Course Acronym:	CIS
Course Number:	156
Descriptive Title:	Security with AWS
Division:	Business
Department:	Computer Information Systems
Course Disciplines:	Computer Information Systems
Catalog Description:	This course focuses on security as it applies to cloud technologies. Students will learn the general security concept of confidentiality, integrity, and availability of computing resources and will use Amazon Web Services (AWS) to explore how security is implemented in a cloud infrastructure. Specific AWS topics include the AWS Shared Responsibility model and how to use AWS security and monitoring tools to analyze hardware, services, and networks. User activity, key management services, various firewalls, and the planning and configuration of private and public subnets will also be covered.
Prerequisite:	CIS 150 with a minimum grade of C or equivalent experience
Co-requisite:	
Recommended Preparation:	Computer Information Systems 152 OR Computer Information Systems 154 OR Computer Information Systems 119
Enrollment Limitation:	
Hours Lecture (per week):	2
Hours Laboratory (per week):	3
Outside Study Hours:	4
Total Course Hours:	90
Course Units:	3
Grading Method:	Letter Grade only
Credit Status:	Credit, degree applicable
Transfer CSU:	Yes
Effective Date:	Proposed
Transfer UC:	No
Effective Date:	
General Education: ECC	
Term:	

Other:	
CSU GE:	
Term:	
Other:	
IGETC:	
Term:	
Other:	
Student Learning Outcomes:	**SLO #1 AWS App Security Requirements** Students will identify important security principles that AWS applications must meet when deployed. **SLO #2 AWS Global Infrastructure and Shared Responsibility** Students will understand the AWS Global Infrastructure Security and the Shared Responsibility Model. **SLO #3 AWS Public and Private Subnets** Students understand how to implement private and public subnets for an AWS infrastructure. **SLO #4 AWS Firewall** Students will understand how to implement a firewall to protect AWS assets.
Course Objectives:	1. Analyze and describe the AWS Global Infrastructure and the AWS Shared Responsibility Model. 2. Evaluate best practices for AWS applications. 3. Utilize AWS tools to create private and public subnets. 4. Utilize AWS tools to monitor various AWS resources. 5. Manage Users, groups, roles, resources, and access. 6. Configure firewalls in AWS for applications and instances. 7. Set up logging for security event using AWS tools. 8. Review security configuration using AWS tools.
Major Topics:	**I. Introduction to AWS Global Infrastructure Security (3 hours, lecture)** A. AWS Global Infrastructure Security B. AWS Shared Responsibility Model **II. Application Security Concepts (9 hours, lecture)** A. Principles of the security triad of Confidentiality, Integrity and Availability B. Application security best practices C. Security access control management of users, groups, roles, and other resources **III. Subnets (9 hours, lecture)** A. AWS Virtual Private Subnets B. Public and private subnets in AWS **IV. AWS Monitoring Tools (6 hours, lecture)** A. AWS Tools for monitoring instance activity

	B. AWS Tools for monitoring user activity C. AWS Tools for monitoring network activity **V. Other AWS Security Tools (3 hours, lecture)** A. Security event logging B. Security configurations **VI. AWS Firewall Configuration (6 hours, lecture)** A. AWS firewall configuration for applications B. AWS firewall configuration for instances **VII. Introduction to AWS Global Infrastructure Security (3 hours, lab)** A. AWS Global Infrastructure Security B. AWS Shared Responsibility Model **VIII. Application Security Concepts (15 hours, lab)** A. Principles of the security triad of Confidentiality, Integrity and Availability B. Application security best practices C. Security access control and management of users, groups, roles, and other resources **IX. Subnets (12 hours, lab)** A. AWS Virtual Private Subnets B. Public and private subnets in AWS **X. AWS Monitoring Tools (9 hours, lab)** A. AWS Tools for monitoring instance activity B. AWS Tools for monitoring user activity C. AWS Tools for monitoring network activity **XI. Other AWS Security Tools (6 hours, lab)** A. Security event logging in AWS B. Security configurations **XII. AWS Firewall Configuration (9 hours, lab)** A. AWS firewall configuration for applications B. AWS firewall configuration for instances
Total Lecture Hours:	36
Total Laboratory Hours:	54
Total Hours:	90
Primary Method of Evaluation:	2) Problem solving demonstrations (computational or non-computational)
Typical Assignment Using Primary Method of Evaluation:	Using the Amazon Web Services console, track user session handling in order to complete various auditing tasks. After your task, write a one-page report describing what an organization might be looking for in a user session audit and why this is important.
Critical Thinking Assignment 1:	A business that formerly self-hosted their IT infrastructure and business application has recently migrated to the AWS Cloud Infrastructure. They are worried that during their migration, their security isn't set up properly and are afraid that unauthorized users may be able to access private parts of the cloud. You are tasked with reviewing their

	infrastructure plan and their security access plan. Write a two- to three-page report detailing the considerations you would undertake to ensure proper access control and exposure to their business.
Critical Thinking Assignment 2:	Set up two separate EC2 instance in AWS, both using an Amazon Machine Image (AMI). One instance will be running an AWS Aurora Database server and the other will be running a simple PHP server. Set up a firewall to limit the Aurora database server to only allow connections from the web server (and ssh). How would you test that your firewall is working?
Other Evaluation Methods:	Homework Problems, Laboratory Reports, Objective Exam, Quizzes, Written Homework
Instructional Methods:	Demonstration, Discussion, Group Activities, Lab, Lecture, Multimedia presentations
If other:	
Work Outside of Class:	Answer questions, Problem solving activity, Required reading, Skill practice, Written work (such as essay/composition/report/analysis/research)
If Other:	
Up-To-Date Representative Textbooks:	Anthony A., Mastering AWS Security: Create and Maintain a Secure Cloud Ecosystem, Packt Publishing, 2017. Vora, Z., Enteprise Cloud Security and Governance, Packt Publishing, 2017.
Alternative Textbooks:	
Required Supplementary Readings:	
Other Required Materials:	
Requisite:	Prerequisite
Category:	sequential
Requisite course(s): List both prerequisites and corequisites in this box.	CIS 150 with a minimum grade of C
Requisite and Matching skill(s):Bold the requisite skill. List the corresponding course objective under each skill(s).	**This course requires an understanding of computer information systems and cloud computing concepts. Students should be able to create cloud applications in AWS.** CIS 150 - Describe the Cloud Computing Model; Create a cloud application utilizing AWS Computing Services (EC2).
Requisite Skill:	Equivalent experience
Requisite Skill and Matching Skill(s): Bold the requisite skill(s). If applicable	Demonstrate an understanding of the development and use of information systems in business.
Requisite course:	Computer Information Systems 152 OR Computer Information Systems 154 OR Computer Information Systems 119

Requisite and Matching skill(s):Bold the requisite skill. List the corresponding course objective under each skill(s).	**Students should be able to design and manage databases in AWS.** CIS 152 - Design databases using AWS database services. **Students should be able to create an application using the AWS serverless compute model.** CIS 154 - Understand and configure serverless web applications. **Students should be able to identify software and hardware technologies needed to defend against intrusions from adversaries, malicious actors and malware.** CIS 119 - Identify software and hardware technologies needed to defend against intrusions from adversaries, malicious actors and malware.
Requisite Skill:	
Requisite Skill and Matching skill(s): Bold the requisite skill. List the corresponding course objective under each skill(s). If applicable	
Enrollment Limitations and Category:	
Enrollment Limitations Impact:	
Course Created by:	Khai Lu
Date:	10/16/2018
Original Board Approval Date:	
Last Reviewed and/or Revised by:	
Date:	
Last Board Approval Date:	12/19/2022