



UNIVERSITY
of VIRGINIA

SCHOOL OF CONTINUING
AND PROFESSIONAL STUDIES

Northern Virginia Center

Course Number and Title:

BUS 5020 Cyber Security Policy Development and Assessment

Instructor:

Instructor Name: Dr. George Kostopoulos

Contact Information: gkk5f@virginia.edu and (210) 401-7130 AM hours

Semester, Dates, Location, Time:

Spring 2015 – March 17 to April 20 – Online web based

Required Textbook:

Cyber Security Policy Guidebook

By Bayuk, Jennifer et al

Wiley: ISBN 978-1-118-02780-6

Optional Reference Material:

Cyberspace and Cybersecurity

By Kostopoulos, George

CRC Press: ISBN 978-1-4665-0133-1

Course Description

BUS 5020 Cyber Security Policy Development and Assessment

Effective security managers must understand how to develop security policies that will be supported by executive management and adopted by all employees. This course examines the steps required in policy development including password protection, acceptable use of organization information technology assets, risk acceptance, identification of internal and external threats, countermeasures, intellectual property, proprietary information and privacy issues, compliance reporting, and escalation procedures. Related topics such as access controls, security standards, and policy implementation are covered.

In the IT Security Policy and Assessment course we will examine the detailed steps that are required in developing cyber security policies, risk assessments, identification of internal and external threats, legal and privacy issues, reports, policy documents and other closely related documents. In support of these documents we will also explore the technology involved in creating firewall access controls, well developed social engineering security controls, and stake holder policy implementation and enforcement. Security Policy development and technology implementation will be covered in depth. Students are required to attend weekly virtual classes to submit discussion posts, reading assignment case studies, media content review and exams.

Course Delivery

This course will be conducted by the use of posted online discussions, class assignments, and exams through the use of the internet using UVaCollab. This course will introduce and study IT Security disciplines within the Open Access Environment Arena. Some of the case studies will serve to survey the subject matter that will be covered in greater depth throughout the Cyber Security Management Certificate program. A number of the case studies will also survey areas in other cyber security management topics. ***Students are required to login and complete an online class discussion post every week.***

Course Objectives / Outcome:

On successful completion, the student will be able to:

Demonstrate an understanding in writing cyber security policy documents and how to mitigate security risks appropriately.

1. Understand the cybersecurity threat landscape as it pertains to both U.S. government and private industry
2. Identify and document the various types of cyber attacks that threaten both U.S. government and private industry information technology enterprises
3. Assess options for mitigating risks after a cyber attack has occurred.
4. Write cyber security policy documents that demonstrate an understanding of how to mitigate security risks appropriately
5. Develop an appreciation for the importance of policy implementation and enforcement

Preparation & Student Expectations

Reading Assignments: Students are expected to read all assigned readings topics before class in where the topics will be discussed in-depth. The instructor will also provide additional materials during class sessions, as needed. As a preliminary preparation for this course, it is necessary that the students effectively review the materials and complete the assignments demonstrating their newly learned techniques.

Course Policy:

All work must be typed and double-spaced.

Work is due as scheduled. Failure to meet deadlines will result in a reduced grade.

Students should be prepared to spend several hours per week on research assignments and posting discussions on UVaCollab. Before each case study posting, each student should study the case studies and how it relates to the lessons in the text and the designated reading materials assigned by the instructor. Each student is expected to participate in posted online class discussions and exercises.

The Academic Honor System

The University of Virginia academic honor system embodies many of Mr. Jefferson's principles. The purpose of the Honor System is to sustain and protect a community of trust in which students can enjoy the freedom to develop their intellectual and personal potential. The concept of an honor system implies that students commit themselves to the pursuit of truth. At the Division of the Continuing Education, course is conducted in the spirit of the Honor System. The instructor will indicate with assignments and activities are to be done individually or which permit collaboration. The following pledge should be written out at the end of all quizzes examinations, individual assignments and papers:

“I pledge that I have neither given nor received help on this examination (quiz, assignment, etc)”. The student should sign the pledge. If you have questions about the Honor System, you may contact the Honor Committee in Charlottesville, VA at 804-924-3452

Evaluation and Grading Criteria:

Student grades will be determined by class participation and course assignments.
 The final grade will be based on the following course components.
 The class will comprise teams that will have team assignments.

	Assignments	Grade	Due Day/Date
Team Activities	Discussions Summary in PPT	6%	During following week.
	Project One: Cybersecurity Framework & Stakeholders	11%	03/23/15
	Project Two: Cybersecurity Compliance and the Law	11%	03/30/15
Individual Activities	Project Three: Cybersecurity Policy Development	11%	04/06/15
	Project Four: Cybersecurity Policy Metrics & Assessment	11%	04/13/15
	Project Five: Corporate Cybersecurity Policy	25%	04/22/15
	Five weekly Participation in five weekly discussions.	25%	During assigned week
	Total:	100%	

Grading Scale

A	95-100	B+	86-89	C+	75-78	F	67 and below
A-	90-94	B	82-85	C	71-74		
		B-	79-81	C-	68-70		

The BUS5020 detailed Course Plan is available in a separate document.