جـامعـة الـزيـتـونـــة الأردنـيـة

Al–Zaytoonah University of Jordan

كلية العلوم وتكنولوجيا المعلومات

Faculty of Science and Information Technology

" عراقة وجودة"

"Tradition and Quality"

QF01/0408-4.0E	**Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department**

Study plan No.	**2024/2025**		**University Specialization**		**Cybersecurity**	
Course No.	0125465		**Course name**		**Cloud Computing Security**	
Credit Hours	**3**		**Prerequisite Co-requisite**		**Database and Security**	
Course type	□ MANDATORY UNIVERSITY REQUIREMENT	□ UNIVERSITY ELECTIVE REQUIREMENTS	□ FACULTY MANDATORY REQUIREMENT	□ Support course family requirements	□ ✓ **Mandatory requirements**	□ Elective requirements
Teaching style	□ **Full online learning**		□ Blended learning		□ ✓Traditional learning	
Teaching model	□ 2Synchronous: 1asynchronous		□ 2 face to face : 1synchronous		□ **3 Traditional**	

Faculty member and study divisions information (to be filled in each semester by the subject instructor)

Name	Academic rank	Office No.	Phone No.	E-mail	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**

Brief description

This course covers cloud computing security principles, including service models, deployment strategies, and the shared responsibility model. Topics include IAM, data encryption, virtualization, network security, compliance, and incident response. Hands-on labs and case studies equip students to design and manage secure cloud solutions.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	Kumar, T.A., Samuel, T.A., Samuel, R.D.J. and Niranjanamurthy, M. eds., 2022. Privacy and security challenges in cloud computing: A holistic approach. CRC Press. Manvi, S. and Shyam, G., 2021. *Cloud computing: Concepts and technologies*. CRC Press.			
Supportive learning resources (Books, databases, periodicals, software, applications, others)	Manvi, S. and Shyam, G., 2021. *Cloud computing: Concepts and technologies*. CRC Press.			
Supporting websites				
The physical environment for teaching	□ **Class room**	□ labs	□ **Virtual educational platform**	□ Others
Necessary equipment and software				

Supporting people with special needs	
For technical support	**E-learning and Open Educational Center. Computer Center**

Course learning outcomes (S= *Skills, C= Competences K= Knowledge,)*

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	Understanding the fundamental principles of cloud computing, including models (IaaS, PaaS, SaaS) and deployment types (Public, Private, Hybrid, Community).	**MK1**
K2	Familiarity with cloud security frameworks and standards (e.g., NIST, ISO/IEC 27017 & 27018, CSA Guidelines).	**MK2**
K3	Knowledge of identity and access management (IAM) principles, including multi-factor authentication (MFA) and role-based access control (RBAC).	**MK4**
K4	Awareness of data security techniques such as encryption, key management, and addressing data sovereignty issues.	**MK1**
K5	Comprehensive understanding of threats, vulnerabilities, and incident response in cloud environments.	**MK5**
	Skills	
S1	Ability to configure IAM roles and enforce access controls in cloud platforms such as AWS, Azure, and GCP.	**MK4**
S2	Skill in securing containerized applications (e.g., Docker, Kubernetes) and virtualized environments.	**MK1**
S3	Proficiency in implementing network security measures, such as configuring Virtual Private Clouds (VPCs) and setting up security monitoring tools.	**MK3**
	Competences	
C1	Capability to design and implement secure cloud architectures while adhering to compliance requirements (e.g., GDPR, HIPAA).	
C2	Competence in analyzing and responding to cloud security incidents, including forensic investigations and remediation.	
C3	Ability to integrate advanced security concepts, such as Zero Trust Architecture and AI-based cloud security measures, into organizational practices.	

Mechanisms for direct evaluation of learning outcomes

Type of assessment / learning style	Fully electronic learning	Blended learning	Traditional Learning (Theory Learning)	Traditional Learning (Practical Learning)
First exam	0	**0**	0	0
Second / midterm exam	%30	**%30**	%30	%30
Participation / practical applications	0	**0**	0	0
Asynchronous interactive activities	%30	**%30**	%30	%30

final exam	%40	**%40**	%40	%40

Note: Asynchronous interactive activities are activities, tasks, projects, assignments, research, studies, projects, work within student groups ... etc, which the student carries out on his own, through the virtual platform without a direct encounter with the subject teacher.

