



Republic of the Philippines
SULTAN KUDARAT STATE UNIVERSITY
Isulan, Sultan Kudarat
College of Computer Studies
S.Y. 2024-2025



IAS314

Information Assurance and Security 1

2nd Semester
School Year 2024 – 2025

Prepared by:
KRISTINE MAE H. AMPAS, MIT



Republic of the Philippines
SULTAN KUDARAT STATE UNIVERSITY
Isulan, Sultan Kudarat
College of Computer Studies
S.Y. 2024-2025



UNIVERSITY VISION

A trailblazer in arts, science and technology in the region.

UNIVERSITY MISSION

The University shall primarily provide advance instruction and professional training in Science and Technology, Agriculture, Fisheries, Education and other related field of study. It shall undertake research and extension services, and provide progressive leadership in its area specialization.

UNIVERSITY GOAL

To produce graduates with excellent and dignity in arts, science na technology.

UNIVERSITY OBJECTIVES

- a. Enhance competency development, commitment, professionalism, unity and true spirit of service for public accountability, transparency and delivery of quality services;
- b. Provide relevant programs and professional trainings that will respond to the development needs of the region;
- c. Strengthen local and international collaborations and partnership for borderless programs;
- d. Develop a research culture among faculty and students;
- e. Develop and promote environmentally-sound and market-driven knowledge and technologies at par with international standards;
- f. Promote research-based information and technologies for sustainable development;
- g. Enhance resource generation and mobilization to sustain financial viability of the university.

Program Objectives and its relationship to University Goals:

PROGRAM OBJECTIVES (PO)		OBJECTIVES						
A graduate of BS in Information Technology can:								
a. Innovate technological concepts and ideas underpinning desired IT solutions;		a	b	c	d	e	f	g
b. Administer competently the computer networks, system development, software applications, hardware and maintenance;		/	/	/	/	/	/	/
c. Design industry-based applications, infrastructures and technologies that will promote the advancement and development of the community;		/	/	/	/	/	/	/
d. Adopt to various national and international industries standards in the practice of the profession; and;		/	/	/	/	/	/	/
e. Demonstrate professionalism in the social, environmental and legal aspects of Information Technology.		/	/	/	/	/	/	/

- 2. **Course Code** : IAS314
- 3. **Course Title** : Information Assurance and Security 1
- 4. **Prerequisite** : None
- 5. **Credits** :3 UNITS

1. Course Descriptions

This course will provide learners with principles of data and technology that frame and define cybersecurity. Learners will gain insight into the importance of cybersecurity and the integral role of cybersecurity professionals. The interactive, self-guided format will provide a dynamic teaming experience where users can explore foundational cybersecurity principles, security architecture, risk management, attacks, incidents, and emerging IT technologies.

6. Course Learning Outcomes and Relationship to Program Educational Objectives

COURSE LEARNING OUTCOMES		PROGRAM OBJECTIVES				
At the end of the semester, the students can:						
a.	Analyze the relationship between threats, vulnerabilities, countermeasures, attacks, compromises, remediation throughout the entire system life cycle.	a	b	c	d	e
b.	Assess cybersecurity risk management policies to protect an organizations critical information asset adequately.	/	/	/	/	/
c.	Detect legal and ethical considerations related to the handling and management of enterprise information assets.	/	/	/	/	/

7. Course Content

Course Objectives, Topics, Time allotment	Desired Student Learning Outcomes	Outcomes-Based Assessment (OBA) Activities	Evidence of Outcomes	Course Objectives	Program Outcomes	Values Integration
Topic: SKSU VMGO, Classroom Policies, Course Overview, Course Requirements, Grading System (2 hours)						
1. Discuss the VMGO of the university, classroom policies, scope of the course, course requirements and grading system	1.1 Student can be aware of and appreciate of the university's VMGO, classroom policies, course overview,	Individual participation in class discussion and group presentation	Individual participation in class discussion and group presentation			Value of appreciation

	requirements and grading system.					
1. Information System Security (lec:6hrs)						
1.1 Cybersecurity Professional and their task risk, threats and vulnerabilities 1.2 The CIA Triad 1.3 Data Classification Standards	1.1 Describe the cybersecurity role of a company 1.2 Identify the importance of data and its worth	Discussion Activities Recitation	Recitation Quizzes Laboratory activity	a	a, d, e	Unity and team work Value of participation Communication Challenge Achievement
2. Security Concepts and Goals (lec:6hrs)						
2.1 Subjects & Objects of Security 2.2 Security Objectives 2.3 IT Security Framework 2.4 Security Architecture	2.1 Identify each security rendered in the network 2.2 Test the probable framework implemented in the network landscape	Discussion Review	Rubrics score cards of laboratory exercise output accomplished by the instructor	b, c, d		Unity and team work Value of participation Communication Challenge Achievement
3. Typical Domains of IT Infrastructure (lec:6hrs)						
3.1 User Domain 3.2 LAN Domain 3.3 WAN Domain	3.1 Execute the domain structures of each IT infrastructure	Discussion Recitation	Recitation Quizzes Laboratory activity	b,c,d		Unity and team work Value of participation

