CLARENCE FITZROY BRYANT COLLEGE

PROGRAMME: ***INFORMATION TECHNOLOGY ASSOCIATE DEGREE***

CURRICULUM:	***Information and Communications Technology***
COURSE TITLE:	*Data Security Concepts*
COURSE CODE:	IFTH2006
LEVEL OF STUDENTS:	N/A
CREDITS:	*3*
SEMESTER:	*2 (Two)*
DURATION:	*45 hours*
PREREQUISITE(S):	IFTH2003

RATIONALE

Data security concepts is an advanced course that focuses on one of the most important and critically needed skill areas in information assurance and networking: network security. It builds upon an introductory course on the fundamentals of networking, TCP/IP and internet, to investigate the concepts and practices for securing networks and network communications. The Data Security course also leverages key information assurance concepts and practices such as encryption, authentication, risk analysis, security policy design and implementation, etc.

COURSE DESCRIPTION

This course provides students with the knowledge and skills to begin supporting network security within an organization. Students who complete this course will be able to identify security threats and vulnerabilities, and help respond to and recover from security incidents.

LEARNING OUTCOMES

On completion of this course students should be able to:

1. Explain how to secure information.
2. Identify and counteract social engineering exploits.
3. Identify and solve security issues with the network of an organization.
4. Create a process to maintain file security.
5. Design policies to guard against security breaches.
6. Create measures to prevent attacks on an organization's network.

CONTENT KNOWLEDGE

1. Securing Information
    - Understand Information Security
    - Implement Physical Security Measures
    - Identify the Need for Cyber Security

2. Counteracting Social Engineering Exploits

- Identify Social Engineering Exploits
- Counteract Social Engineering Exploits
- Evolve Social Engineering Organization Policies

3. Identifying Security Measures

- Strengthen Desktop Security
- Strengthen Software Security
- Strengthen Network Security
- Secure Wireless Networks

4. Maintaining File Security

- Implement Security in Windows Vista
- Back up Data
- Restore Data
- Dispose of Computer Information

5. Guarding Against Attacks

- Protect Computer from Security Threats
- Protect Computers from Virus Attacks
- Block Spyware

10. Handling Security Breaches

- Identify Incidents
- Respond to Incidents

11. Network Defense

- Network Defense Fundamentals
- Security policy Design & implementation
- Network Traffic signatures

- Firewalls-Designing and choosing
- Firewalls-Deploying and operating
- Intrusion Detection systems (IDS)
- Intrusion Detection and Incident Response
- Virtual Private Network (VPN) Concepts
- VPN Implementation

TEACHING AND LEARNING METHODS

1. Lecture
2. Lab
3. Tutorial questions (worksheet)
4. Demonstration
5. Discussion
6. Presentation

Assessment Procedures

1. Coursework 60%
2. Examination 40%

ASSESSMENT SUMMARY

Task / Assignment No. & Name	Due Date	Time	Weight	Type	Learning Outcomes
1. Oral Presentation / Video	19th Feb.	3:30 pm	20%	Class Work	1, 2
2. Practical / Video	18th Mar.	3:30 pm	30%	Project	3, 4
3. Mid Term	22nd April.	3:30 pm	20%	Test	5, 6
4. Final Exam	May		30%	Individual	1 - 6

Nb: Dates are subjected to be changed. Textbooks and References

TEXTBOOKS AND REFERENCES

Weaver. R., (2007). *Guide to network defense and countermeasures* (2nd ed.). Boston, MA: Thomson Course Technology.

Reading List

- Simpson, M. (2006). *Hands-on ethical hacking and network Defense*. Boston, MA: Thomson Course Technology.

- Howlett, T. (2004). *Open source security tools: A practical guide to security applications*. Upper Saddle River, New Jersey: Prentice Hall.

- Harris, S., Harper, A., Eagle, C., & Ness, J. (2005). *Gray hat hacking: The ethical hacker's handbook.* McGraw Hill Osborne Media.