ST. VINCENT AND THE GRENADINES COMMUNITY COLLEGE

Associate Degree in Cyber Security

Associate Degree in Cyber Security

Introduction

Cyber-attacks have grown in frequency and sophistication in recent years in the regional and international arenas. To immediately address this ever evolving threat which can compromise the nation's safety and security, it has become necessary to outsource the relevant expertise from outside of St. Vincent and the Grenadines to put the necessary systems in place as we do not have sufficient expertise locally and there is no training available to assist locals who are interested.

Our country and the region have been embarking on a number of initiatives in ICT over the last 10 years but nothing is being done (of a substantive nature) that the NTRC is aware of on this issue either locally or regionally. Anti-viruses and similar software cannot stop the real threats that we can face from this issue in the short to medium term. St. Vincent and the Grenadines should not wait until something goes very wrong before we act. For natural (and some man made) disasters, St. Vincent and the Grenadines have established specialized agencies to address these types of disasters both locally and regionally but we have no similar agencies to handle threats and damages from cyber-attacks. Now take it a step further and imagine that our banks start having losses due to fraudulent electronic activity, our institutions, especially the Government service (most susceptible) start losing confidential electronic documents, our private sector IT companies not able to operate and worst we start having our electronic records altered so as to provide wrong data to the user.

Noting this fact, the NTRC identified the issue of cyber security as a priority goal which needs to be addressed since 2009. Additionally, The Prime Minister Dr Hon. Ralph Gonsalves who was also the Minister of Telecommunication at the time, approved the cyber security priority from a policy perspective to be addressed. Following Discussions in 2011 with the Dean and other officials from the St. Vincent and the Grenadines Community College with regards to the implementation of the cybersecurity program, the Commission and the College were in agreement for the implementation of such a cyber-security program to address the concerns of the Prime Minister and that of the Commission.

Through the SMART project, which was signed with LIME on November 20th 2012, this has come to reality. The NTRC with the assistance of the SMART project implementation committee has developed a comprehensive Associate Degree program consisting of relevant courses and course outlines to provide students who will undertake this program, a solid foundation on which to continue their studies in Cyber Security. These courses were identified by the SMART Project committee comprising of relevant individuals from various sectors including the SVG Community College. The development of this program and the course outlines took several months to be completed.

It is now up to the St. Vincent and the Grenadines Community College to take this step in including this program in its already well rounded Associate degree programs being offered at evening classes. Taking this step is of vital importance as it will facilitate the medium by which local students will be able to get training in Cyber Security and thus creating a generation of cyber security specialist. This will assist in the securing of our local content and developing a cadre of students versed in Cyber Security issues with the skill to mitigate against treats which can become reality.

This program is structured to meet the needs of the working population and address an existing need within our education system which ties in with the mission of the St. Vincent and the Grenadines

Community College. With the acceptance of the program to be offered at the SVG Community College, qualified individuals will be afforded the ability to undertake this innovative program.

Programme Objectives

This program aims to give individuals who are interested in becoming Cyber Security professionals, a solid framework on which to build upon before going and attain higher level of qualification in this area. This Associate Degree program will provide the student with the practical and theoretical frameworks around cyber security.The program will provide a framework for protecting computer systems of businesses, organizations and government agencies. It will present a systematic approach for professionals concerned with the development of secure systems and the protection of an organization's assets. The Associate Degree program gives an overview of the strategies, policies, ethical and legal issues associated with securing systems in the workplace. It will provide a foundation for the development of critical thinking skills that are transferrable to analysing and responding to new cyber security threats and allows working professionals to add a focus in cyber security to their existing career track, improve their skill set or to begin a career in this area. It is also ideal for companies, firms and government agencies who wish to advance employees' training in the field and the Commission envisages that companies will send their employees to get the training in this area to assist with their own internal networks.

Programme Structure

The Associate Degree program in Cyber Security utilises a semester system. It is designed to run as a part time programme over two years. The part time programme utilises four semesters and a summer session for each of two academic years. Each semester is 15 weeks plus the examination period and the summer session is 8 weeks plus the examination period.

Qualifications for Admission for the Associate Degree in Cyber Security

Applicants should at least have the following:

1. Two A Level or CAPE passes inclusive of Information Technology or Math.(Grade A B or C)

   OR

2. Holders of approved relevant certificates from the UWI School of Continuing Studies or Open Campus or other notable institution.

OR

3. Persons who do not meet the above requirements but who have relevant work experience.

NOTE: Prospective candidates will be required to attend an interview prior to admission

NOTE: Prospective candidates will be required to attend an interview prior to admission

Scheduling of courses for Associate Degree in Cyber Security

COURSE CODE	**COURSE TITLE**	**Hours per week**					**Total Credits**
		Year 1		**Year 2**		**Hrs**	
		Sem 1	**Sem 2**	**Sem 1**	**Sem 2**		
	GENERAL EDUCATION						
	Networking 1	3					
	Discrete Maths	3					
	Business and IT Law	3					
	Networking 2		3				
	Technical Report Writing		3				
Minimum number of General Education Course credit required							**15**
	CORE COURSES						
	Foundations in Cyber Security		3				
	Data Security Concepts			3			
	Fundamental to Programming Problem Solving			3			
	Data Management Systems			3			
	Cyber Terrorism & Cyber Crime				3		
	Information System Security				3		
	E- Commerce				3		

Minimum number of elective credits required							
Minimum number of credits needed to graduate							

GRADING SYSTEM

The authorized grading system is as indicated below. In the determination of the Grade Point Average (GPA), the defined grades with the corresponding quality points are as indicated below.

Grade	**Mark**	**Quality Points**
A+	90% - 100%	4.00
A	85% - 89%	3.75
A-	80% - 84%	3.5
B+	75% - 79%	3.25
B	70% - 74%	3.0
B-	65% - 69%	2.75
C+	60% - 64%	2.5
C	55% - 59%	2.25
C-	50% - 54%	2.0
D	40% - 49%	1.0
F	0% - 39%	0.0

CATEGORIES OF AWARD OF THE ASSOCIATE DEGREE

The categories of award for the certificates are: Distinction, Merit and Pass

The categories are based on the GPA system as follows:

Distinction	GPA of 3.75 and above
Merit	GPA of 3.50-3.74
Pass	GPA of 1.00-3.49

DETAILED COURSE OUTLINES

1. **Course title:** **Cyber terrorism and Cyber Crime**

2. **Course code**: CBT101

3. **Course Provider**: SVG Community College: – Division of Arts, Science and General Studies

4. **Level**: **Second year course**

5. **Semester** Semester **2**

   Provided across Departments/Faculties

6. **No. of credits/ Hours**: 5 Credits/ 45 Hours

7. **Total study hours**: Includes:
   - teaching time
   - study time
   - a student's preparation time for classes

8. **Course Description**** Intensive hands on investigation of computer related crime designed for the profession as an electronic crime investigator. Course prepares students to become effective cybercrime investigators. Students will identify, evaluate, classify, and demonstrate proficiency in investigating computer related crimes. Students subject to background investigation prior to admittance.

9. **Course Rationale:**

   Cyber terrorism has emerged as a growing threat to national security. This is true not just for the United States but many countries around the world. With over 180 countries connected to the Internet, this technical communications medium is a primary channel for commerce, communications and citizen interaction. Terrorists have recognized the value of the Internet for recruiting and covert communication, as well as a weapon against the adversaries they despise. This 1 day program will provide the background to understand this growing threat. It will provide unique insight into how terrorists use the Internet, as well as insights into the challenges that we face.

10. Learning Outcomes:

Upon successful completion of this course, the student will be able to;

- Recognize and describe the functions of internal hardware components of computers.
- Apply techniques in analysis of sequences in electronic crime.
- Comprehend motivational factors in deviant behavior of computer criminals.
- Analyze historical concepts of operating systems.
- Understand how data is transferred from input devices to electronic media.
- Analyze the differences in operating systems when performing investigations.
- Understand network applications for investigations.
- Evaluate search warrant requirements for computer network centers.
- Synthesize the procedures of how to structure a cybercrime investigation.
- Analyze the processes an investigator should follow when searching for evidence on a network.
- Demonstrate procedures for doing e-mail tracking for use as evidence.
- Analyze the operation of wireless networks, layering, RF concepts, Ethernets and microchips to assist the investigator in the processing of digital evidence

11. Content:

- Historic Analysis of Computer Related Crime
- Evaluation of the DOS File System and where data could be hidden
- Recovering Erased Files
- Motivational Factors in deviant behaviour of computer criminals
- Process Analysis and Seizure Considerations – Preserving Computer Based Evidence
- Automated Search Techniques
- Network Investigations
- Investigative Framework Methods
- Embezzlement
- What is Fraud
- What is an Investigation
- Larceny
- Interviewing/Interrogating Suspect
- Methods of Committing Check Fraud

12. Teaching Methodology Classroom discussions, group work, case study, lectures, texts, supplied readings and internet use (video clips, research medium).

