IS411T
Security Policies and Implementation Issues
[Onsite]

Course Description:

The course includes a discussion on security policies that can be used to help protect and maintain a network, such as password policy, e-mail policy and Internet policy. The issues include organizational behavior and crisis management.

Prerequisite(s) and/or Corequisite(s):

Prerequisites: IS305T Managing Risk in Information Systems or equivalent

Credit hours: 4

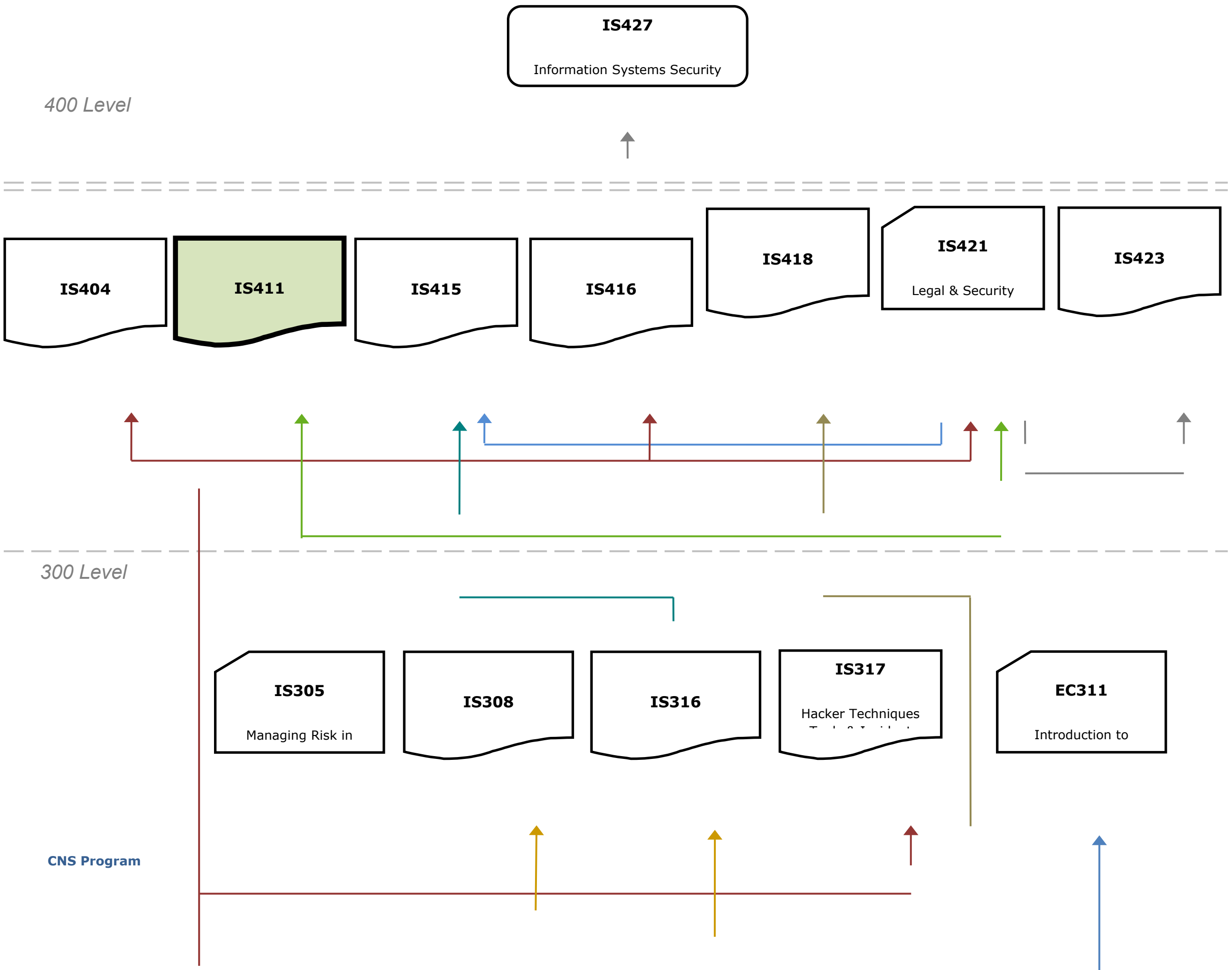
Contact hours: 60 (36 Theory Hours, 24 Lab Hours)

