**THE UNIVERSITY OF THE WEST INDIES** 

**PROPOSAL FOR REVISED UNDERGRADUATE COURSE**

**Campus and Faculty: St. Augustine Campus, Faculty of Science and Technology School, Department, or Centre: Department of Computing and Information Technology Course Code and Title: INFO 2604, Information Systems Security**

**Semester and Level: Semester 2, Level 2**

**Pre-requisites: COMP 1602**

**Co-requisites: None**

**Anti-requisites: None**

**Course Type: Core**

**Credits: 3**

**Projected Enrolment: 100**

**Projected Start Date: January 2020**

**Mode of Delivery: Face-to-Face** ☑ **Blended** ❑ **Online** ❑

**1. Course Description**

This course introduces students to the area of Information Systems Security by building upon concepts explored in Computer Programming II. Concepts needed to manage the necessary processes that guarantee information assurance are explored such as operational issues, policies and procedures, attacks and defence mechanisms, risk analyses and information security theory.

**2. Rationale**

With the proliferation of online databases and networked systems, the security of a system’s infrastructure is important. This course provides students with an extensive understanding of information security management with an emphasis on network security. Whereas other courses provide an overview of the basics of the discipline, this course promotes awareness of information security as a simultaneously technical and managerial discipline with enterprise-wide implications for employees, operations and systems at every level.

**3. Course Aims**

The primary aim of the course is to develop essential information security knowledge, awareness and skills in undergraduate students from theoretical, technical and business perspectives. This addresses the need for students to be able to articulate and apply practical solutions with a clear understanding of the implications of specific recommendations and policies for business settings.

**4. Course Learning Outcomes**

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

1. Explain the challenges and scope of information security

2. Apply basic security concepts which are used frequently in the field of information security: confidentiality, integrity, authentication, non-repudiation, authorization and availability 3. Evaluate cryptographic algorithms used in information security in the context of the overall information technology (IT) industry

4. Investigate mechanisms used for authentication

5. Configure a firewall to satisfy security policy goals

6. Formulate security policies for a given business scenario

7. Demonstrate interpersonal skills and teamwork group presentations.

8. Demonstrate effective written and oral communication techniques when completing reports and presentations.

**5. Course Content/Syllabus**

The following main topics are covered in this course:

1. Attacks, Threats, Vulnerabilities and Controls

2. Security Risk Model.

3. Authentication, Confidentiality, Integrity, Authorization, Availability and Non-Repudiation 4. Shared and Public Key Cryptography

5. Asset Management and Security Policies

**6. Teaching Methods**

This course will be delivered primarily through weekly interactive lectures, tutorials and lab activities. These are supplemented with lecture notes, handouts, case study documents and online quizzes and activities posted on myeLearning.

**7. Contact and credits hours:**

| **Type** | **Duration**  **(Number of weeks)** | **Contact Hours**  **(Weekly)** | **Credit Hours**  **(Weekly)** |
| --- | --- | --- | --- |
| Lecture | 13 weeks | 2 hours | 2 |
| Lab Tutorials | 13 weeks | 2 hours | 1 |
| **Total:** | 13 weeks | 4 hours | 3 |

**8. Course Assessments Description**

Assessments are designed to test student knowledge through written assignments, a coursework exam and a group project which requires research and preparation of strategies to address a particular topic or problem in information security.

There are four assessments in this course: 2 individual assignments, 1 group project, and one coursework exam.

**9. Course Assessment Type and Course Learning Outcome Matrix**

| **Assessment** | **Learning Outcomes** | | | | | | | | **Weighting %** | **Assessment**  **Description** | **Duration** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Assignment 1 |  |  | X |  |  |  |  |  | 5% | Algorithmic  Problems |  |
| Assignment 2 |  | X |  | X |  |  |  |  | 10% | Problems &  Short Answer  Questions |
| Group Project |  |  |  | X | X | X | X | X | 15% | Case Studies,  Project Report |
| CW Exam | X | X | X | X | X |  |  |  | 20% | Algorithmic and Scenario-based Problems, Short Answer  questions | 2 hours |
| Final  Examination | X | X | X | X | X | X |  |  | 50% | Algorithmic and Scenario-based Problems, Short Answer  questions | 2 hours |
| TOTAL % |  | | | | | | |  | 100% |  | |

**10. Readings/Learning Resources** *(Online and Print)*

*Required/Essential*

• Computer Security: Principles and Practice. 2018. William Stallings and Lawrie Brown • Unlocking the Mysteries of Information Security: Wayne Goodridge

**11. Staffing Requirements: 1 Lecturer, 1 Tutor, 1 Marker**

**12. Projected additional Cost (if any) for Proposed Undergraduate Course: None**

**13. Collaboration/ Consultation**

Academic staff from the Department of Computing and Information Technology were consulted on the proposal and full support was given for the changes to the curriculum.

**14. All relevant BUS Policies are available at: http://uwi.edu/undergraduatestudies/ default.aspx**

Have you taken these policies into account in the design of this Course? **Yes No \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Academic Staff Member / Contact Person Responsible/Coordinator**

Name: Dr. Wayne Goodridge Telephone: 868-662-2002 ext 85381

Email: wayne.goodridge@sta.uwi.edu

**Campus/Faculty/Department**:

**Date of Recommendation by Faculty Board/APAD:**

**Signature: Dean/Director\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: Department Head**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Checked and endorsed by:** ❑ Campus Bursary ❑ CETL ❑ Library ❑ Bookshop ❑ Faculties on other Campuses ❑ OOL ❑ Other \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ NB. Attach supporting documents as appendix e.g. CETL. Library, online checklist

**Course Calendar**

| **Week** | **Topics** | **Required**  **Readings**  **Learning**  **Resources** | **Learning Activities** | **Assessment** |  |
| --- | --- | --- | --- | --- | --- |
| **Topic** | **Date** |
| 1. | Security Goals  Passive/Active Threats | Selected  chapters  from  required  text,  Content  posted on  myElearning weekly | Face to  Face  Lectures, Lab  Tutorials |  |  |
| 2. | Shared key Cryptography, Caesar Cipher, Rail Fence, Encryption (DES) | Assignment 1  (Programming Ciphers) | Week 2 |
| 3. | Authentication, Hash  Functions, MACs |  |  |
| 4. | Biometric Authentication, Token Based Authentication, Single SignOn Systems and Key Distribution Centers |  |  |
| 5. | Public key Cryptography, RSA Algorithm |  |  |
| 6. | Digital Signatures, Message Digests, Certificates | Assignment 2  (Biometric Techniques) | Week 6 |
| 7. | Security in Internet Commerce |  |  |
| 8. | Revision | Coursework Exam  (Topics from Week 1-7) | Week 8 |
| 9. | Presentation of Biometric Techniques, VPNs |  |  |
| 10. | Firewalls and Packet Filters, Access Lists |  |  |
| 11. | Application Attacks: Input/ Output Validation, Exception Handling, Sign-On, Access Control, Library Linking, Configuration Management, Session Handling and Program Execution | Group Project  (Security Policies) | Week 11 |
| 12. | Risk Management – Assets & Vulnerabilities & Attacks, Presentation of Application Attacks |  |  |
| 13. | Course Review |  |  |  |  |