13. Assessment Students will complete a course work assignment, a midterm, and a final exam.

(i)Assessed coursework

Assignment 1:	Midterm	30%
	Final exam	60%

14. Course Evaluation Formative and summative

15. Required Readings

Text:

Bishop, Matt. (Latest edition), Computer security: art and science. Addison-Wesley / Pearson Education

Other readings will be determined by the lecturer.

16. Course Calendar

Teaching Schedule

Week 1: **Historic Analysis of Computer Related Crime**

The student is expected to;

- Understand the development of cyber crime
- Have a good understanding of the evolution of computer hardware

Content

1. Historic Analysis of Computer Related Crime

    a. State and Federal Laws as they pertain to establishing expert witness status.

II. Importance of historical knowledge of Computer Operating Systems

a. Evolution of computer hardware IDE / EIDE / ATA Interface

b. Switch settings on Hard Drives, Modems, Printers, Memory, RAM

c. DOS Commands MD, CD, DIR, COPY, CHKDSK, DEL, TYPE, RENAME, PATH, ATTRIB

d. DOS' Edit Program, Redirection, Wildcards.

Evaluation of Computer Data (Bits and Bytes)

a. From bits and bytes to ASCII

b. The ANSI/ASCII standard – what are bits, nibbles, bytes, characters, words, and beyond.

c. DISKEDIT in hex mode.

Understand Logical and Physical Characteristics of Hard Drives

a. Cylinders, Heads, and Sectors

b. Verification of the total data capacity of a seized hard drive.

c. The difference between Physical and Logical drives.

d. Using FDISK to partition a drive

e. DOS Format – Chat changes it does and does not make.

f. Sectors, clusters, File Allocation Tables (FAT) and system areas

g. Un-formatting – Recovery techniques

h. Drive Letter Assignment

Week 2: Evaluation of the DOS File System and where data could be hidden

Students should be able to;

- Find where any data is stored or hidden
- Have a clear understanding of the DOS file system

Content

a. Sectors, Clusters, System Area

b. Subdirectory clusters

c. Storage issues with respect to size, date and time

d. Tracing out the chain of a file

e. The problem with slack space

f. Understanding the dot and dot-dot pointe.

Week 3: Recovering Erased Files

Students should be able to;

- Recover any file which has been deleted

Content

a. Deleting files – What changes and what does not

b. What it takes to manually unerase a file using Norton's DISKEDIT program

c. Automatic unerase using the unerase utility

d. Long File Names/Recycle Bin

Creating Controlled – Boot Floppies, Boot Sequence

a. Power on sequence

b. How to examine CMOS settings – Hard drive parameters, Power-on passwords, drive sequence

c. Boot record

d. DOS 7 modifications

e. Creating an autoexec.bat file

f. Hard drive write blockers and other utilities

Week 4: Motivational Factors in deviant behavior of computer criminals

Students should be able to;

- Identify various factors which causes deviant behavior with regards to Cyber Crime

Content

a. Financial

b. Spite Revenge

c. Pedophilia

d. E-Bay Fraud

Week 5- **<u>Process Analysis and Seizure Considerations – Preserving Computer Based Evidence</u>**

The students should be able to;

- Properly process and analyze evidence seized.
- Comfortably preserve computer base evidence

<u>Content</u>

a. Pre-Raid considerations

b. Raid Kit items: tools, hardware, tape, labels, camera and film

c. Securing and processing an electronic crime scene

d. Safeguarding evidence

e. Evidence analysis considerations

f. Duplicate image versus file–by-file copy

g. Hardware and software considerations – validation of tools

h. Working with SAFEBACK and removable media

i. Imaging floppy disks

Week 6: Automated Search Techniques

The students should be able to;

- To perform automated searches by the use of various key words

Content

a. Identifying Files

b. Headers and Extensions

c. Keyword concepts

d. Working with automated tools and Disk Edit

Week 7- Network Investigations

The students should be able to;

- Perform the necessary network investigation

Content

a. Network Topologies

b. Conducting the Network Investigation

c. Dealing with the Network Administrator

d. Wireless

Week 8 **Investigative Framework Methods**

The students should be able to;

- Identify the and undertake necessary methods of investigative frameworks

Content

a. Introduction to TCP/IP

b. E-Mail Headers

c. USENET, News,

d. Trace route

e. Ping

f. NEOTRACE g. NSLOOKUP

h. Host, Message Digest, File Signatures, Cyclic Redundancy Checks

i. Break-in-Intrusion Logs

j. Kernel Hacking, Root Kits

Week 9: **What is Fraud?**

The students should be able to;

- Clearly outline what is fraud
- Identify the different elements of fraud

Content

a. An intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right

b. Deceit

c. Trickery

d. Cheating

Week 10 .What is an Investigation?

The students should be able to;

- Define and Conduct an investigation

Content

a. An Investigation is a Search for the Truth

b. The Investigator

c. The Investigation

d. Unbiased

e. Truthful

f. Integrity

11: LARCENY

The students should be able to;

- Define larceny
- Identify the various forms of larceny

LARCENY

a. Unlawful taking

b Personal Property

c Intent

d Permanently Deprive

Week 12: **Embezzlement**

The students should be able to;

- Define embezzlwment
- Identify the various forms of larceny

Content

a. Common Methods

b. Limited only by imagination.

c. Cash is received and the employee merely pockets it without making a record of the transaction.

2. Types of Embezzlement

a. Point of Sale

b. Payroll Frauds

c. Kickbacks

d. Pad expense accounts.

e. Failure to return property

f. Inventory theft

g. Lapping

h. Real-estate?

3.Computer/Internet Related Embezzlement

a. Do traces of all IP address discovered

b. 2703f Preservation Letter

c. Pin register on Suspect's telephone d. Search Warrant on ISP's

e. Forensic on both Complainant's & Suspect's PCU (documents, internet history, e-mail, diary etc…)

Week 13: Interviewing/Interrogating Suspect

The students should be able to;

- Effectively conduct an interrogation
- Have a full understanding about the different methodologies in interrogation

Content

a. Interview Suspect at home if possible (not in custody)

b. Inquire about financial institution/situation

c. Show empathy

d. Ask the suspect why did he/she took the money

2. If Confession is Obtained

a. Ask when (time line) and why?

b. Method of Embezzlement (could be another incident or different crime they are confessing to)

c. Amount taken

d. Account for all the money that was taken

e. Any co-conspirators?

f. Use search warrants to “freeze” defendant’s accounts

Week 14.Methods of Committing Check Fraud

The students should be able to;

- Investigate and identify check fraud occurrences

Content

a. Theft and forgery of a legitimate check

b. Issuance of genuine checks to fictitious entities

c. Alteration of legitimate checks

d. Duplication or counterfeit copies of checks

e. Check-Kiting

CRIMINALS USE COMPUTERS TO COMMIT FRAUD

a. Fraudulent Checks

b. Fraudulent Checks

c. Obtain Original Document

d. Process for fingerprints

e. Handwriting analysis (after suspect is arrested)

f. Needed as Evidence in Court g. Fraudulent Checks

h. Investigative Techniques

i. Merchants

Week 15: **Final Exam**

Readings: Lecturers Notes and Handouts; Required Text **Final Exam:** based on the topics covered from week 11 through 15, handouts, readings, and class activities.

17. Pre-requisites:	None
18. Co-requisites:	None
19. Post-requisites	None
20. Forbidden	None
21. combinations:	

21. Academic staff member who may be contacted for more information:

Name:	Telephone: 784 457-5403
Title: Mr.	E-mail:
Faculty: Arts, Science and General Studies	Department:

1.	**Course Title**	**Foundations in Cyber Security**
2.	**Course Code**	**CYB101**
3.	**Course Provider**	SVG Community College: Division of Arts, Science and General Studies
4.	**Level**	First Year Course
5.	**Semester in which it will be offered**	Semester 2
6.	**No. of Credits/ hours**	5 Credits/ 40 Hours
7.	**Total Study Hours**	45 Hrs. Includes: • Teaching time • Study time • A student's preparation time for classes
8.	**Course Description**	This course aims to provide a solid understanding of the theory and practice used to maintain security on computer systems and networks. In more detail, it includes material providing an overview of computer and communications security, risk assessment, human factors, identification and authentication, access controls, malicious software, software security, O/S security, trusted computer systems, network attacks and defences, firewalls, intrusion detection and prevention, database security, legal and ethical issues.
9.	**Course Rationale**	The ability to secure information within a modern enterprise—large or small—is a growing challenge. Threats to information security are global, persistent, and increasingly sophisticated. Long gone are the days when managers could hope to secure the enterprise through ad hoc means. This course is designed to teach security practitioners how to engage all functional levels within their enterprise to deliver information system security. To this end, the course addresses a range of topics, each of which is vital to securing the modern enterprise.