3.4 Remote Access Domain	3.2 Analyze cases regarding appropriate ethics in the internet					Communication
3.5 System/Application Domain						Challenge
3.6 Ethic and the Internet						Achievement
4. Security System Engineering (lec:3hrs)						
4.1 Policy Development	4.1 Outline the important of network policies and compliance	Discussion Recitation	Recitation Quizzes Laboratory activity	b, c, d, e		Unity and team work
4.2 Process Management						Value of participation
4.3 Network Compliance	4.2 Perform different methods of encryptions for information security					Communication
4.4 Cryptography						Challenge
						Achievement
5. Ontology of Malwares (lec:3hrs)						
5.1 Spyware	5.1 Compare the different classification of hackers and their roles in society	Discussion Recitation	Quizzes Laboratory activity	b, c, d, e		Unity and team work
5.2 Adware						Value of participation
5.3 Rootkit	Communication					
5.4 Ransomware	Challenge					
5.5 Worms	5.2 Identify the validity of each attack and foresee					Achievement
5.6 Trojan Horses						

5.7 Backdoors	the patterns of attack					
6. Risk Management (lec:3hrs)						
6.1 Elements and categories of risks	6.1 Identify possible risks encountered in the network during an attack	Discussion Activities Recitation	Quizzes Laboratory activity	b, c, d, e		Unity and team work
6.2 Risk Monitoring and Responses	6.2 Perform root-cause analysis in managing possible risks before during and after an attack					Value of participation
6.3 Incident Handling and Documentation						Communication
6.4 Backup and Recovery						Challenge
						Achievement
7. Incident Countermeasure (lec:3hrs)						
7.1 Netiquette	7.1 Outline the importance of fail-safe methods	Discussion Recitation	Quizzes Laboratory activity	b, c, d, e		Unity and team work
7.2 User Management	7.2 Identify actions to counter the soonest intrusions and attacks					Value of participation
7.3 Firewall and Software						Communication
7.4 Authentication Mechanism						Challenge
						Achievement
Examination (4 hours) Lectures (30 hours) Total No. of Hours: 34 hours						

7. Course Evaluation

Course Requirement: Demonstrate Problem Solving skills in python programming language.

Grading System:

MIDTERM TERM

Exam 40%

Attendance 10%

Assignment/Quizzes 15%

Laboratory Exercise/Project 35%

FINAL TERM

Exam 40%

Attendance 10%

Assignment/Quizzes 15%

Laboratory Exercise/Project 35%

MTG+FTG/2=FG

References:

TextBooks:

1. Death, D. (2017). Computer and information security handbook. Birmingham: Packt Publishing
2. Supporting Learning Flow Through Integrative Technologies, Edited by, Tsukasa Hirashima, Ulrich Hoppe, Shelley Shwu-Ching Young
3. Combining Multiple Knowledge Representation Technologies into Agent Programming Languages, Mehdi M. Dastani, Koen V. Hindriks, Peter Novák, Nick A. M. Tinnemeier

Supplemental:

1. <https://content.sciendo.com/view/journals/rput/26/42/article-p127.xml>
2. [https://ascelibrary.org/doi/abs/10.1061/\(ASCE\)1527-6988\(2008\)9:2\(61\)](https://ascelibrary.org/doi/abs/10.1061/(ASCE)1527-6988(2008)9:2(61))
3. <https://academic.oup.com/bioinformatics/article/36/3/982/5554700>
4. <https://www.igi-global.com/chapter/building-integrative-enterprise-knowledge-portals/24415>

Prepared by:

KRISTINE MAE H. AMPAS, MIT

Faculty

Reviewed by:

ESNEHARA P. BAGUNDANG, MSIT

Faculty Program Chairperson, BSIT

Approved:

ELBREN O. ANTONIO, DIT

Dean, College of Computer Studies