POSTGRADUATE DIPLOMA IN INFORMATION TECHNOLOGY SECURITY

1. INTRODUCTION

The Postgraduate Diploma in Information Technology Security (ITS) is a professional program that follows the project method of teaching which is designed to enable students to learn how to stay current and be abreast with the rapidly-evolving IT security field and cyber-crime activities. The project method provides students with the experience to apply core course materials to a substantial project in the workplace. Today network attacks, data breaches and advanced intrusions are occurring daily. Sensitive and confidential data and intellectual property are stolen from systems that are protected by sophisticated network and host based security. A motivated criminal group or nation state can and will always find a way inside enterprise networks. In the commercial, non-governmental and government sectors, hundreds of victims responded to serious intrusions costing millions of dollars and loss of untold terabytes of data. The latest cyber-attacks dubbed the Advanced Persistent Threat (APT) have proved difficult to suppress and are continuously racking havoc to private networks worldwide. The PGD in ITS seeks to train IT Security specialists to respond to and investigate these incidents and provide rapid countermeasures. It equips students with a firm understanding of advanced incident response and computer forensics tools and techniques to investigate data breach intrusions, tech-savvy rogue employees, advanced persistent threats, and complex digital forensic cases.

2. OBJECTIVES

The overall objective of the course is to train IT security graduates who are skilled, knowledgeable and motivated to manage enterprise network resources security needs. The specific objectives are:

(a) To assess the security needs of computer and network systems,

(b) To recommend safeguard solutions,

(c) To equip students with skills needed to understand the implementation and enforcement of Information System Security Policies and Practices,

(d) To manage the implementation and maintenance of security devices, systems, and procedures including security auditing standards and best practices, and

(e) To motivate students to acquire up-to-date techniques required in identification, analysis, assessment and evaluation of information system threats and vulnerabilities and their impact on an organization’s critical information infrastructures.

3. ADMISSION REQUIREMENTS

To qualify for admission into the Postgraduate Diploma (PGD) applicants shall be:

- Holders of a computer science degree or related field from a recognized University.

4. COURSE STRUCTURE AND DURATION

The Postgraduate Diploma (PGD) program shall normally take 2-semesters

Courses shall be offered in units. A course unit is defined as that part of a semester subject described by coherent syllabus and taught normally over a period of a semester. It is designated as a total of 42 hours of study in a semester. For this purpose, one 1-hour lecture is equivalent 2-hours tutorial or 3-hours practical or any combination as may be approved by the Board of the School of Informatics and Innovative Systems.

Part-time students shall be allowed to take not less than 50% of the courses prescribed for the year.

All course units will be taught for a total of 42 contact hours, including examinations except project work which will take 480 hours of practical work and project writing.

5. EXAMINATIONS REGULATIONS

Jaramogi Oginga Odinga University of Science and Technology Examinations rules and regulation shall apply.

6. COURSE DISTRIBUTION

Students shall choose courses and topics for their projects in consultation with Departmental Postgraduate Faculty Coordinator. All candidates shall be required to normally participate in the seminars arranged by the Department.

YEAR ONE: SEMESTER ONE

Course Code	Course Title	Contact Hours			Weight (Units)
		Lecture	Practical	Total	

IIT 4111	Principles of Computer Security	28	14	42	1C
IIT 4112	Network Security	28	14	42	1C
IIT 4113	Enterprise Systems Management & Security	28	14	42	1C
IIT 4114	Advanced Cryptography and Secure Communications	28	14	42	1C
IIT 4115	IT Security Capstone Research Project	0	42	42	1C
Total		**112**	**98**	**210**	**5**

YEAR ONE: SEMESTER TWO

Course Code	**Course Title**	**Contact Hours**			**Weight (Units)**
		Lecture	**Practical**	**Total**	
IIT 4121	Information Systems Control and Audit	28	14	42	1C
IIT 4122	Computer Digital Forensics	28	14	42	1C
	Electives (Any 3 Electives)*				

ELECTIVES: - Any Three Electives.

Course Code	**Course Title**	**Contact Hours**			**Weight (Units)**
		Lecture	**Practical**	**Total**	
IIT 4123	Legal Issues, Ethics and Incident Response in IT Security	28	14	42	1E
IIT 4124	Computer Security, Risk Management and Control	28	14	42	1E
IIT 4125	Strategic Information Systems Management	28	14	42	1E
IIT4126	Fundamentals of IT Security Law and	28	14	42	1E

	Policy				
IIT 4127	Information Security Policy and Compliance	28	14	42	1E
IIT 4128	Cybercrime Investigations	28	14	42	1E
IIT 4129	Advanced Linux/UNIX System Administration	28	14	42	1E

PROJECT

Course Code	**Course Title**	**Contact Hours**			**Weight (Units)**
		Lecture	**Practical**	**Total**	
IIT 4131	Project	0	84	84	2C

7. COURSE DESCRIPTION

YEAR ONE: SEMESTER ONE

IIT 4111 Principle of Computer Security (42 hrs)

Computer security overview: basics of computer security, including an overview of threat, attack and adversary models; social engineering; essentials of cryptography; traditional computing security models; malicious software; secure programming; operating system security in practice; trusted operating system design; public policy issues, including legal, privacy and ethical issues; network and database security overview.

