CENTRAL UNIVERSITY OF TECHNOLOGY, FREE STATE
SENTRALE UNIVERSITEIT VIR TEGNOLOGIE, VRYSTAAT
YUNIVESITHI E BOHARENG YA THEKENOLOJI, FOREISTATA

School for Information Technology

INSTRUCTIONAL OFFERING : **COMPUTER SECURITY**
: **060703306 CSY41AB**

INSTRUCTIONAL PROGRAM : **B.TECH. INFORMATION TECHNOLOGY**
3306017 - BCBTIP

EXAMINATION : **3 HOURS**

-SYLLABUS-

1. Data security
2. Internet security
3. PC security

-EXTENDED SYLLABUS-

UNIT	SPECIFIC OUTCOME	ASSESSMENT CRITERIA	CREDITS	NOTIONAL HOURS	WEEKS
1	Demonstrate an understanding of the history of computer security.	Define and describe the definition of information security. Effectively comprehend the history of computer security and how it evolved into information security. Define and describe the key terms and critical concepts of information security as presented in the chapter. Effectively outline the phases of the security systems development life cycle Define and describe the role professionals involved in information security within an organization.	0.5	5	0.5

2	Demonstrate an understanding of the need for security	Effective understand the business need for information security. Effectively understand a successful information security program is the responsibility of an organization's general management and IT management. Identify the threats posed to information security and the more common attacks associated with those threats. Differentiate threats to information systems from attacks against information systems.	0.5	5	0.5
3	Demonstrate an understanding of legal, ethical and professional issues in Information Security	Effectively differentiate between laws and ethics. Identify major national laws that relate to the practice of information security. Understand the role of culture as it applies to ethics in information security.	1	10	1
4	Demonstrate an understanding of risk management	Define and describe risk management, risk identification and risk control Effectively understand how risk is identified and assessed Effectively assess risk based on probability of occurrence and impact on an organization Effectively grasp the fundamental aspects of documenting risk through the creation of a risk assessment Describe the risk mitigation strategy options for controlling risks Identify the categories that can be used to classify controls Recognize the conceptual frameworks that exist for evaluating risk controls and be able to formulate a cost benefit analysis Understand how to maintain and perpetuate risk controls	2	20	2
5	Demonstrate an understanding of planning for security	Define and describe management's role in the development, maintenance and enforcement of information security policy, standards, practices, procedures and guidelines Effectively understand what an information security blueprint is, what its major components are, and how it is used to support the information security program Understand how an organization institutionalizes its policies, standards, and practices using education, training, and awareness programs Explain what contingency planning is and how incident response planning, disaster recovery planning, and business continuity plans are related to contingency planning	2	20	2

6	Demonstrate an understanding of Security Technology in terms of firewalls and VPNs	Effectively understand the role of physical design in the implementation of a comprehensive security program Understand firewall technology and the various approaches to firewall implementation Effectively identify the various approaches to remote and dial-up access protection – that is, how these connection methods can be controlled to assure confidentially of information, and the authentication and authorization of users Understand content filtering technology Describe the technology that enables the use of Virtual Private Networks	2	20	2
7	Demonstrate an understanding of intrusion detection, access control, and other security tools	Identify and describe the categories and operating models of intrusion detection systems Identify and describe honey pots, honey nests and padded cell systems List and define the major categories of scanning and analysis tools, and describe the specific tools used within each of these categories Discuss various approaches to access control, including the use of biometric access mechanisms	1	10	2
8	Demonstrate an understanding of cryptography	Describe the most significant events and discoveries from the history of cryptology Understand the basic principles of cryptography Understand the operating principles of the most popular tools in the area of cryptography List and explain the major protocols used for secure communications Effectively Understand the nature and execution of the dominant methods of attack used against cryptosystems	1	10	1

9	Demonstrate an understanding of physical security	Effectively understand the conceptual need for physical security. Identify threats to information security that are unique to physical security. Describe the key physical security considerations for selecting a facility site. Identify physical security monitoring components. Recognize the essential elements of access control within the scope of facilities management. Understand the importance of fire safety programs to all physical security programs. Describe the components of fire detection and response. Understand the impact of service interruptions of supporting utilities. Understand the technical details of uninterruptible power supplies and how they are used to increase availability of information assets. Discuss critical physical environment considerations for computing facilities. Discuss countermeasures to the physical theft of computing devices.	0.5	5	1
10	Demonstrate an understanding of implementing Information Security	Effectively understand how the organization's security blueprint becomes a project plan. Understand the numerous organizational considerations that must be addressed by a project plan. Appreciate the significance of the project manager's role in the success of an information security project. Understand the need for professional project management for complex projects. Effectively follow technical strategies and models for implementing the project plan. Identify the non-technical problems that organizations face in times of rapid change.	0.5	5	1
11	Demonstrate an understanding of security and personnel	Effectively understand where and how the information security function is positioned within organizations Understand the issues and concerns about staffing the information security function Identify the credentials that professionals in the information security field may acquire to gain recognition in the field. Appreciate how an organization's employment policies and practices can support the information security effort Understand the special security precautions that must be taken when contracting non-employees Recognize the need for the separation of duties Understand the special requirements needed for the privacy of personnel data	0.5	5	1

12	Demonstrate an understanding of Information Security maintenance	Effectively understand why maintenance of the information security program is needed on an ongoing basis. Effectively recognize recommended security management models. Define a model for a full maintenance program. Identify the key factors involved in monitoring the external and internal environment. Understand how planning and risk assessment tie into information security maintenance. Understand how vulnerability assessment and remediation tie into information security maintenance. Understand how to build readiness and review procedures into information security maintenance.	0.5	5	1