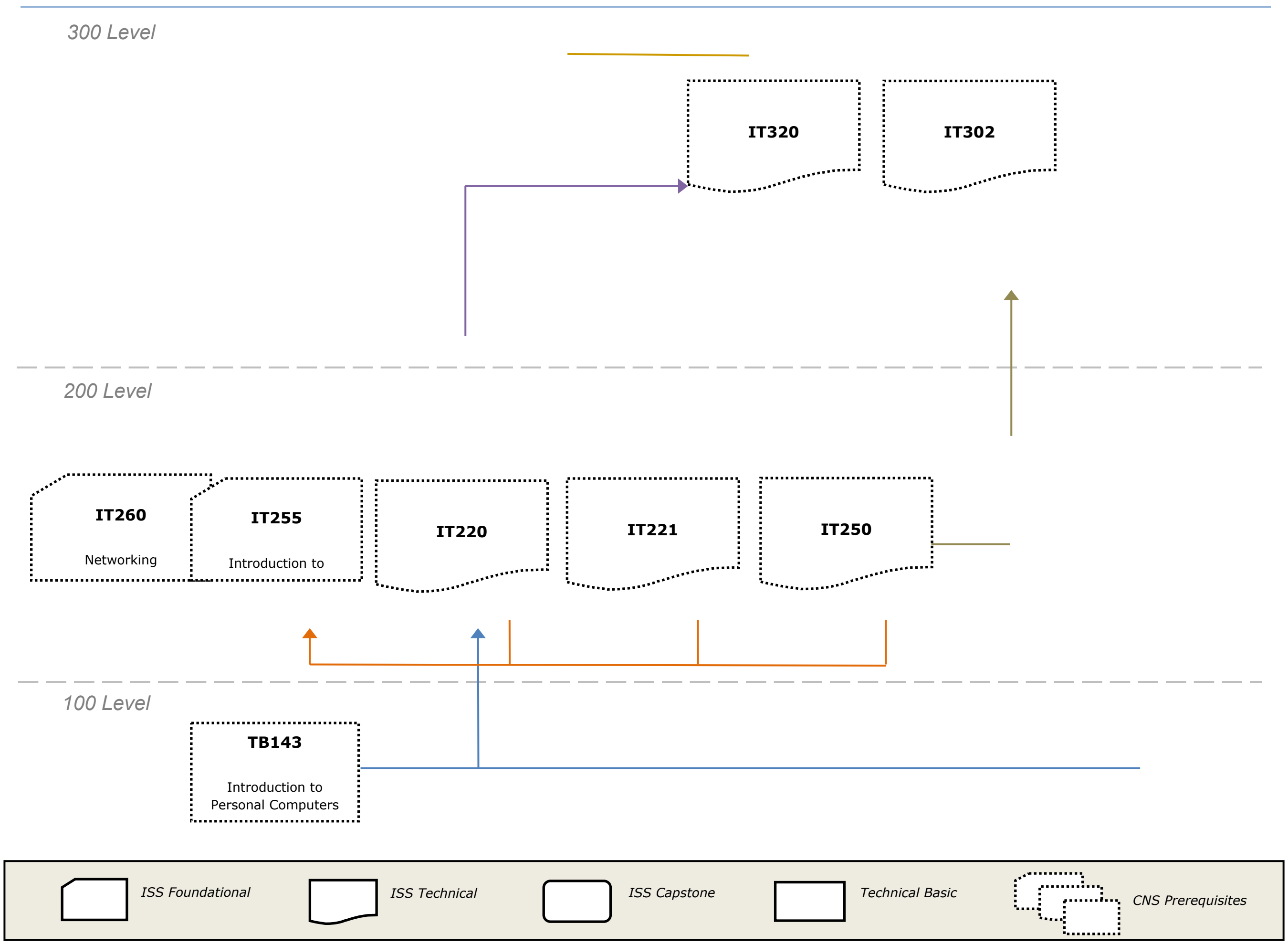
Where Does This Course Belong?

This course is required for the Bachelor of Science in Information Systems Security program. This program covers the following core areas:

- Foundational Courses
- Technical Courses
- BSISS Project

The following diagram demonstrates how this course fits in the program:




300 Level
IT320
IT302
200 Level
IT260
Networking
IT255
Introduction to
IT220
IT221
IT250
100 Level
TB143
Introduction to
Personal Computers
ISS Foundational
ISS Technical
ISS Capstone
Technical Basic
CNS Prerequisites

Course Summary

Course Description

The course includes a discussion on security policies that can be used to help protect and maintain a network, such as password policy, e-mail policy and Internet policy. The issues include organizational behavior and crisis management.

Major Instructional Areas

1. Security policy requirements
2. Security policy framework
3. Creation of security policies
4. Implementation issues
5. Security policy controls

Course Objectives

1. Identify the role of an information systems security (ISS) policy framework in overcoming business challenges.
2. Analyze how security policies help mitigate risks and support business processes in various domains in the information technology (IT) infrastructure.
3. Describe the components and basic requirements for creating a security policy framework.
4. Describe the different methods, roles, responsibilities, and accountabilities of personnel, along with the governance and compliance of security policy framework.
5. Describe the different ISS policies associated with the user domain.
6. Describe the different ISS policies associated with the IT infrastructure.
7. Describe the different ISS policies associated with risk management.