10. Learning Outcomes

By the end of this course, students will be able to:

- State the basic concepts in information security, including security policies, security models, and security mechanisms.
- Explain the concepts of malicious code, including virus, Trojan horse, and worms.
- Outline the requirements and mechanisms for identification and authentication.
- Explain issues about password authentication, including dictionary attacks (password guessing attacks), password management policies, and one-time password mechanisms.
- Explain and compare security mechanisms for conventional operating systems
- Explain the requirements for trusted operating systems, and describe the independent
- Describe security requirements for database security, and describe techniques for ensuring database reliability and integrity, secrecy, inference control, and multi-level databases.
- Describe threats to networks, and explain techniques for ensuring network security, including encryption, authentication, firewalls, and intrusion detection.
- Explain the requirements and techniques for security management, including security policies, risk analysis, and physical threats and controls.

11. Content

1. Basic Security Concepts
2. Basic Cryptography
3. Program Security
4. Security in Conventional Operating Systems
5. Trusted Operating Systems
6. Database Management Systems Security
7. Network Security
8. Management of Security
9. Privacy & Ethics

12. Teaching Methodology

To facilitate fulfilment of the requirements of this course lesson will utilise the following methods:

- Presentations
- Demonstrations
- Individual & Group work
- Discussions
- Independent Problem Solving Labs

13. Assessment

1. Course Work (40%)
   - i. Independent Problem Solving Assignments (20 %)
   - ii. Group Problem Solving Assignments (20 %)
2. Final Examination (60%)

14. Course Evaluation Approaches

Formative and Summative

15. Required Readings

Charles P. Pfleeger and Shari L. Pfleeger. Security in Computing (Latest edition). Prentice-Hall.

16. Course Calendar

Week 1 & 2

Introduction

Students should be able to;

- Identify the basic concepts involved in cyber security
- Have a good understanding of the evolution of cyber security

Content

- Basic concepts: threats, vulnerabilities, controls; risk; confidentiality, integrity, availability; security policies, security mechanisms; assurance; prevention, detection, deterrence.

Basic cryptography

- Basic cryptographic terms
- Historical background
- Symmetric crypto primitives
- Modes of operation
- Cryptographic hash functions
- Asymmetric crypto primitives

Week 3 & 4 **Program security**

The student will be able to;

- Should be able to identify malicious codes
- Write malicious program codes

Content

Flaws

- Malicious code: viruses, Trojan horses, worms
- Program flaws: buffer overflows, time-of-check to time-of-use flaws, incomplete mediation

Defenses

- Software development controls
- Testing techniques

Week 5 & 6 Security in conventional operating systems

The student will be able to;

- Identify various security features in various operating systems

Content

- Memory, time, file, object protection requirements and techniques
- Protection in contemporary operating systems
- Identification and authentication
    - Identification goals
    - Authentication requirements
    - Human authentication
    - Machine authentication

Week 7 & 8

Trusted operating systems

The student will be able to;

- Review and have a good understanding of the more used operating systems
- Identify similarities and differences in the operating systems.

Content

- Assurance; trust
- Design principles
- Evaluation criteria
- Evaluation process

Week 9 & 10

Database management systems security

The student will be able to;

- Design systems to ensure that a database is secure from threats and functions properly.

Content

- Database integrity
- Database secrecy
- Inference control
- Multilevel databases

Week 11 & 12

Network Security

The student will be able to;

- Identify various network security techniques
- Identify the similarities and differences in each technique identified

Content

- Network threats: eavesdropping, spoofing, modification, denial of service attacks
- Introduction to network security techniques: firewalls, virtual private networks,
- intrusion detection

Week 13 & 14 Management of Security

The student will be able to;

- Understand legal and ethical issues in the management of security

Content

- Security policies
- Risk analysis
- Physical threats and controls

Miscellaneous

- Legal aspects of Security
- Privacy and ethics

Week 15 Final Exam

17.	**Pre-requisites**	Basic knowledge on operating systems and C programming skills
18.	**Co-requisites**	None
19.	**Post-requisites**	None
20.	**Forbidden Combinations**	None
21.	**Academic staff member who may be contacted for more information:*****	

1. **Course Title** **Discrete Mathematics**

2. **Course Code** **MS 101**

3. **Course Provider** SVG Community College: Division of Arts, Science and General Studies

4. **Level** First Year Course

5. **Semester in which it will be offered** Semester 1

6. **No. of Credits/Hours** 5 Credits/ 45 Hours

7. **Total Study Hours** 45 Hrs.

   Includes:

   - Teaching time
   - Study time
   - A student’s preparation time for classes

8. **Course Description** This course equips student with the relevant mathematical concepts and methods required for adequately undertaking courses in data processing management techniques and related areas. It aims to advance students’ appreciation of and abilities in the use of Mathematics as a precise model of thought and communication as well as a tool for modelling various problem situations arising in data processing and the business world at large.

9. **Course Rationale** Mathematics is fundamental to the ICT profession as the ability to think logically, reason to solve problems are assets that all ICT professionals must have if they are to program computers, mange data processing and analyse systems. This course in the discrete Mathematics provides students with formal training in higher level problem-solving, such a logics and proof, set theory, matrices, logarithms and algorithms. Through it students will develop better understandings of how to use mathematics as a tool when solving data process issues that arise in businesses and other types of organisations.

10. Learning Outcomes

Upon completion of this course students should be able to:

- Identify, convert and locate errors in different number systems.
- Explain, define and set theory.
- Identify and construct logic and proof
- Classify, compute and interpret Matrices.
- Explain the concepts of exponents, logarithms, relations and algorithms.
- Explain and demonstrate the concepts of function and graphs
- Create and evaluate function graphs

11. Content

Computer Arithmetic
Set Theory
Logic and Proof
Matrices
Exponents and Logarithms
Relations
Algorithms
Functions and Graphs

12. Teaching Methodology

To facilitate fulfilment of the requirements of this course lesson will utilise the following methods:

- Presentations
- Demonstrations
- Individual & Group work
- Discussions
- Independent Problem Solving Labs

13. Assessment

Course Work (40%)
iii. Independent Problem Solving Assignments (20 %)
iv. Group Problem Solving Assignments (20 %)
Final Examination (60%)

14. Course Evaluation Approaches

Formative and Summative

15. Required Readings

Johnsonbaugh, R. (2008). Discrete mathematics. (7th ed.). New Jersey: Prentice Hall.

Supplemental Text Readings

- Lipschutz S. & Lipson M. (2007). *Schaum's outline of discrete mathematics*. (Schaum's outline series) (3rd ed.). Ohio: McGraw Hill.
- Kolman, B., Dusby, R., & Ross, S.C. (2009). *Discrete mathematical structures*. (6th ed.). New Jersey: Prentice Hall.

16. Course Calendar

Week 1 Computer Arithmetic

The student will be able to;

- Demonstrate a good understanding of computing arithmetic

Content

- Number systems – binary, decimal, octal and hexadecimal
- Conversion between the number systems
- Representation of numbers in various forms including fractional forms:
  i. Fixed and
  ii. Floating point
- Errors in computing

Week 2 Set Theory

The student will be able to;

- Understand and various theories in sets

Content

- Definition of sets and the following terms: finite sets, infinite sets, equality of sets
- Representation
- Recognition of universal set, empty set, subsets etc
- Operation of sets: union, intersection, complement, etc
- Venn diagram and computations
- Evaluation of the number of subsets

Week 3 & 4 Logic and Proof

The student will be able to;

- Understand sentential and predicate logic

Content

- Identification of negation, conjunction, disjunction,
- Construct truth tables using the notations above
- Qualifier – existential and universal
- Proof by induction and contradiction

Week 5 & 6 Matrices

The student will be able to ;

- Perform matrix operations
- Interpret evaluate and resolve practical matrices

Content

- Classification of matrices
- Matrix operations
- Computation of determinants, the adjoin or inverse matrices, and transposition of a matrix
- Solution of linear simultaneous equations using:
    - i. Cramer's rule
    - ii. Abdugate method
    - iii. Gauss-Jordan method (Row operations)
- Interpretation and evaluation of practical problems

Week 7 & 8 Exponents and Logarithms

Students will be able to;

- Cleary understand the laws of logarithms

Content

- $a^x = p, where\ a \in R, x \in Q\ and\ P > 0$
- Laws of Indices and Logarithms
- Implied in specific objective 2 and 3 above
- $a^x = p \leftrightarrow \log_a P = x$

Week 9 & 10 Relations

Students will be able to ;

- Determine by the use of analysis, ordered pairs and recurrence relations

Content

- Determination of ordered pairs
- Construction of tree diagram (binary trees)
- Equivalence relation:
  i. Symmetric
  ii. Reflexive
  iii. Transitive
- Recurrence relations

Week 11 & 12 Algorithms

Students should be able to ;

- Be able to explain fundamental data structures (see Course Objectives) and their use.
- Know the working of and be able to apply fundamental computing algorithms (see Course Objectives).
- Be able to analyse time and space complexity of algorithms in terms of asymptotic notations, identify the difference between best-, average- and worst-case behaviours, use recurrence relations to analyse recursive algorithms, and explain the time and space trade-off in algorithms.
- Be able to apply basic algorithmic strategies (see Course Objectives) to design algorithms for concrete problems of reasonable difficulty.