IIT 4112 Network Security (42 hrs)

Network Security: weaknesses and vulnerabilities in network protocols (TCP/IP, ARP, DNS, ICMP, SMTP, Telnet, FTP, TFTP) and routing protocols. Footprinting and Intelligence gathering introduction to currently available tools. VPNs, Intrusion Detection Systems; Firewalls: Packet-filters, Application-Level, DMZ's. Introduction to Cisco Configmaker; Configuring a firewall. Introduction to Penetration testing. Network attacks; Denial of Service attacks, SQL injection, Cross-site scripting. Legal issues; Regulation of Investigatory Powers Act, Computer Misuse

Act, Police and Criminal Evidence Act. Overview of Digital Signatures and Message Digests, MD5, SHA. Network administration, Access control lists, VLANs. Introduction to network forensics investigations.

IIT 4113 Enterprise Systems Management & Security (42 hrs)

Concepts of enterprise security: Installation, administration and security in Windows and Linux/UNIX. Server hardware, energy management, virtual machines and hypervirtualization. Principles of authentication and access control, Kerberos, MAC, DAC and RBAC. Directory services, LDAP, NIS, Windows Active Directory, permissions, users, groups and roles. TCP, DNS servers, BIND. Web server installation, administration and security, Apache, IIS, proxy servers and web clients. SSL and TLS, creating and installing certificates, RSA, DSA, DES, MD5 and blowfish. Telnet, rsh, SSH and tunnels. FTP server installation, administration and security, SFTP. Database server installation, administration and security with MS SQL Server, MySQL and PostgreSQL. Email, SMTP, MUA, MTA, MSA, MDA, Sendmail, Procmail, Postfix, Exchange, POP, IMAP and Majordomo. System recovery: Backup technology, Storage Area Network (SAN), Network Attached Storage (NAS), Raid, Data Replication.

IIT 4114 Advanced Cryptography and Secure Communications (42 hrs)

Introduction to Number Theory and its application to cryptography; Advances and history of cryptographic techniques employed to secure data over time. Investigation of various encryption algorithms, from simple ciphers to modern public key encryption systems. Discussion of various crypto-algorithms. Algorithm complexity, advanced number theory (Galois fields, quadratic residues, zero knowledge schemes, one-time signatures), efficient implementation of encryption schemes in hardware and software and other advanced topics in cryptography.

IIT 4115 IT Security Capstone Research Project (42 hrs)

This course provides the student the opportunity to put into practice all the skills learned to this point. Emphasis on: security policy, process planning, procedure definition, business continuity, and systems security architecture. Upon completion, students should be able to design and implement comprehensive information security architecture from the planning and design phase through implementation. Selected topic: Information Systems Security, the Information Systems Security/Operating Systems, and the Information Systems Security/Security Hardware issues.

YEAR ONE: SEMESTER TWO

IIT 4121 Information Systems Control and Audit (42 hrs)

Trends and advances in information systems audit and controls. Cryptographic algorithms, protocols and applications. Secure e-commerce. Cryptosystems: basic hash checksums, symmetrical and asymmetrical cryptography algorithms, basic protocols and standards like RSA and SSL, digital signatures and digital cash, the concept of a PKI and X509 certificates, and various crypto-software applications. Computer security and controls to information systems: authentication and access control, protection against malicious code and coders, database security, formal models, and policy issues, Computer crime and abuse, Risk management. Layered protection mechanisms for secure web-based client/server systems on the Internet. Auditing processes; auditing transaction databases: auditing methodology, evaluation of secure financial transactions, and detections of unauthorised access.

IIT 4122 Computer Digital Forensics (42 hrs)

Latest advances in cybercrime activities; digital forensics: crime scene investigation and processing, forensic science and computer forensics topics. Selected topics: crime scene procedures and documentation, collecting and preserving integrity of evidence to present to court, computer forensic science, locating digital evidence (e.g., computer systems, networks, wireless communications, and storage devices), and basic legal principles related to computer forensics. The role of computer forensics specialist in cyber-crime investigations: incidence response techniques; determination of losses and compromises to the security of enterprise information. E-discovery tracking and reporting techniques.

