Course Name: **Computer Security**
Course Code: **GCS1112**
Year of Study: **1**
Semester: **1**
Contact Hours: **45**
Credit Units: **3**

Description
This course provides the foundation for understanding the key issues associated with protecting information assets, determining the levels of protection and response to security incidents, and designing a consistent, reasonable information security system, with appropriate intrusion detection and reporting features.
The purpose of the course is to provide the student with an overview of the field of computer security.

Students will be exposed to the spectrum of security activities, methods, methodologies and procedures.

Course Objectives
This Course aims at:
i) Identify and prioritize information assets
ii) Identify and prioritize threats to information assets
iii) Define an information security strategy and architecture
iv) Plan for and respond to intruders in an information system
v) Present a disaster recovery plan for recovery of information assets after an incident
vi) Describe legal and public relations implications of security and privacy issues.

Course Learning Outcome
i) Upon completion of this course, the students will acquire knowledge that will enable them to:
ii) Describe the functioning of various types of malicious code, such as viruses, worms, trapdoors.
iii) Enumerate a set programming technique that enhances security.
iv) Explain the various controls available for protection against internet attacks, including authentication, integrity check, firewalls, and intruder detection systems.
v) Describe the different ways of providing authentication of a user or program.
vi) Describe the mechanisms used to provide security in programs, operating systems, databases and networks.
vii) Describe the background, history and properties of widely-used encryption algorithms such as DES, AES, and RSA

Indicative Content

No.	Content	Contact Hours
1.	**Basic Computer Security Concepts** Threats, vulnerabilities, controls; risk; confidentiality, integrity, availability; security policies, security mechanisms; assurance; prevention, detection, deterrence.	4 Hours

2.	**Basic Cryptography** Basic cryptographic terms; historical background; symmetric crypto primitives; modes of operation; cryptographic hash functions; asymmetric crypto primitives.	5 Hours
3.	**Program Security** Flaws (malicious code - viruses, Trojan horses, worms; program flaws - buffer overflows, time-of-check to time-of-use flaws, incomplete mediation); defences (software development controls, testing techniques).	5 Hours
4.	**Security in Conventional Operating Systems** Memory, time, file, object protection requirements and techniques; protection in contemporary operating systems; identification and authentication - identification goals, authentication requirements, human authentication, machine authentication.	6 Hours
5.	**Trusted Operating Systems** Assurance; trust; design principles; evaluation criteria; evaluation process.	4 Hours
6.	**Database Management Systems Security** Database integrity; database secrecy; inference control; multilevel databases.	6 Hours
7.	**Network Security** Network threats (eavesdropping, spooling, modification, denial of service attacks); introduction to network security techniques (firewalls, virtual private networks, intrusion detection).	6 Hours
8.	**Management of Security** Security policies; risk analysis; physical threats and controls.	5 Hours
9.	**Ethics, Social and Professional Issues** Legal aspects of security; privacy and ethics.	4 Hours
	TOTAL	**45 HOURS**

Study Material

Laptops with a modern operating system for which the student has administrator privileges, LCD projector, networking tools, printers and fast Internet.

Method of Delivery

This Course will be delivered primarily through the lecture method complemented by students' group discussions. In addition, case studies will be used to enhance the students' analytical and communication skills.

Method of Assessment
Assessment will be in terms of tests and practical exercises (40%) and annual examination (60%)

Reference Lists

1. Michael Goodrich and Roberto Tamassia (2010). Introduction to Computer Security. 1st ed., Addison Wesley.
2. Charles P. Peeger and Shari L. Peeger (2003). Security in Computing. 3rd Edition. Prentice Hall. ISBN: 0-13-035548-8.
3. Matt Bishop (2004). Introduction to Computer Security. Addison-Wesley Professional. ISBN-10: 0321247442, ISBN-13: 978-0321247445.
4. https://www.cs.utexas.edu/users/byoung/cs361/syllabus361.html

Course Name: **Fundamentals of Programming**
Course Code: **GCS1113**
Year of Study: **1**
Semester: **1**
Contact Hours: **60**
Credit Units: **4**

Description
The course introduces the fundamental concepts of procedural programming, including data types, control structures, functions, arrays, files, and the mechanics of running, testing, and debugging. The course also offers an introduction to the historical and social context of computing and an overview of computer science as a discipline.
Students should have sufficient foundation of high-school mathematics to solve simple linear equations and to appreciate the use of mathematical notation and formalism.

Course objectives
This course provides students with
i) Skills to produce algorithms for solving simple problems and trace the execution of computer programs.
ii) Constructing object-oriented, structured, and functional programming methodologies.
iii) Designing the language translation phases of compiling, interpreting, linking and executing, and differentiate the error conditions associated with each phase.

Course Learning Outcome
Upon completion of this course, the students will acquire knowledge that will enable them to:
i) Construct a simple program for solving simple problems and trace the execution of computer programs.
ii) Apply the program development process to problems that are structured, and functional programming methodologies.
iii) Decompose a program into subtasks and use parameter passing to exchange information between the subparts.