Content

- Identification of algorithms
- Analysis of algorithms
- Euclidean algorithm
- Algorithm pertaining to Permutations and Combinations

- Evaluation of binomial coefficients
- Recurrence relations
- Proof by Mathematical Induction:
  i. Divisibility of expressions
  ii. Validity of summation formula for series

Week 13 & 14 Functions and Graphs

Students will be able to;

- Identify and demonstrate a good understanding of functions and grapjs

Content

- Graphing Linear$(y = mx + c)$, Polynomial (up to degree n = 3), Exponential $(y = a^x)$ and Logarithmic $(y = \log_b x)$ functions.
- For $(y = mx + c)$ or $(ax + by = c)$, *the y- intercept is when x = 0, and the x – intercept is when y = 0*
- Gradient of a Linear Function = $\frac{increase\ in\ y}{increase\ in\ x} = \frac{Vertical\ distance}{Horizontal\ distance}$
- Positive Gradient denotes an increasing function while a negative gradient denotes a decreasing function

Week 15 Final Exam

17. Pre-requisites None

18. Co-requisites None

19. Post-requisites None

20. Forbidden Combinations None

1. **Course Title** **Information Systems Security**

2. **Course Code**

3. **Course Provider** SVG Community College: Division of Arts, Science and General Studies

4. **Level** Second Year Course

5. **Semester in which it will be offered** Semester 2

6. **No. of Credits/ Hours** 5 credits/ 45 Hours

7. **Total Study Hours** 45 Hrs.

   Includes:

   - Teaching time
   - Study time
   - A student's preparation time for classes

8. **Course Description** This course focuses on the large scale implementation of information systems security with emphasis on current threats and vulnerabilities. Students will identify key elements that enable these cyber security threats and apply security controls that can mitigate the risk associated with these threats. Students will protect systems and networks from threats. This course will explore methods, tools, and techniques that intruders use to exploit vulnerabilities in systems. The student will apply the elements of information assurance and computer security from risk assessment to public key encryption. Additionally awareness training, countermeasures and safeguards and continuity of operations are taught.

9. **Course Rationale** This course is intended to provide the student with the knowledge and tools to protect systems and networks from threats and vulnerabilities thus providing the highest level of information system assurance.

10. Learning Outcomes

On completion of this course students should be able to:

- Manage all aspects of information systems security.
- Understand the elements of information assurance and computer and network security
- Develop and implement policies to provide confidentiality, integrity, and availability of data.
- Understand how to certify and audit systems.

11. Content

- Security Basics
- Security Management Concepts and Principles
- Security Planning
- Security Technology
- Security Organization
- Access Control Models
- Security Architecture and Models
- Physical Security
- Cryptography
- Disaster Recovery and Business Continuity
- Laws, Investigations and Ethics
- Applications Security
- Operational Security
- Web Security

12. Teaching Methodology

To facilitate fulfilment of the requirements of this course lesson will utilise the following methods:

- Presentations
- Demonstrations
- Discussions
- Independent Problem Solving
- Labs

13. Assessment

Course Work (40%)
Independent Problem Solving Assignments (20 %)
Group Problem Solving Assignments (20 %)
Final Examination (60%)

14. Course Evaluation Approaches

Formative and Summative

15. Required Readings

Textbook(s): Peter Gregory,2010, CISSP Guide to Security Essentials, 1st Edition

ISBN-10: 1435428196 ISBN-13: 9781435428195 , Course Technology

Course Calendar

16.

Week 1

Security Basics

Students should be able to;

- Demonstrate a good knowledge in the various terms used
- Be able to identify the structures which exist in the creation of a security architecture.
- Identify the weakness and strengths in a security policy for an organization

Content

a. Security Definitions, security principles and objectives
b. Security architecture, model, and layers
c. Threats, confidentiality, integrity and availability
d. Accountability, auditing and non-repudiation
e. Case study of the security policy for an organization

Week 2 **Security Management Concepts and Principles**

The student will be able to;

- Identify the various concepts for security management
- Be able to implement the principles and concepts outlined above

Content

a. Security management concepts and principles
b. Change control management
c. Data classification system
d. Information/data value, collection, and analysis techniques
e. Employment policies and practices
f. Information security assessment methodology
g. Security awareness, training, and education

Week 3 **Security Planning**

The student will be able to ;

- Identify the various threats and risks to network
- Mitigate against the risks and threats identified

Content

a. Risk Management and Security Policy
b. Continuity of operations and security maintenance
c. Policy, procedures, standards, and guidelines
d. Risk assessment case study

Week 4 **Security Technology**

The student will be able to ;

- Identify and Implement various technologies to secure a network

Content

a. Cryptography, virtual private networks, firewalls and intrusion detection systems
b. Scanning and analysis tools and access controls

Week 5 **Security Organization**

- Effectively develop and implement a security plan for an organization.

Content

a. The organization and security
b. Personnel and security
c. The Computer Incident Response team (CIRT)
d. The security function to include organization, location, responsibility, and resources.

Week 6 **Access Control Models**

Students should be able to;

- Identify access control methods
- Mitigate against various threats

Content

a. Access control techniques and models.
b. Access control methodology and implementation.
c. Discretionary, mandatory and nondiscretionary access control.
d. File and data ownership and custodianship.
e. Threats and methods of attack.
f. Monitoring techniques and lines of defence.
g. Penetration testing.
h. Single-point-of failure.

Week 7 **Security Architecture and Models**

Students will be able to;

- Identify various security architecture and security models

Content

a. Computer Architecture
b. System Architecture
c. Security Models
d. Security Modes of Operation
e. Trust & Assurance
f. Systems Evaluation Methods

g. Rainbow Series
h. IT Security Evaluation Criteria
i. Common Criteria
j. Certification versus Accreditation
k. Open versus Closed Systems
l. Threats to Security Models & Architecture

Week 8 **Miscellaneous**

Students will be able to;

- Understand the various legal and ethical issues to security

Content

- Legal aspects of Security
- Privacy and ethics

Week 9 **Physical Security**

Students should be able to;

- Identify possible weakness in current systems for physical intrusion
- Develop and implement the necessary steps to guard against physical intrusion

Content

a. Administrative, Technical, Physical Controls
b. Planning Process
c. Protecting Assets
d. Internal Support Systems
e. Perimeter Security
f. Intrusion Detection

Week 10 **<u>Cryptography</u>**

Students should be able to;

- Understand the concepts involved in cryptography
- Be able to encrypt and decrypt

<u>Content</u>

a. The basics of Cryptography
b. Cryptographic Concepts, Terms and Definitions
c. Symmetric and Asymmetric Cryptography
d. Cryptographic Algorithms
e. Hash Functions and Message Digests
f. Digital Signatures and Certificates
g. Certification Authorities and Public Key Infrastructure (PKI)
h. Cryptographic Keys and Key Management
i. Link Encryption vs. End-to-end
j. Email
k. Internet Security
l. Attacks
m. Policies for cryptography implementations

Week 11 **<u>Disaster Recovery and Business Continuity</u>**

Students should be able to ;

- Design and implement systems to assist in disaster recovery to ensure that there is continuity in an organization.

<u>Content</u>

a. Disaster Recovery vs Business Continuity
b. Contingency Planning Process
c. Project Initiation
d. Business Impact Analysis
e. Backup Strategies
f. Plan Development
g. Implementation
h. Testing & Drills
i. Maintenance

Week 12

Laws, Investigations and Ethics

Students will be able to;

- Identify and understand the necessary legislative documents in place to address cyber issues
- Understand the procedures necessary for equipment and software handling and disposal.

Content

a. Major Laws
i. Import/Export
ii. Privacy
iii. Copyright
iv. Software Piracy
b. Ethics
i. Generally Accepted Information Security Principles
c. Criminal versus civil law
d. Laws, Directives & Regulations
e. Equipment and Software Disposal
f. Incident-handling Procedures
g. Types of Evidence

Week 13

Security

Students will be able to;

- Identify the necessary security feature necessary for applications and various operating systems.

Content

Applications Security

a. The Computing Environment
b. Database Management
c. System Development
d. Application Development
e. Malicious Code
f. Capability Maturity Modeling

Operational Security

a. Concepts of Computer Operations
b. Administrative Management requirements
c. Computer Operations Concepts
d. Control Types
e. Operation Controls
i. Change Control
ii. Media Controls
f. Fault Tolerance Mechanisms Required
i. Single Points of Failure
ii. RAID
g. E-Mail Security
h. Facsimile Security
i. Auditing and Audit Trails
j. Monitoring Tools and Techniques
k. Penetration Testing Techniques
l. Threats and Countermeasures

Week 14

Web Security

Students will be able to ;

- Ensure that electronic transactions are safe

Content

a. Secure Sockets Layer
b. Secure Electronic Transactions

	Week 15	Final Exam
17.	**Pre-requisites**	Basic knowledge on operating systems and C programming skills
18.	**Co-requisites**	None
19.	**Post-requisites**	None
20.	**Forbidden Combinations**	None
21.	**Academic staff member who may be contacted for more information:*****	

1. **Course Title** **E-Commerce**

2. **Course Code** **ECM101**

3. **Course Provider** SVG Community College: Division of Arts, Science and General Studies

4. **Level** Second Year Course

5. **Semester in which it will be offered** Semester 2

6. **No. of Credits** 5

7. **Total Study Hours** 45 Hrs.

