3.2.9 Bachelor of Computing in Information Security

Objective

The Bachelor of Computing in Information Security aims to:

- To provide a broad-based, inter-disciplinary information security undergraduate programme within NUS
- To contribute to the national focus on growing the pool of cyber security professionals in Singapore.
- To produce graduates who are able to understand information security issues and practices from both technical and organisational points of view.

Graduates of this programme are expected to have possible career choices as software engineers, systems administrators, malware researchers, security analyst, cybersecurity incident responder, and security consultant. They are expected to find employment in industries that deal with sensitive information (e.g., banks, insurance, defence), government organisations (e.g., CSIT, DSO, DSTA, MHA, Cyber Security Agency) and firms that provide security consultation/systems/services (e.g., Symantec, FireEye).

This programme enables students to attain, by the time of graduation:

1. Strong knowledge of computer science foundations and fundamentals, including (a) familiarity with common computer science themes and principles, (b) high-level understanding of systems as a whole, (c) understanding of the theoretical underpinnings of computer science and their influences in practice.
2. An ability to design, implement, and evaluate a computer-based system, process, components, or program to meet the security needs.
3. An understanding of the processes and challenges that support the delivery and management of information security in an organisation.
4. An ability to function effectively in teams to accomplish a common goal.
5. An understanding of professional, ethical, legal, security, and social issues and responsibilities.
6. An ability to communicate effectively with a range of audiences
7. An ability to analyse the local and global impact of computing on individuals, organisations, and society.
8. Recognition of the need for and an ability to engage in continuing professional development
9. An ability to use the current techniques, skills, and tools necessary for information security practice.

Degree Requirements

The Bachelor of Computing (Information Security) requires at least 160 MCs.

Students will be required to satisfy 12 MCs of industrial experience (mandatory requirement) by doing:

1. A 6-month internship through CP3880 Advanced Technology Attachment Programme (12 MCs)
2. Two 3-month internships through CP3200 Internship (6 MCs) and CP3202 Internship II (6 MCs).

3. IS4010 Industry Internship Programme (12 MCs) from the Department of Information Systems and Analytics.
4. A 3-month internship through CP3200 Internship (6 MCs) and CP3107 Computing for Voluntary Welfare Organisations (6 MCs).
5. iLead or NOC [1].
6. Other forms of industry experience approved by the Department of Computer Science.

1. **PROGRAMME REQUIREMENTS (Total of 108 MCs)**

Computing Foundation (36 MCs)

CS1010 Programming Methodology[2]
CS1231S Discrete Structures
CS2040C Data Structures and Algorithms
CS2100 Computer Organisation
CS2102 Database Systems
CS2105 Introduction to Computer Networks
CS2106 Introduction to Operating Systems
CS2113T Software Engineering & Object-Oriented Programming[3]
IS3103 Information Systems Leadership and Communication

Information Security Requirements (32 MCs)
CS2107 Introduction to Information Security
CS3235 Introduction to Computer Security
Either
IFS4205 Information Security Capstone Project; or
(CS4238 Computer Security Practice and IFS4103 Penetration Testing Practice)
IS4231 Information Security Management

Complete 12 MCs from the following list of modules:
CS3236 Introduction to Information Theory
either
CS4236 Cryptography Theory and Practice
or
MA4261 Coding and Cryptography
CS4238 Computer Security Practices
CS4239 Software Security
CS4257 Algorithmic Foundations of Privacy
CS5231 Systems Security
CS5321 Network Security
CS5322 Database Security

CS5331 Web Security
CS5332 Biometric Authentication
IFS4101 Legal Aspects of Information Security
IFS4102 Digital Forensics
IFS4103 Penetration Testing Practice
IS4204 IT Governance
IS4233 Legal Aspects of Information Technology
IS4234 Compliance and Regulation Technology
IS4302 Blockchain and Distributed Ledger Technologies
Other modules approved by the SoC UG Office

Computing Breadth (8 MCs)
Complete 8 MCs of CP-coded, CS-coded or IS-coded modules at level-3000 or above.

Industrial Experience Requirement

IT Professionalism (8 MCs)
IS1103/X IS Innovations in Organisations and Society
CS2101 Effective Communication for Computing Professionals

Mathematics (12 MCs)
MA1101R Linear Algebra I
MA1521 Calculus for Computing
ST2334 Probability and Statistics[4]

2. **UNIVERSITY LEVEL REQUIREMENTS (20 MCs)**

As specified in Section 3.2.1.

3. **UNRESTRICTED ELECTIVES (20 MCs)**

As specified in Section 3.2.1.