Schedule of simultaneous / face-to-face encounters and their topics

Week	Subject	learning style*	Reference **
1	Introduction to Cloud Computing and Security • Overview of Cloud Computing: Models (IaaS, PaaS, SaaS) and Deployment Types (Public, Private, Hybrid, Community). • Importance of Cloud Security. • Shared Responsibility Model.	Traditional learning	Manvi, S. and Shyam, G., 2021. *Cloud computing: Concepts and technologies*
2	Cloud Security Frameworks and Standards • NIST Cloud Security Framework. • ISO/IEC 27017 & 27018. • Cloud Security Alliance (CSA) Guidelines.	Traditional learning	Manvi, S. and Shyam, G., 2021. *Cloud computing: Concepts and technologies*
3	Identity and Access Management (IAM) • Principles of IAM in the cloud. • Multi-factor Authentication (MFA) and Single Sign-On (SSO). • Role-Based Access Control (RBAC) and Policy-Based Access Control.	Traditional learning	Manvi, S. and Shyam, G., 2021. *Cloud computing: Concepts and technologies*
4	Data Security in the Cloud • Data encryption in transit and at rest. • Key management and Hardware Security Modules (HSM). • Data residency and sovereignty issues.	Traditional learning	Manvi, S. and Shyam, G., 2021. *Cloud computing: Concepts and technologies*
5	Virtualization and Container Security • Virtual Machine (VM) security. • Container security challenges (e.g., Docker, Kubernetes). • Best practices for securing virtualization.	Traditional learning	Manvi, S. and Shyam, G., 2021. *Cloud computing: Concepts and technologies*
6	Network Security in Cloud Environments • Cloud-native firewalls and security groups. • Virtual Private Cloud (VPC) and subnets. • Secure communication protocols.	Traditional learning	Kumar, T.A., Samuel, T.A., Samuel, R.D.J. and Niranjanamurthy, M. eds., 2022. Privacy and security challenges in cloud computing: A holistic approach. CRC Press
7	Midterm Review and Exam		
8	Threats and Vulnerabilities in the Cloud • Common threats: DDoS, insider threats,	Traditional learning	Kumar, T.A., Samuel, T.A., Samuel, R.D.J. and

	misconfigurations. • Vulnerability assessment tools and methodologies		Niranjanamurthy, M. eds., 2022. Privacy and security challenges in cloud computing: A holistic approach. CRC Press
9	Cloud Security Monitoring and Incident Response • Monitoring tools: CloudWatch, Azure Monitor. • Incident response lifecycle. • Log management and analytics.	Traditional learning	Kumar, T.A., Samuel, T.A., Samuel, R.D.J. and Niranjanamurthy, M. eds., 2022. Privacy and security challenges in cloud computing: A holistic approach. CRC Press
10	Regulatory and Legal Compliance • GDPR, HIPAA, PCI-DSS in the cloud. • Contracts and Service Level Agreements (SLAs). • Auditing cloud providers.	Traditional learning	Kumar, T.A., Samuel, T.A., Samuel, R.D.J. and Niranjanamurthy, M. eds., 2022. Privacy and security challenges in cloud computing: A holistic approach. CRC Press
11	Cloud Application Security • Secure Software Development Lifecycle (SDLC) in the cloud. • Protecting APIs and serverless applications. • OWASP Top 10 for cloud apps.	Traditional learning	Kumar, T.A., Samuel, T.A., Samuel, R.D.J. and Niranjanamurthy, M. eds., 2022. Privacy and security challenges in cloud computing: A holistic approach. CRC Press
12	Cloud Forensics and Legal Challenges • Conducting forensics in a cloud environment. • Chain of custody in cloud investigations. • Challenges in multi-tenant environments.	Traditional learning	Kumar, T.A., Samuel, T.A., Samuel, R.D.J. and Niranjanamurthy, M. eds., 2022. Privacy and security challenges in cloud computing: A holistic approach. CRC Press
13	Advanced Security Concepts • Zero Trust Architecture in the cloud. • Securing hybrid and multi-cloud environments. • Artificial Intelligence and Machine Learning in cloud security.	Traditional learning	Kumar, T.A., Samuel, T.A., Samuel, R.D.J. and Niranjanamurthy, M. eds., 2022. Privacy and security challenges in cloud computing: A holistic approach. CRC Press
14	Cloud Penetration Testing • Legal considerations and scope. • Tools and methodologies for cloud pen testing. • Reporting and remediation.	Traditional learning	Kumar, T.A., Samuel, T.A., Samuel, R.D.J. and Niranjanamurthy, M. eds., 2022. Privacy and security challenges in cloud computing: A holistic approach. CRC Press
15	Emerging Threats and Future Directions • Quantum computing implications for cloud security. • Advances in cryptography. • Securing IoT and edge devices in the cloud.	Traditional learning	Kumar, T.A., Samuel, T.A., Samuel, R.D.J. and Niranjanamurthy, M. eds., 2022. Privacy and security challenges in cloud computing: A holistic approach. CRC Press