   Includes:

   - Teaching time
   - Study time
   - A student’s preparation time for classes

8. **Course Description**

   This course introduces students to the field of electronic commerce, including the Internet and World Wide Web, planning e-commerce initiatives, marketing, legal and ethical issues, web design, usability and implementation, payment systems and security.

9. **Course Rationale**

   The purpose of this course is to provide students with an overview of the key concepts, strategies, business models, and technologies behind E-business. It explores in detail, opportunities and challenges of doing business on the Internet, and the challenges of introducing e-commerce techniques into existing organizations.

10. Learning Outcome

On completion of this course students will be able to:

- Distinguish between the different categories of Electronic Commerce.
- Discuss the advantages and disadvantages of Electronic Commerce.
- Demonstrate an in-depth understanding of the roles of various Internet Technology Infrastructure.
- Explain revenue models
- Discuss marketing strategies for the web.
- Discuss and explain Legal and Ethical Issues
- Explain the purpose of web server hardware and software
- Discuss the features of Electronic Commerce Software
- Discuss security for Client and Server Computer
- Discuss the different types of Payment Systems
- Develop a plan for an E-Commerce Initiative

11. Content

Introduction to Electronic Commerce
The Internet and the World Wide Web
Revenue Models and Building a Web Presence
Marketing on the Web
Legal, Ethical and Tax Issues
Web Server Hardware and Software
Electronic Commerce Software
Electronic Commerce Security
Payment Systems
Planning for Electronic Commerce

12. Teaching Methodology To facilitate fulfilment of the requirements of this course lesson will utilise the following methods:

- Presentations
- Demonstrations
- Individual & Group work
- Discussions

13. Assessment

Coursework (60%)
[Quizzes 20%]
[Mid Semester Exam 10%]
[Project and Presentation 30%]

Final Examination (40%)

14. Course Evaluation Approaches Formative and Summative

15. Required Readings Schneider, Gary, "Electronic Commerce", Ninth Edition, Thomson Course Technology 2010

16. Course Calendar

Week 1 & 2 **Introduction to Electronic Commerce**

The students will be able to;

- Describe the advantages and disadvantages of E-Commerce
- Identify various opportunities for Electronic commerce opportunities.

Content

- Advantages and Disadvantages
- Identifying Electronic Commerce Opportunities

Week 3 & 4 The Internet and the World Wide Web

Students will be able to;

- Learn the various internet protocols
- Identify and discuss the various markup texts on the web

Content

- Internet Protocols
- Mark-up Languages and the Web

Week 5 Revenue Models and Building a Web Presence

Students will be able to ;

- Identify measures which can be implemented for easy website navigation

Content

- Revenue Strategy Issues
- Web Site Usability

Week 6 Marketing on the Web

Students should be able to;

- Identify web marketing strategies which can be implemented

Content

- Web Marketing Strategies
- Search Engines and Web Directories

Week 7

- Mid Semester Exam

Week 8 **Legal, Ethical and Tax Issues**

Students should be able to;

- Identify the various legal, ethical and tax issues with regards to Electronic Commerce.

Content

- Intellectual Property
- Internet Crime

Week 9 **Web Server Hardware and Software**

Students should be able to;

- Identify and explain the hardware and software necessary for a web server

Content

- Software for Web Servers
- Web Server Hardware

Week 10 **Electronic Commerce Software**

The student should be able to;

- Identify E Commerce software
- Explain the functions of each aspect of the software

Content

• Basic Functions of Electronic Commerce Software

Week 11 **Electronic Commerce Security**

Students should be able to;

- Use the electronic commerce software functionally

Content

• Basic Functions of Electronic Commerce Software

Week 12 **Electronic Commerce Security**

Students should be able to

- Discuss the necessary mechanisms that should be in place on the client computers and on the servers to ensure that transactions are safe
- Be able to implement policy and software to secure the servers and computers.

Content

- Security for Client Computers
- Security for Server Computers

Week 13 **Payment Systems**

The student should be able to ;

- Identify the various online payment options
- Identify the structure of the online payment facilities

Content

- Online Payment Basics
- Phishing and Identity Theft

Week 14 **Planning for Electronic Commerce**

Students will be able to;

- Identify practical examples from research done on strategies for developing E- Commerce websites.

Content

Strategies for Developing E-Commerce Web Sites

Week 15	Final Exam

17.	**Pre-requisites**	Basic knowledge on operating systems and C programming skills
18.	**Co-requisites**	None
19.	**Post-requisites**	None
20.	**Forbidden Combinations**	None
21.	**Academic staff member who may be contacted for more information:*****	

1. **Course title:** **Fundamentals of Networking 1**

2. **Course code**: **IT 105-1**

3. **Course Provider**: SVG Community College: Department of Computer Science – Division of Arts, Science and General Studies

4. **Level**: **First year course**

5. **Semester in which**

it will be offered: Semester **1**

6. **No. of credits**: 5

7. **Total study hours**: Includes:45

- teaching time
- study time
- a student’s preparation time for classes

8. **Course Description**** **IT105-1** Introduces students to data communication and computer networking. It provides opportunities to develop deeper understandings of network technologies, media, topologies and devices, than they would have encountered during CSEC. It focuses on basic network management tools, data communication and network security.

9. Course Rationale: This course has been included in the programme of study of the SMART Project Cyber Security Associate degree programme because it provides instruction that equips students with the basic skill set that they will need to understand the role of networks and how they impact cyber security. The content knowledge therein presents students with the skills necessary to succeed in Caribbean networking-related degree programs and helps them prepare for external certification.

10. Learning Outcomes:

- Apply common networking terms.

- Determine reasons to create an onsite network for a company.
- Identify the layers and functions of the OSI model.
- Write cabling specifications for a given project.
- Name the various types of network topologies and the advantages and disadvantages of each.
- Identify telecommunications network components.
- Calculate bandwidth needs for wide area networks.
- Describe how information travels through the network.
- Design a wide area network using existing hardware components.
- Summarize common network protocols.
- Justify a remote access solution.
- Outline the pros and cons of various network design techniques.
- Prepare a comprehensive network design plan

11. Content:

- Overview of Networks and Terminology
- Network layers and functions of the OSI model Network Topologies:
- Network Design Techniques:
- Wide Area Network Equipment:
- Wide Area Network Design:

12. Teaching Methodology Classroom discussions, lectures, films, texts, practical, supplied readings and internet use (video clips, research medium).

13. Assessment Students will complete a course work assignments, a project and a final exam. Each exam will consist of questions based on material covered both in the textbook chapters, lecture material and class discussion. The coursework is 60% of the grade while the final is the remaining 40%.

(i)Assessed coursework

Coursework (60%)

[Written assignments 30 marks]

[Project 30 marks]

Examination (40%)

14. Course Evaluation Practical, Formative and summative

Approaches

15. Required Readings

Text: Muller, S., & Ogletree, W. T. *Upgrading and repairing of networks (*latest edition.). Que Books..

16. Course Calendar

Week 1 & 2: Overview of Networks and Terminology

Students will be able to;

- Have a full understanding of networking principles
- Understand the commonly used terminologies in networking

Content

- Common networking terms

- Local area network

Week 3 - 5 : Network layers and functions of the OSI model network topologies

Students will be able to;

- Understand the specifications of the different hardware necessary for networking.

Content

- Cabling specifications
- Type of network topologies

Week 6 - 8: Network Design Techniques

Students will be able to;

- Outline the various techniques available for the development of a network design
- Differentiate between each type of design

Content

- The pros and cons of various network design techniques
- Network design plan

Week 9 - 11: Wide Area Network Equipment

Students will be able to;

- Identify bandwidth needs and the components necessary for a network

Content

- Telecommunications network components
- Bandwidth needs for wide area networks

Week 12 - 14: Wide Area Network Design

Students will be able to;

- Outline the principles of network communication

Content

- Principles of Network Communication
- Wide Area Network hardware components

Week 15. Final Exam

Pre-requisites	none
Co-requisites	None
Post-requisites	None
Forbidden Combinations	None
Academic staff member who may be contacted for more information:*	

1. **Course title:** **Fundamentals of Networking 2**

2. **Course code**: **IT 105-2**

3. **Course Provider**: SVG Community College: Department of Computer Science – Division of Arts, Science and General Studies

4. **Level**: **First year course**

5. **Semester in which it will be offered :** Semester 2

   Provided across Departments/Faculties

6. **No. of credits**: 5

7. **Total study hours**: Includes 45 hours:
   - teaching time
   - study time
   - a student's preparation time for classes

8. **Course Description**** **IT105-2** introduces students to data communication and computer networking. It provides opportunities to develop deeper understandings of network technologies, media, topologies and devices, than they would have encountered during CSEC. It focuses on basic network management tools, data communication and network security.