8. Describe the different ISS policies associated with incident response teams (IRT).

9. Describe different issues related to implementing and enforcing ISS policies.

10. Describe the different issues related to defining, tracking, monitoring, reporting, automating, and configuration of compliance systems and emerging technologies.

SCANS Objectives

SCANS is an acronym for Secretary's Commission on Achieving Necessary Skills. The committee, appointed by the National Secretary of Labor in 1990, created a list of skills and competencies that continue to be a valuable resource for individuals developing their careers in a high-tech job market. For more information on the SCANS objectives, visit The U.S. Department of Labor Employment and Training Administration: www.doleta.gov.

Learning Materials and References

Required Resources

Textbook Package	New to this Course	Carried over from Previous Course(s)	Required for Subsequent Course(s)
Johnson, Rob, and Merkow. *Security Policies and Implementation Issues.* 1st ed. Sudbury, MA: Jones & Bartlett, 2011.	▪		
Printed IS411 Student Lab Manual	▪		
ISS Mock IT Infrastructure (1) – Cisco Core Backbone Network consisting of Cisco 2811 routers, 2950/2960 catalyst switches, ASA 5505s for classroom hands-on labs that require a live, IP network. (For onsite only)	▪	▪	▪
ISS Mock IT Infrastructure (2) – VM Server Farm (2 Microsoft Windows Servers and 2 Ubuntu Linux Servers) for classroom hands-on VM labs. (For both onsite and online)	▪	▪	▪
ISS Mock IT Infrastructure (2) – VM Workstation (Microsoft Windows XP Professional Workstation with Core ISS Apps and Tools) for classroom hands-on VM labs. (For both onsite and online)	▪	▪	▪

Recommended Resources

Books, Professional Journals

Please use the following author's names, book/article titles and/or keywords to search in the ITT Tech Virtual Library for supplementary information to augment your learning in this subject:

Books

Periodicals

EbscoHost

Books24X7

Sandy BacikBuilding an Effective Information Security Policy Architecture (Chapter 1 & 7)

Seymour Bosworth, et al

Security Handbook, 5th ed. (Chapters 3, 21 and 26)

Debra S. Herrmann

Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI (Chapters 3, 4 and 5)

Ronald L. Krutz, et al

The CISM Prep Guide: Mastering the Five Domains of Information Security Management (Chapters 2, 5 and Appendix B)

Harold F. Tipton, et al

Information Security Management Handbook, 6th ed. (Chapters 2, 5, 7, 14, 16, 41 and 42)

John R. Vacca

Computer and Information Security Handbook (Chapter 15)

Jeffrey L. Ott

“Information security in the new millennium”, Information Systems Security, Mar/Apr2000, Vol. 9 Issue 1, (AN 2881038)

Kenneth A. Bamberger

Texas Law Review, Mar2010, Vol. 88 Issue 4, “Technologies of Compliance: Risk and Regulation in a Digital Age” (Pages 669-739), (AN 48969651)

A. S. Vydrin

“Theoretical aspects of information security”, Journal of Mathematical Sciences, Jan2009, Vol. 156 Issue 2, (Pages 261-275), (AN 36034907)

Keywords:

Policies

Regulations

Laws

Standards

Information systems security

Information assurance

Four information security controls

U.S. compliancy laws and industry standards

Risk management

Risk mitigation

Policy management and maintenance

Responsibilities of and accountability

Users

Privileged users

Local Area Network (LAN)

Wide Area Network (WAN)

Telecommunications

Acceptable use policy (AUP)

Business impact analysis (BIA)

Business continuity planning (BCP)

Disaster recovery planning (DRP)

Incident response

Course Plan

Instructional Methods

This course is designed to promote learner-centered activities and support the development of cognitive strategies and competencies necessary for effective task performance and critical problem solving. The course utilizes individual and group learning activities, performance-driven assignments, problem-based cases, projects, and discussions. These methods focus on building engaging learning experiences conducive to development of critical knowledge and skills that can be effectively applied in professional contexts.

Suggested Learning Approach

In this course, you will be studying individually and within a group of your peers. As you work on the course deliverables, you are encouraged to share ideas with your peers and instructor, work collaboratively on projects and team assignments, raise critical questions, and provide constructive feedback.