NUS Overseas Colleges (NOC) – Information Security

Students who attended NOC programme may :
1. count TR3201 Entrepreneurship Practicum (8 MCs) towards Computing Breadth.
2. count TR3202 Start-up Internship Programme (12 MCs) towards Industrial Experience Requirement.
3. count TR3203 Start-up Case Study and Analysis towards Unrestricted Electives. Students working

on information security-related projects for TR3203 may seek approval to instead take TR3203P, which counts towards IFS4205 Information Security Capstone Project requirement.

University Scholars Programme (Information Security)

Students in the University Scholars Programme who choose the Bachelor of Computing (Information Security) major will take the Information Security programme, but with the following variations:

1. They will read GER1000 Quantitative Reasoning (4 MCs) as compulsory module for the University Level Requirements (ULR). The remaining 16 MCs in ULR are replaced by the 3 USP Inquiry Modules and 1 USP Foundation module (i.e. University Scholars Seminar).
2. They will not be required to read CS2101 Effective Communication for Computing Professionals. It is replaced by USP Foundation module: Writing and Critical Thinking.
3. They will read IFS4205 Information Security Capstone Project, which is an 8-MCs independent study modules (ISMs) which will be counted as 2 USP Inquiry modules in Sciences and Technologies Basket.
4. They will further complete 3 more USP Inquiry modules (for a total of 8, including IFS4205) and the USP Reflection module (the Senior Seminar). They will have 16 MCs under the Unrestricted Electives.

Table 4: Summary of degree requirements for Bachelor of Computing (Information Security)

MODULES	MCS	SUBTOTALS
UNIVERSITY LEVEL REQUIREMENTS		**20**
PROGRAMME REQUIREMENTS		**108**

MODULES	MCS	SUBTOTALS
Computing Foundation	**36**	
CS1010 Programming Methodology [2]	4	
CS1231S Discrete Structures	4	
CS2040C Data Structures and Algorithms	4	
CS2100 Computer Organisation	4	
CS2102 Database Systems	4	
CS2105 Introduction to Computer Networks	4	
CS2106 Introduction to Operating Systems	4	
CS2113T Software Engineering and Object-Oriented Programming [3]	4	
IS3103 Information Systems Leadership and Communication	4	
Information Security Requirements	**32**	
CS2107 Introduction to Information Security	4	
Either IFS4205 Information Security Capstone Project; or (CS4238 Computer Security Practice and IFS4103 Penetration Testing Practice)	8	
CS3235 Introduction to Computer Security	4	
IS4231 Information Security Management	4	
Programme Electives Complete 12 MCs from the following list of modules: CS3236 Introduction to Information Theory Either CS4236 Cryptography Theory and Practice; or MA4261 Coding and Cryptography CS4238 Computer Security Practices CS4239 Software Security CS4257 Algorithmic Foundations of Privacy CS4276 IoT Security CS5231 Systems Security CS5321 Network Security CS5322 Database Security CS5331 Web Security CS5332 Biometric Authentication IS4204 IT Governance IFS4101 Legal Aspects of Information Security IFS4102 Digital Forensics IFS4103 Penetration Testing Practice IS4233 Legal Aspects of Information Technology IS4234 Compliance and Regulation Technology IS4302 Blockchain and Distributed Ledger Technologies Other modules approved by the SoC UG Office	12	
Computing Breadth	**20**	
Complete 8 MCs of CP-coded, CS-coded or IS-coded modules at level-3000 or above.	8	
Industrial Experience Requirement	12	
IT Professionalism	**8**	
IS1103/X IS Innovations in Organisation and Society	4	
CS2101 Effective Communication for Computing Professionals	4	
Mathematics	**12**	
MA1101R Linear Algebra I	4	
MA1521 Calculus for Computing	4	

MODULES	MCS	SUBTOTALS
ST2334 Probability and Statistics[4]	4	
UNRESTRICTED ELECTIVES[5]		**32**
Grand Total		**160**

[1] For students who opt for iLead or NOC, the additional MCs beyond the 12-MCs allocated to Industry Experience Requirement should be taken from Unrestricted Electives and/or exempted modules.

[2] CS1010 can be replaced by CS1101S Programming Methodology.

[3] Students taking CS2113T Software Engineering & Object-Oriented Programming must take CS2101 Effective Communication for Computing Professionals in the same semester.

[4] Students pursuing a Second Major in Mathematics or Statistics will take ST2131 Probability in place of ST2334 Probability and Statistics. The students will take ST2132 as a core module in the second major in Statistics programme and are highly encouraged to take ST2132 as an elective module in the second major in Mathematics programme. If a student who has already taken ST2131 quits the Second major in Mathematics or Statistics, he/she will have to take ST2132 to fulfil the BComp (Information Security) degree requirements.

[5] Students without A-level Mathematics are required to complete MA1301 or MA1301X Introductory Mathematics as part of the Unrestricted Electives.