IIT 4123 Legal Issues, Ethics and Incident Response in IT Security(42 hrs)

Advances in IT incidence response techniques; practical approach for responding to computer incidents, a detailed description of how attackers undermine computer systems in order to learn how to prepare, detect, and respond to them. Concepts of risk management; explore the ethics and legal issues associated with responding to computer attacks: employee monitoring, working with law enforcement, and handling evidence. Focus in particular on practical, computer-assisted techniques for risk-related modeling and calculations. Identification of threats through Hazard and Operability Analysis [HAZOP]) and PHA (Process Hazards Analysis, probabilistic techniques for estimating the magnitude and likelihood of particular loss outcomes.

IIT 4124 Computer Security, Risk Management and Control (42 hrs)

Fundamentals of IT security risk management and control. Explore the threats and risks present in organizations due to the pervasive use of technology. Concepts of risk evaluation techniques and identify security and control techniques used to minimizing threats and risk to the organization's network infrastructure. Selected topics on computer and information security: threat techniques, protective techniques, risk analysis, contingency planning and incidence response, password techniques, encryption, network protocol, and intercept devices. Case studies of latest risk associated with cyber-attacks and cyber-crime activities. Capstone term project/paper research on network cyber-activities.

IIT 4125 Strategic Information Systems Management (42 hrs)

Introduction; information systems strategy and management: business models and organization forms in the information age, IT as a business enabler, IT and competitive strategy, information for management control, analysis and redesign of business structure and processes, knowledge management and information networks, interorganizational networks, sourcing strategies, interfacing with the IT function, reliability and security, and ethical and policy issues. Advances in security management in information systems and networks. Intrusion detection systems, intrusion prevention systems, anomaly detection, network forensics, application monitoring and logging, auditing and data management, contingency planning, digital immune systems; alarm and responses; security standards; ethical and legal issues in information; cyber-evidence. Case studies.

IIT 4126 Fundamentals of IT Security Law and Policy (42 hrs)

Overview and introduction to Law, IT Security and Policy; survey the existing/general legal issues that must be addressed in establishing institutional InfoSec standards and best practices. Canvasses the many new laws on data security, and evaluates InfoSec as a field of growing legal liability. Focus on: computer crime and intellectual property laws when a network is compromised, emerging topics like honeypots, and active defenses, i.e., enterprises hacking back against hackers. Study on impact of future technologies on law and investigations.

IIT 4127 Information Security Policy and Compliance (42 hrs)

Latest advances in organizational security policy and compliance. Legal and privacy issues; Concepts of organizational security policies; Evaluation tools: standards and best practices. Procedures and processes required to enforce policy and compliance. Techniques: install, monitor and audit key information security regulatory requirements: SOX, PCI, HIPAA, GLBA & best practices like COBIT, ITIL and ISO17799.

IIT 4128 Cybercrime Investigations (42 hrs)

Introduction to cybercrimes investigations techniques: unauthorized access, mischief to data, possession of hacking tools, possession of child pornography. Legal aspects: organization legal issues, Kenyan judicial system, computer crime laws, rights of citizens, common law, mutual legal assistance treaty, search warrants, production and assistance orders, international laws, upcoming legal changes; Investigation process: search planning, acquisition methods, environment recognition, evidence identification. Reporting process: investigation and analysis reports, notes taking; Authority of seizure; Forensic Interviews; Computer crime trials: witness preparation, court sentencing, rebuttal witness, cross-examination, testimony, credibility attacks; Real world issues case studies. Students will undertake a capstone research project on cybercrime activities in Kenya and laws that govern it.

IIT 4129 Advanced Linux/UNIX System Administration (42 hrs)

Overview and concepts of DNS (domain name system) servers and the Apache Web server (httpd). Fundamental concepts of LDAP (lightweight directory access protocol) directory queries and authentication. Administration and configuration of server-side programming tools (e.g., CGI, mod_perl, PHP, JSP, Jakarta Tomcat, and Java SDK). Setup and configure: SAMBA, FTP, Telnet, and SQUID proxy servers. SMTP (simple mail transfer protocol) theory implemented via Sendmail and Postfix e-mail systems. E-mail protocols such as IMAP and POP are configured;

spam filtering techniques. Discuss next generation networks, applications, and services: Voice over IP (VoIP), Instant Messaging (IM), Streaming media (unicast, broadcast, and multicast), and peer-to-peer networking.

IIT 4131 Project (84 hrs)

Each student will conduct his or her research with the approval and under the direction of the designated Departmental Course Coordinator. Prerequisites: Successful completion of all core Information Technology Security Specialist (ITSS) courses