Metropolitan State University of Denver
Regular Course Syllabus

CSS - 2751 - Principles of Cybersecurity Fall 2016

Status	completed
Tracking:	LAS1617-26
Department	Mathematical and Computer Sciences, Department of
Prefix:	CSS
Course Number:	2751
Course Type:	Computer Science Studies
Course Title:	Principles of Cybersecurity
Transcript Course Title:	Principles of Cybersecurity
Equivalent/ Crosslisted?	
List all equivalent courses:	
List all crosslisted courses:	
Check All That Apply:	Elective
Credit Hours:	3
Schedule Type:	Lecture
Grade Mode:	Letter
Lecture:	45
Lab:	
Internship:	
Practicum:	
Other:	
Additional Student Work Hours per course:	90
Variable topics umbrella course:	No
If yes, number of credits/ repeats allowed	
Specified repeatable course:	No
If yes, number of credits/ repeats allowed	
Prerequisite(s):	CIS/CSS 1010 with a grade of "C" or better; or appropriate score on the computer literacy screening test.
Corequisite(s):	
Prerequisite(s) and/or Corequisite(s):	
Banner Prerequisite(s):	
Banner Corequisite(s):	
Banner Prerequisite(s) and/or Corequisite(s):	
Level	
Class	
Program/Major	

Student attribute	
Catalog Course Description:	This course provides a broad overview of cybersecurity. The terminology, approaches, and underlying technologies used in cybersecurity are covered. How computers and networks are attacked, how the attackers benefit, and how to mitigate attacks are addressed. Social engineering, cryptography, and application security are introduced.
Required Reading and Other Materials will be equivalent to:	John R. Vacca (2013), Computer and Information Security Handbook, Second Edition, ISBN-13: 978-0123943972
Specific, Measurable Student Behavioral Learning Objectives:	1. Assess threat models and their influence on a particular organization. 2. Compare the various uses and approaches to cryptography. 3. Prepare for and respond to secuirty incidences. 4. Design effective and efficient password schemes. 5. Plan environments that are resistant to malware. 6. Choose an effective set of training experiences for an organization. 7. Prepare a plan to defend from the usual attacks on networks and hosts.
Detailed Outline of Course Content (Major Topics and Subtopics) or Outline of Field Experience/ Internship	1. Dimensions of computer security. 1. Confidentiality. 2. Integrity. 3. Availability. 2. Models of computer security. 3. Essentials of cryptography. 1. Public key encryption. 2. Private-key encryption. 3. Secure hashing and message authentication. 4. Digital signatures. 4. Types of malicious software. 5. Authentication and authorization. 6. Levels of trust and authorization. 7. Secure programming. 8. Operating system security overview. 9. Network and database security overview. 10. Securing the human.
Evaluation of Student Performance	Required: a midterm and final exam and four papers. Optional: quizzes. participation, classwork, homework, projects.
Learning Objectives	
Distribution of Credit Hours	3 (3+0)

Steps	**Decision**	**Date**	
Originator			
Steve Beaty	approve	09/12/2016 10:07AM	
Department Curriculum Committee Chair			
Clark Dollard	approve	09/12/2016 02:56PM	
Department Chair			
Lindsay Packer	approve	09/12/2016 03:28PM	
Dean's Office Tracking Assignment			
Cynthia Philbrook	approve	09/14/2016 08:36AM	
Substantive College Level			
Linda Lang-Peralta	approve	12/19/2016 05:00PM	

Mona Mocanasu	approve	12/14/2016 10:50AM	
Steve Beaty	approve	12/11/2016 04:03PM	
Faculty Senate President			
Matthew Makley	None		
Erica Buckland	force-approve	01/05/2017 10:57AM	
AVP Academic and Student Affairs			
Bernice Harris	approve	01/13/2017 04:42PM	