
5. Pre-requirements for this course (if any)**:**				
None				
6. Pre-requirements for this course (if any)**:**				
None				
7. Course Main Objective(s):				

- To provide fundamental knowledge and procedures for handling cybersecurity attacks, data breaches, and data damage incidents.
- ;To be able to conduct fundamental forensic analysis of Windows and Linux systems
- To be able to use popular tools in analyzing compromised systems and conducting static and dynamic malware analysis.
- To be able to conduct basic penetration testing such as information gathering and exploitation.
- To be able to use Wireshark for network traffic capture and analysis, and use Splunk .software to process and analyze security logs

2. Teaching Mode: (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	60	100%
2	E-learning	N/A	N/A

No	Mode of Instruction	Contact Hours	Percentage
3	Hybrid • Traditional classroom • E-learning	N/A	N/A
4	Distance learning	N/A	N/A

3. Contact Hours: (based on the academic semester)

No	Activity	Contact Hours
1.	**Lectures**	30
2.	**Laboratory/Studio**	20
3.	**Field**	-
4.	**Tutorial**	-
5.	**Others (specify) Seminar**	10
	Total	60

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods:

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	State the essentials of Incident Response Technologies	K1	**Interactive Lectures**	**Quizzes and Tests**
1.2	Explain the concepts of incidents security and response technologies.	K2	**Interactive Lectures**	**Quizzes and Tests**
1.3	Demonstrate various algorithm methods of Incident Response Technologies	K3	**Interactive Lectures**	**Quizzes and Tests**

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
2.0	**Skills**			
2.1	Design basic cyber defence applicationss.	S1	**Hands-On Labs**	**Assignments**
2.2	Implement algorithms that prevent cyber threats and mitigate cyber incidents.	S2	**Hands-On Labs**	**Code Review Peer Assessment**
2.3	Detect cyber threats of operating systems, networks and various applications.	S3	**Case Studies**	**Code Review Peer Assessment**
3.0	**Values, autonomy, and responsibility**			
3.1	Cooperate requirements and techniques for wireless security, risk analysis, security controls in team through communication, negotiate and dialogue for any cyber threats and incidents.	V1	**Project-Based Learning**	**Project Presentations**
3.2	Ability to engage in lifelong learning to secure society against cyber attacks	V2	**Peer Teaching**	

C. Course Content:

No	List of Topics	Contact Hours
1.	Introduction to incident response technologies and overview of Mobile and Wireless Networks. Mobile cellular networks, different generations (1G) (2G) (3G) (4G) (5G) mobile.	5

2.	IEEE wireless networks, WLAN: IEEE 802.11, WPAN: IEEE 802.15, WMAN: IEEE 802.16, WMAN mobile: IEEE 802.20, MIH: IEEE 802.21, WRAN: IEEE 802.22	5
3.	Wireless and Mobile Network Security, All-IP, IMS and FMC, B3G and 4G, Vulnerabilities of Wired and Wireless Networks. Security in the digital age, Private property,	5
4.	Trust and subjectivity in security Threats and risks to telecommunications systems, the Role of Threat models, homogeneity vs. heterogeneity, security Risks to the infrastructure, Security Mechanisms, Secure communication protocols, and VPN, Secure Socket Layer (SSL), and Transport Layer Security (TLS), IPsec VPN and SSL VPN.	5
5.	AAA protocols to control access to a private network or an operator's network. Access control, Firewalls, Wi-Fi Security Dedicated Architectures Hot spot architecture: captive portals, Wireless intrusion detection systems (WIDS), architectures, events, for example, Rogue access point detection and prevention systems.	4
6.	Wireless honeypots, requirements, design, expected results, multimedia content marking, steganography, cryptography, and peculiarities in the mobility context.	4
7.	Bluetooth Security, technical specification, Organization of Bluetooth nodes in the network, Protocol architecture in a Bluetooth node SCO and ACL logical transports, Security mode in Bluetooth, Authentication and pairing, Bluetooth encoding, and Attacks.	4
8.	Wi-Fi Security, Attacks, Security in the IEEE 802.11 standard, mechanisms, WEP (Wired Equivalent Privacy), Security in 802.1x, architecture, Authentication, The 802.11i security WiMAX, Security evolution, Security according to 802.16-2004.	4
9.	Security in Mobile Telecommunication Networks, Signaling System 7 (SS7), protocol stack, Vulnerability of SS7 networks, Security in the GSM, GPRS security, 3G security	4
10.	Security in Next Generation Mobile Networks, SIP generalities, SIP security flaws, VoIP, VoIP security flaws, Making VoIP secure, Security of IP-Based Mobile Networks, Vulnerabilities of Mobile IP networks, IPv6 mobility mechanisms (MIPv6, HMIPv6, FMIPv6).	4
11.	**Incident Response and Management:** Incident Detection, Incident Response Life Cycle, Key Steps in Incident Handling, Communication and Reporting, Role of SOC in Incident Response	4
12.	**Advanced Threat Detection Techniques:** Behavioral Analysis, Threat Intelligence, Machine Learning in Threat Detection, Zero-Day Attack Identification, Use of AI in Security	4

13.	**Forensics in Mobile and Wireless Security:** Introduction to Digital Forensics, Mobile Forensics Techniques, Evidence Collection and Analysis, Chain of Custody, Challenges in Mobile Forensics	4
14.	**Cybersecurity in 5G Networks:** Security Challenges in 5G, 5G Network Architecture, 5G Security Protocols, Potential Vulnerabilities, Privacy in 5G, Emerging Threats and Mitigation Strategies	4
Total		**60**

D. Students Assessment Activities:

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1	Assignments	Weekly	10%
2	Quiz in blackboard/traditional mode	4th week	10%
3	Lab test	4th week	10%
4	Midterm exam	6th week	20%
5	Group project and presentation	8th week	10%
6	Final exam	End of the semester	40%
	Total		100

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.)

E. Learning Resources and Facilities:

1. References and Learning Resources:

Essential References	• Wolfgang Osterhage, Wireless Network Security, Goethe-Universität Frankfurt, Germany Second Edition,2018 • Hakima Chaouchi, Maryline Laurent-Maknavicius, Wireless and Mobile Network Security, British Library, ISBN: 978-1-84821-117-9
Supportive References	
Electronic Materials	http://www.honeyd.org/ http://www.citi.umich.edu/u/provos/cybersecurity/
Other Learning Materials	Students must find articles and other documents related to the topics covered in each unit from various sources, such as the IEEE

	and ACM digital libraries. Some of these textbooks are listed under References below.

2. Educational and Research Facilities and Equipment Required:

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Classrooms, laboratories, demonstration rooms/labs
Technology equipment (Projector, smart board, software)	Smart Board, projector, internet, and whiteboard.
Other equipment (Depending on the nature of the specialty)	Connected computers (local network) with internet through switch and firewall.

F. Assessment of Course Quality:

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	• Students. • Quality Assurance Committee.	• Direct
Effectiveness of students' assessment	• Instructor. • Program Leader.	• Direct
Quality of learning resources	• Peer Reviewers. • Quality Assurance Committee.	• Indirect. • Direct.
The extent to which CLOs have been achieved	• Quality Assurance Committee. • Independent faculty members.	• Direct. • Indirect.
Other	• Quality Assurance Committee. • Program Leader. • Plans and Curriculum Committee.	• Direct. • Indirect.

Assessor (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)

Assessment Methods (Direct, Indirect)

G. Specification Approval Data:

COUNCIL /COMMITTEE	
REFERENCE NO.	

DATE	