Use the following advice to receive maximum learning benefits from your participation in this course:

DO	DON'T
▪ Do take a proactive learning approach ▪ Do share your thoughts on critical issues and potential problem solutions ▪ Do plan your course work in advance ▪ Do explore a variety of learning resources in addition to the textbook ▪ Do offer relevant examples from your experience ▪ Do make an effort to understand different points of view ▪ Do connect concepts explored in this course to real-life professional situations and your own experiences	▪ Don't assume there is only one correct answer to a question ▪ Don't be afraid to share your perspective on the issues analyzed in the course ▪ Don't be negative towards the points of view that are different from yours ▪ Don't underestimate the impact of collaboration on your learning ▪ Don't limit your course experience to reading the textbook ▪ Don't postpone your work on the course deliverables – work on small assignment components every day

Course Outline

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
1	Information Security Policy Management	*Security Policies and Implementation Issues:* ▪ Chapter 1 ▪ Chapter 2 ▪ Chapter 3	Discussion	1.1	Importance of Security Policies	1
			Lab	1.2	Craft an Organization-Wide Security Management Policy for Acceptable Use	2
			Assignment	1.3	Security Policies Overcoming Business Challenges	2
2	Risk Mitigation and Business Support Processes	*Security Policies and Implementation Issues:* ▪ Chapter 4 ▪ Chapter 5	Discussion	2.1	Risk Mitigation	1
			Lab	2.2	Develop an Organization-Wide Policy Framework Implementation Plan	2
			Assignment	2.3	Good Policy Implementation	2
3	Policies, Standards, Procedures, and Guidelines	*Security Policies and Implementation Issues:* ▪ Chapter 6 ▪ Chapter 7	Discussion	3.1	Business Considerations	1
			Lab	3.2	Define an Information Systems Security Policy Framework for an IT Infrastructure	2
			Assignment	3.3	Security Policy Frameworks	2
4	Information Systems Security Policy Framework	*Security Policies and Implementation Issues:* ▪ Chapter 8	Discussion	4.1	Separation of Duties (SOD)	1
			Lab	4.2	Craft a Layered Security Management Policy - Separation of	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
						Grade Allocation
			Grading Category	#	Activity Title	(% of all graded work)
					Duties	
			Assignment	4.3	Security Policy Creation	2
5	User Policies	*Security Policies and Implementation Issues:* ▪ Chapter 9	Discussion	5.1	Best Practices for User Policies	1
			Lab	5.2	Craft an Organization-Wide Security Awareness Policy	2
			Assignment	5.3	Create User Policy	2
6	IT Infrastructure Security Policies	*Security Policies and Implementation Issues:* ▪ Chapter 10	Discussion	6.1	IT Infrastructure Security Policies	1
			Lab	6.2	Define a Remote Access Policy to Support Remote Healthcare Clinics	2
			Assignment	6.3	IT Infrastructure Policies	2
7	Risk Management	*Security Policies and Implementation Issues:* ▪ Chapter 11	Discussion	7.1	Business Impact Analysis (BIA), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP)	1
			Lab	7.2	Identify Necessary Policies for Business Continuity - BIA & Recovery Time Objectives	2
			Assignment	7.3	Risk Management in a Business Model	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
						Grade Allocation
			Grading Category	#	Activity Title	(% of all graded work)
8	Incident Response Team Policies	*Security Policies and Implementation Issues:* ▪ Chapter 12	Discussion	8.1	Support Services	1
			Lab	8.2	Craft a Security or Computer Incident Response Policy – CIRT Response Team	2
			Assignment	8.3	Create an Incident Response Policy	2
9	Implementing and Maintaining an IT Security Policy Framework	*Security Policies and Implementation Issues:* ▪ Chapter 13 ▪ Chapter 14	Discussion	9.1	Information Dissemination—How to Educate Employees	1
			Lab	9.2	Assess and Audit an Existing IT Security Policy Framework Definition	2
			Assignment	9.3	Policy Monitoring and Enforcement Strategy	2
10	Automated Policy Compliance Systems	*Security Policies and Implementation Issues:* ▪ Chapter 15	Discussion	10.1	Tracking, Monitoring, and Reporting	1
			Lab	10.2	Align an IT Security Policy Framework to the 7Domains of a Typical IT Infrastructure	2
			Assignment	10.3	Automated Policy Compliance Systems	2
11	Course Review and Final Examination	N/A	Project	11.1	Department of Defense (DoD) Ready	25
			Exam	11.2	Final Exam	25

Evaluation and Grading

Evaluation Criteria

The graded assignments will be evaluated using the following weighted categories:

Category	Weight
Discussion	10
Lab	20
Assignment	20
Project	25
Exam	25
TOTAL	**100%**

Grade Conversion

The final grades will be calculated from the percentages earned in the course, as follows:

Grade	Percentage	Credit
A	90–100%	4.0
B+	85–89%	3.5
B	80–84%	3.0
C+	75–79%	2.5
C	70–74%	2.0
D+	65–69%	1.5
D	60–64%	1.0

F	<60%	0.0

Academic Integrity

All students must comply with the policies that regulate all forms of academic dishonesty, or academic misconduct, including plagiarism, self-plagiarism, fabrication, deception, cheating, and sabotage. For more information on the academic honesty policies, refer to the Student Handbook.

(End of Syllabus)