9. **Course Rationale:** This course has been included in the programme of study of the SMART Project Cyber Security Associate degree programme because it provides instruction that equips students with the basic skill set that they will need to understand the role of networks and how they impact cyber security. The content knowledge therein presents students with the skills necessary to succeed in Caribbean networking-related degree programs and helps them prepare for external certification.

10. **Learning Outcomes**:

- Determine common applications that business users require in a networked office.
- Summarize remote access techniques.
- Justify a remote access solution.
- Analyze basic network security principles.
- Assess potential solutions for disaster recovery.
- Describe different backup and disaster recovery solutions.
- Prepare a backup and disaster recovery plan.

11. **Content**:

- Business Uses for Networks:

- Common applications in a networked office Network Remote Access:
- Securing the Network
- Backup and Disaster Recovery

12. Teaching Methodology Classroom discussions, lectures, films, texts, practical, supplied readings and internet use (video clips, research medium).

13. Assessment Students will complete a course work assignment, a midterm, and a final exam. Each exam will consist of questions based on material covered both in the textbook chapters, lecture material and class discussion. **Exams** (midterm and final) comprise a total of **75%** of the final mark, while the **assignment** will contribute the last **25%** of the final mark.

(i)Assessed coursework

Coursework (60%)
[Written assignments 30 marks]
[Project 30 marks]
Examination (40%)

14. Course Evaluation Practical, Formative and summative

Approaches

15. Required Readings

Text: Muller, S., & Ogletree, W. T. (2006). *Upgrading and repairing of networks (*5th ed.). Que Books..

16. Course Calendar

Teaching Schedule

N.B. Most chapters, unless otherwise specified, are taken from Muller & Ogletree (2006).

Week 1 - 3 : Business Uses for Networks

Students will be able to;

- Explain the use of networks in a business environment

Content

- Common network protocols

Week 4 – 5 : Common applications in a networked office Network Remote Access

Students will be able to;

- Identify applications used in the office
- Be able to set up a VPN

Content

- Remote Access techniques
- Remote access solutions

Week 6 - 9: Securing the Network

Students will be able to;

- Understand the principles of network security
- Be able to ensure that a network is secured with the use of various hardware and software
- Be able to detect intrusion attempts on the network

Content

- Basic network security principles
- Potential solutions for disaster recovery

Week 10-14: Backup and Disaster Recovery

Students will be able to;

- **Ensure measures are in place to recover deleted files or files lost through a disaster.**
- **Ensure that the information which is backed up is safe**

Content

- Backup and disaster recovery solutions
- Backup and disaster recovery plan.

Week 15. Final Exam

Pre-requisites	none
Co-requisites	None
Post-requisites	None
Forbidden Combinations	None

Academic staff member who may be contacted for more information:***

Course title: Technical Report Writing

2. **Course code**: **ENGL 124**

3. **Course Provider**: SVG Community College: Department of Computer Science – Division of Arts, Science and General Studies

4. **Level**: **First year course**

5. **Semester in which it will be offered :** Semester 2

   Provided across Departments/Faculties

6. **No. of credits**: 3

7. **Total study hours**: Includes 45 hours:
   - teaching time
   - study time
   - A student's preparation time for classes

8. **Course Description****

   This course provides students with a rich background of knowledge and adequate practice in the preparation and writing of contemporary forms of technical reports. There is a special unit in the course, which prepares students for making oral presentations of reports.

9. **Course Rationale:**

   Technical Report Writing is the practical writing that people in engineering and its related fields do as a regular part of their job. One of the most critical skills required in today's technical and vocational world is the ability to communicate effectively, both verbally and in writing. Effective communication, which is at the heart of technical report writing, has a direct impact on one's potential within an organization. Participation in such a course therefore, enhances the engineering students' potential to succeed in today's competitive world.

.

10. **Learning Outcomes**:

- Demonstrate an understanding and appreciation of the function of technical writing within the technical and vocational fields;
- Recognize and appreciate the variety of technical reports which persons in the technical engineering and allied fields use;
- Utilize a wide variety of styles and formats to prepare, plan and write effective technical reports; and Select, evaluate and apply a variety of oral presentation strategies to enhance students' ability to convince and persuade people to desired actions.
- At the end of the course students should be able to:
- Define the task involved in writing a technical report;

- Identify the major sections, which constitute a technical report;
- Identify and describe the parts of a technical report from beginning to end;
- Write effective summaries of technical reports;
- Use appropriate style for writing technical reports;
- Write various types of reports, Proposals, Specifications and Manuals
- Produce well written Proposals, Specifications and Manuals;

11. Content:

- Technical Reports in General
- Basic Computer Applications
- Proposal, Specifications and Manuals
- Special Reports
- Oral Presentations

12. Teaching Methodology Lecture; discussions; audio and video tape evaluation; student presentations; group projects; home assignments.

13. Assessment This course will be assessed using continuous assessment and a final examination. The Continuous assessment will contribute 40 percent of the total assessment, while the final examination will contribute 60 percent. The continuous assessment will be based on class tests, home assignments, and student presentations and student class participation.

(i)Assessed coursework

Coursework (60%)
]
Examination (60%)

14. Course Evaluation Practical, Formative and summative

Approaches

15. Required Readings

Text:

- Riordan, Daniel and Pauley, Steven E. (2004) Technical Report Writing Today, Wadsworth Publishing.

- William Sabin (2004)The gregg reference manual, Mc. Graw Hill Shelly, Gary B., Cashman, Thomas J., Starks, Joy L. (2007) Microsoft Office Publisher 2007: Complete Concepts and Techniques, Course Technology; 1St edition.
- Jerry Joyce, Jerry & Moon, Marianne (2007) 2007 Microsoft Office System Plain and Simple, Microsoft Press, First Edition

16. Course Calendar

Week 1 - 2 : Technical Reports in General

Students should be able to;

- Understand the need for technical report writing
- Identify and explain the various types of report
-

Content

Defining the Task - Subject, aim, readership

- Structure - Numbering, headings and subheadings
- Beginning and end - -Title page, summary, contents, introduction, body, conclusions and recommendations, references, appendices Style -Words (spelling, use, meaning), Sentences (formation, punctuation), Grammar and style
- Summaries - Techniques
- Appearance - Covers and binding
- Types of Reports -Visit reports, fieldwork reports, test/investigation reports, feasibility study reports, design reports, progress report

Week 3 – 4: Basic Computer Applications

- Overview of the computer
- Applications – Word processing, spread sheets
- Microsoft Office applications
- Special features

Week 5 - 6: Proposal, Specifications and Manuals

- Proposals -Problem definition, objectives, proposed solutions, benefits, programme and resources, cost.
- Specifications
- Manuals -Planning and writing

Week 7: Assessment

Week 8 - 9: Special Reports

- Planning
- Contents – Relevance of Projects, Aims, Theory, Previous Work, Analysis, Conclusions and Recommendations, Appendices
- Writing – Level, General Style, What was done
- Technical Information

Week 10 - 11: Special Reports Continued

References - Purposes of references:

- To support a statement
- To show how your work relates to other people's
- To allow your readers to find more information on publications to which you refer

- To acknowledge your sources
- Method of referencing - Journal article, book, contribution in book, paper proceedings, report, thesis, Quoting (spacing)

Week 12 - 13: Oral Presentations

- State of mind
- Visual Aids – Multi-media projector, Slide and other projectors, Video
- Preparing - Notes, preparing content, planning visual aids, practicing
- Giving the Presentation - Basics, using visual aids, timing and pausing, style, group presentations, answering questions.

Week 14. Review

Week 15 Final Exam

Pre-requisites	none
Co-requisites	None
Post-requisites	None

Forbidden Combinations None

Academic staff member who may be contacted for more information:***

Course title: **Database Management System**

2. **Course code**:

3. **Course Provider**: SVG Community College: Department of Computer Science – Division of Arts, Science and General Studies

4. **Level**: **First year course**

5. **Semester in which it will be offered :** Semester 2

   Provided across Departments/Faculties

6. **No. of credits**: 3

7. **Total study hours**: Includes:
   - teaching time
   - study time
   - A student's preparation time for classes

8. **Course Description**** Students will be exposed to database concepts including functional dependencies, SQL and normalization. Emphasis will be placed on the creation and manipulation of databases using MYSQL particularly to support the back end of web development, building on the foundation covered in the Webpage Design and MIS courses.

9. Course Rationale: Database management systems are standard tools that enable the storage and retrieval of data within modern information systems. Courses that introduce database concepts are now an accepted part of most computer science programs. The content within this advanced course deals with the implementation aspects of relational systems, and tests the students' knowledge of the current enhancements to relational database systems and object-oriented database systems.

.

10. Learning Outcomes:

- Overview of Databases
- Database Management System overview
- The traditional/file oriented approach
- The database approach
- Advantages of databases

11. Content:

- Overview of Databases
- The Relational Model
- Database Design Methodology
- Detailed Logical Design
- Structured Query Language SQL using MySQL
- Distributed Databases
- DBMS Features and Security Issues
- Roles of Database Personnel

12. Teaching Methodology Lecture; discussions; audio and video tape evaluation; student presentations; group projects; home assignments.