16	Final Exam and Capstone Project	Face to Face	

*** Learning styles: Lecture, flipped learning, learning through projects, learning through problem solving, participatory learning ... etc.**

**** Reference: Pages in a book, database, recorded lecture, content on the e-learning platform, video, website ... etc.**

Schedule of asynchronous interactive activities (in the case of e-learning and blended learning)

Week	Task / activity	Reference	Expected results
1	Exploring Google Cloud Console and Core Services.	Google Cloud Documentation, *Getting Started with Google Cloud Console* (2024).	tudents will navigate the Cloud Console, identify key services (Compute Engine, Cloud Storage, IAM, Cloud Run), and understand regional vs zonal resources.
2	Hands-on Lab: Creating a Secure Virtual Machine in Compute Engine.	Google Cloud Documentation, *Getting Started with Google Cloud Console* (2024).	Students will create a VM with minimal permissions, apply SSH key management, and enable VPC firewall rules for controlled network access.
3	Configuring IAM Roles and Policies for Least Privilege.	Google Cloud Documentation, *Identity and Access Management (IAM)* (2024).	Students will assign roles, test role bindings, and verify access control using the Policy Troubleshooter to ensure principle of least privilege.
4	Encrypting Data in Transit and at Rest using Cloud KMS.	Google Cloud Documentation, *Identity and Access Management (IAM)* (2024).	Students will create CMEK keys, encrypt/decrypt sample files, and demonstrate how CMEK protects data residency and regulatory compliance.
5	Building a Secure Container Image and Deploying to Cloud Run.	Google Cloud Documentation, *Cloud Run Security Best Practices* (2024).	Students will develop a containerized application, scan for vulnerabilities with Container Analysis, and deploy it privately using IAM-based invocation.
6	Configuring VPC Networks and Subnets with Firewall Policies.	Google Cloud Documentation, *Virtual Private Cloud (VPC)* (2024).	Students will create custom VPC networks and subnets, apply egress and ingress rules, and test connectivity between secure zones.,
7	Implementing Binary Authorization for Container Deployment.	Google Cloud Documentation, *Binary Authorization for GKE and Cloud Run* (2024).	Students will configure policy attestors to enforce deployment of signed container images and observe policy violations handling.
8	Monitoring Cloud Resources with Cloud	Google Cloud	Students will create log-

	Monitoring and Logging.	Documentation, *Operations Suite (Cloud Monitoring & Logging)* (2024).	based metrics, set alert policies, and analyze events to detect security anomalies in real time.
9	Case Study: Incident Response using Security Command Center (SCC).	Google Cloud Documentation, *Security Command Center Overview* (2024).	Students will simulate a misconfiguration event, review findings in SCC, and document an incident response report including remediation steps.
10	Capstone Exercise: Designing a Zero-Trust Architecture on Google Cloud.	Google Cloud Documentation, *Zero Trust and BeyondCorp Enterprise Model* (2024).	Students will design an integrated cloud security architecture incorporating IAM, VPC-SC, KMS, Cloud Armor, and SCC to illustrate defense-in-depth and compliance controls.