13. Assessment This course will be assessed using continuous assessment and a final examination. The Continuous assessment will contribute 40 percent of the total assessment, while the final examination will contribute 60 percent. The continuous assessment will be based on class tests, home assignments, and student presentations and student class participation.

(i)Assessed coursework

Coursework (60%)

Examination (40%)

14. Course Evaluation Practical, Formative and summative

Approaches

15. Required Readings

Text:

- Material/Bibliography
- Hoffer, J.A., Prescott, M., & Topi, H., (2008) Modern database management. (9th ed.)
- NJ: Prentice Hall.
- Reading List
- Date, C. J., (2003) An introduction to database systems. (8th ed.). NJ: Addison Wesley.
- Shah, N., (2004) Database systems using oracle. (2nd ed.). NJ: Prentice Hall.
- Elmasri, R & Navathe, S. (2007) Fundamentals of database systems (5th ed.). NJ: Prentice Hall.

16. Course Calendar

Week 1 : Overview of Databases

- Database Management System overview
- The traditional/file oriented approach
- The database approach
- Advantages of databases

Week 2: Database Concepts

- Basic Concepts – character, field, record, table/file, database, Database Management System, primary key, foreign key, secondary key, composite key, super key, candidate key
- Relational Algebra Operators: Select, Project, Join
- Components of a DBMS – DDL, DML, Query Language, Report Generator

- The different types of databases – hierarchical, network, relational, object-oriented, object-relational

Week 3: Database Life Cycle

- The Database Management System Life Cycle - Database Analysis, Database Design, Database Implementation, Database Testing and Evaluation, Operation, Database Maintenance
- Database Design – Conceptual versus Logical versus Physical
- Identification of User Views
- Entity- Relationship Diagrams, entity/relation, attribute, relationships, cardinality

Week 4: Lab Exercise

- Entity and Referential Integrity
- Physical Database Design: tables, primary keys, foreign keys
- Top-down versus Bottom-up Design: use of both approaches for correct, complete result
- Functional Dependencies
- 1st , 2nd , 3rd Normal Forms
- Relational Schema
- Update and Delete Data Anomalies

Week 5: Relational DMLs and DDLs

- The role of Relational DMLs and DDLs.
- Introduction to Relational algebra – Simple projection, selection, difference, renaming, union, intersection, division, join (natural, equi, inner, outer) and Cartesian product.
- Installation of MySQL
- Basic Rules for SQL Statements
- SQL Commands - CREATE TABLE (using constraints – primary key, foreign key)

Week 6: Relational DMLs and DDLs Continued

- ALTER TABLE, INSERT, SELECT (using WHERE, GROUP BY, ORDER BY, HAVING, aggregate functions, logical operators, comparison operators), SELECT sub queries,
- UPDATE, DELETE, CREATE VIEW, CREATE INDEX,
- DROP TABLE, DROP VIEW, DROP INDEX,

Week 7: Grant and Revoke

- GRANT and REVOKE, COMMIT and ROLLBACK.
- Getting Multiple Columns
- DISTINCT and LIMIT
- Sorting Results

Week 8: Sort

- Sort Direction
- Advanced filtering
- Wildcards, functions, JOINS
- How Search Engines Work

Week 9: Grant and Revoke

- Characteristics of a distributed database
- Definition of logical database, local and global application, global intelligence
- Assessment of a distributed database versus a loose connection of independent site
- Work on Assignment (Supervised)

Week 10: Distributed databases

- Terms and concepts used in distributed databases – transparency, homogeneous versus heterogeneous distribution, fragmentation – vertical/horizontal, replication, and allocation
- Advantages and disadvantages of a distributed database

Week 11: Data

- Data mart
- Data warehouse
- Differences between data warehouse and operational database
- On-line analytical processing
- Data mining
- Transactions – Atomic, Consistent, Isolated, Durable (ACID)
- Concurrency control

Week 12: Database Dictionary

- The role of the Data Dictionary, maintenance
- Database protection methods - backup and restore methods.
- Integrity Preservation – keys (primary and foreign), data validation, authority levels
- Security Control – unauthorized access and use, encryption, anti-virus, firewall, SQL views

Week 13: Database Modellers

- Data modellers, Business Analysts, Database Designers, Systems Analysts, Programmers and Database Administrators.
- The Database Administrator
- Selection, installation and maintenance of DBMS

- Training
- Work on Assignment (Supervised)

Week 14. **Review**

Week 15 Final Exam

Pre-requisites	none
Co-requisites	None
Post-requisites	None
Forbidden Combinations	None
Academic staff member who may be contacted for more information:***	

Course title: **Data Security Concepts**

2. **Course code**:

3. **Course Provider**: SVG Community College: Department of Computer Science – Division of Arts, Science and General Studies

4. **Level**: **First year course**

5. **Semester in which it** Semester 2

   will be offered : Provided across Departments/Faculties

6. **No. of credits**: 3

7. **Total study hours**: Includes:
   - teaching time
   - study time
   - A student's preparation time for classes

8. **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.

9. **Course 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 work covered in IT107, 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.

.

10. Learning Outcomes:

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

11. Content:

- Securing Information
- Counteracting Social Engineering Exploits
- Identifying Security Measures
- Maintaining File Security
- Guarding Against Attacks
- Handling Security Breaches
- Network Defense

12. Teaching Methodology Lecture; discussions; audio and video tape evaluation; student presentations; group projects; home assignments.

13. Assessment This course will be assessed using continuous assessment and a final examination. The Continuous assessment will contribute 40 percent of the total assessment, while the final examination will contribute 60 percent. The continuous assessment will be based on class tests, home assignments, and student presentations and student class participation.

(i)Assessed coursework

Coursework (60%)

Examination (40%)

14. Course Evaluation Practical, Formative and summative

Approaches

15. Required Readings

Text:

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.

16. Course Calendar

Week 1: Securing Information

- Understand Information Security
- Implement Physical Security Measures
- Identify the Need for Cyber Securities

Week 2-3: Counteracting Social Engineering Exploits

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

Week 4-5: Identifying Security Measures

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

Week 6-7: Maintaining File Security

- Implement Security in Windows Vista
- Back up Data
- Restore Data
- Dispose of Computer Information1st , 2nd , 3rd Normal Forms

Week 8-9: Guarding Against Attacks

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

Week 10-11:. Handling Security Breaches

- Identify Incidents
- Respond to Incidents

Week 11-12: Network Defence

- Network Defence Fundamentals
- Security policy Design & implementation
- Network Traffic signatures
- Firewalls-Designing and choosing
- Firewalls-Deploying and operating

Week 13: Network Defence

- Intrusion Detection systems (IDS)
- Intrusion Detection and Incident Response

- Virtual Private Network (VPN) Concepts
- VPN Implementation

Week 14. Review

Week 15 Final Exam

Pre-requisites	none
Co-requisites	None
Post-requisites	None
Forbidden Combinations	None
Academic staff member who may be contacted for more information:***	

Course title: Fundamentals of Programming and Problem Solving

2. **Course code**:

3. **Course Provider**: SVG Community College: Department of Computer Science – Division of Arts, Science and General Studies

4. **Level**: **First year course**

5. **Semester in which it** Semester 2

   will be offered : Provided across Departments/Faculties

6. **No. of credits**: 3

7. **Total study hours**: Includes:

   - teaching time
   - study time
   - A student’s preparation time for classes

8. **Course Description**** This course introduces the fundamentals of computer programming and problem solving. It provides basic instructions on the process of problem solving, and deep exploration of fundamental computer-related problem solving techniques such as flowcharting, pseudo code and algorithms. It introduces students to the syntax of the C++ programming language, and provides them with opportunities to use this language to generate solutions to real organisational and societal problems

9. **Course Rationale:** The mass production of computers and constant reduction in their cost has given more people access to computer technology in their homes, schools and places of work. The prevalence of computer communication hardware

in developed and developing societies have given far more people access to powerful computers, in the form of desktops, laptops, handhelds, and notebooks, than was the case a decade ago. Yet, the myth surrounding the complexity of the matter of programming has kept many brilliant Caribbean scholars from pursuing programming as a business. Hence, Caribbean nationals remain more interested in being end-users rather than developers of computer programs. This course seeks to change the skills set of the Caribbean Associate degree graduate by providing all ICT majors with the building blocks of problem solving and programming in C++. It provides the right instructional conditions to develop, in students, programming skills that will enable them to create original computer programs that are solutions to problems that are unique to us in the Caribbean. The course content challenges students to use their natural talents and creative powers to apply more imagination to the problems that exist among Caribbean societies. Thus, we hope that knowledge that is gained from this course will not only stimulate the student's interest in pursuing a career in programming, but provide adequate foundational skills that enable those who choose to do additional programming courses to master them, and those who choose to pursue program development as a career to be exceptional creative programmers.

10. Learning Outcomes:

On completion of this course students should be able to:

- Describe the basic control structures in C++
- Apply the principles of flowcharting to the software develop cycle.
- Create pseudo codes for real life problems and use to develop algorithms.
- Use abstraction to create Computer Software in an efficient manner.
- Analyze the features of one high level language to determine its constructs and program structure.
- Describe data types and structures for computer representation.
- Evaluate the functions and subroutines that are embedded in the C++ programming a language
- Write a simple program in C++ and use it to make decisions.
- Explain Event Driven Programming and Object Oriented Programming methods

11. Content:

- An Overview of Programming Technologies
- Introduction to programming language-independent analysis and the problem solving process.
- Fundamentals of Programming Languages
- Programming languages
- Programming in C ++:
- Basic Control Structures of C++
- Assignment operators
- Logical operators
- Structured Programming Summary

- Functions
- Arrays
- Pointers and strings
- Classes and data abstractions

12. Teaching Methodology Lecture; discussions; audio and video tape evaluation; student presentations; group projects; home assignments.

13. Assessment This course will be assessed using continuous assessment and a final examination. The Continuous assessment will contribute 60 percent of the total assessment, while the final examination will contribute 40 percent. The continuous assessment will be based on class tests, home assignments, and student presentations and student class participation.

(i)Assessed coursework

1 Coursework (60%)

- Programming Assignment [20 marks]
- Programming Project [40 mark]

2. Examination (40%)

14. Course Evaluation

Practical, Formative and summative

Approaches

15. Required Readings

Text:

Zak, D. (2009). An introduction to programming with C++. Custom fifth edition, Course Technology.

16. Course Calendar

Week 1-2 : An Overview of Programming Technologies

- Machine Languages
- Assembly Language and high level languages
- Structured Programming
- Software Trends: Object Technology
- Hardware Trends

Week 3: Introduction to programming language-independent analysis and the problem-solving process.

- Flowcharting
- Algorithms
- Pseudo codes

Week 4: Fundamentals of Programming Languages

- High level languages
- Procedural Programming language constructs, conditional branching, looping
- Data Types
- Operators
- Functions and Subroutines
- Event Driven Programming, Object Oriented Programming

Week 5: Programming languages

- Popular Languages: C, C++, Visual BASIC and Java;
- Mark-up Languages: HTML & XTML.

Week 6: Programming in C ++:

- The Basics of a typical C ++ environment
- Writing a simple program
- Printing one line of text
- Adding two integer
- Memory concepts
- Arithmetic
- Decision-making- Equalities and relational operators

Week 7: Basic Control Structures of C++

- Algorithms
- Formulating algorithms
- Formulating algorithms with top down and stepwise refinement
- Pseudo code
- If Selection structure
- If/ else selection structures
- While repetition structure:
- Increment and decrement operators
- Logical operators
- Functions
- Arrays
- Pointers and strings
- Classes and data attributes
- Operator overloading
- Inheritance

Week 8: Assignment operators

- Increment Operators
- Recrement operators

Week 9: Logical operators

- Confusing equalities (= =)
- Assignment (=) operators

Week 10: Structured Programming Summary

Week11: Functions

- Programme components of C++
- Math Library functions
- Function Definitions
- Function prototypes

Week 12: Arrays

- Elements Arrays
- Static Arrays

Week 13: Pointers and strings

- Referencing variables
- Printing a string

Week 14: Classes and data abstractions

- Creating a structure
- Setting structure members
- Printing structure
- Utility functions
- Constructors and default arguments

Week 15 Final Exam

Pre-requisites	none
Co-requisites	None
Post-requisites	None
Forbidden Combinations	None

Academic staff member who may be contacted for more information:***

Course title: **Ethics and IT Law**

2. **Course code**:

3. **Course Provider**: SVG Community College: Department of Computer Science – Division of Arts, Science and General Studies

4. **Level**: **First year course**

5. **Semester in which it Will be offered:** Semester 2

   Provided across Departments/Faculties

6. **No. of credits**: 3

7. **Total study hours**: Includes:
   - teaching time
   - study time
   - A student's preparation time for classes

8. **Course Description**** A study of the impact of the technological revolution on our Privacy; digitized information and legal and ethical issues Surrounding computer technologies in the global marketplace

9. **Course Rationale:** Computer scientists need to practice with a high level of ethics since there are so many grey areas in this field especially as it relates to the use of the Internet. This course will bridge the divide which exist.

10. **Learning Outcomes**:

On completion of this course students should be able to:

- Define what a profession is and why society regulates professions
- Identify options to solving ethical issues by applying various ethics theories
- Identify specific legal issues related to professional and personal life.
- Apply legal principles to create resolutions to issues

11. Content:

- **Introduction**:
- **Professions and Professionalism**
- **Ethics and Information Technology**:
- **Ethics and Engineering**
- **Framework of the Legal and Court System**:
- **Framework of the Legal and Court System**
- **Contracts**
- **Tort Law and Negligence**
- **Remedies Law**
- **Contracts and Torts in IT Practice**
- **Contracts and Torts in General Engineering Practice**:
- **Business Organizations and Miscellaneous Legal**

12. Teaching Methodology Lecture; discussions; audio and video tape evaluation; student presentations; group projects; home assignments.

13. Assessment This course will be assessed using continuous assessment and a final examination. The Continuous assessment will contribute 20 percent of the course work of which a midterm exam will be graded at 50%, while the final examination will contribute 50 percent. The continuous assessment will be based on class tests, home assignments, and student presentations and student class participation.

(i)Assessed coursework

1 Coursework (50%)

- Assessment [20 marks]
- Midterm [30 mark]

2. Examination (50%)

14. Course Evaluation Practical, Formative and summative

Approaches

15. Required Readings

Text:

Sara Baase A Gift of Fire: Social, Legal, and Ethical Issues for Computers and the Internet, latest Edition, Prentice Hall, ISBN: 0130082155

Reference:

M. David Ermann, Michele S. Shauf; Computers, Ethics, and Society latest Edition, Oxford University Press, ISBN: 0195143027

16. Course Calendar

Week 1: Introduction

Introduction:

This unit will provide a setting for the entire course. Using the Quebec Bridge case as an illustration, students will be introduced to many of the concepts to be dealt with in greater detail later in the course. Specifically, they will understand the impact that engineering decisions can have on society and individuals as well as some of the concepts of ethics and professional responsibility

Week 2: Professions and Professionalism

The definition of a profession is explored with the connected question: Why does society regulate professions? The session then moves to the question of how is a profession regulated and the tools that are used to effect such regulation. These include Codes of Conduct, Disciplinary Committees and public complaints processes.

Week 3: Ethics and Information Technology:

This session moves to the study of Ethics. Unlike most engineering courses, we discover that ethics is more related to philosophy rather than science. We consider different approaches to ethics and then, with respect to Information technology, we consider each of the following issues: Privacy; Risks; Intellectual Property;

Week 4: Ethics and Engineering

The previous unit deals with ethical issues as categories. This unit now moves to a more practical consideration of how to deal with such questions in practice. We will devise an approach to solving ethical problems and then examine problems in: Employment; Management and Consulting engineering

Week 5: Framework of the Legal and Court System

The course now shifts to legal issues. This unit provides an introduction to the structure of law making and the court system in in the Caribbean and the Americas. We also examine a number of specific issues including: Limitation periods; Alternative dispute resolution; and International law issues

Week 6: Contracts

This unit and the next deal at length with two separate legal regimes that have a large amount of applicability to engineering practice. In this unit on Contracts, we begin by examining how contracts are formed and issues related to that such as the Statute of Frauds requiring certain types of contracts to be in writing. We also deal with the application of contracts and the issue of misrepresentations and how the law deals with those. Finally, the issue of the discharge and breach of contracts is covered.

Week 7: Mid-term exam

Week 9: Tort Law and Negligence

The law of torts or wrongs underlies professional liability. This unit will provide students with the background on torts including an in depth review of the rules of negligence.

Week 10: Remedies Law

Once the law of torts and contracts has been covered, the analysis then turns to the law of remedies: what happens when there has been a tort or the breach of a contract. We will also examine the interaction and how the same action might create liability under both tort and contract law. An examination of the law of fundamental breach is also given together with coverage of the issue of waiver clauses.

Week11: Contracts and Torts in General Engineering Practice:

Contracts between engineers and their client are covered in this unit. Broader than the information technology area, contracts that are found in other engineering domains will be covered. In the construction area, the types of standard contracts that engineers use will be covered together with the issue of performance bonding. Other domains such as consulting and employment contracts will also be considered.

Week 12 -13: Business Organizations and Miscellaneous Legal Topics

There are many different legal forms that a business can take. This unit will examine each of those different forms emphasizing information that students may need if they are looking to form their own business. Then some miscellaneous types of legal issues of interest to the engineering profession will be covered. These topics include workers' liens, intellectual property, and environmental protection legislation. There will also be a pre-exam review of the material covered.

Week 14: Review

Review

Week 15 Final Exam

Pre-requisites	none
Co-requisites	None
Post-requisites	None
Forbidden Combinations	None
Academic staff member who may be contacted for more information:*	