3.3.5.4.3 Double Major in Information Security

The School of Computing offers a second major in Information Security (InfoSec) for non-SoC students.

Objective

The objectives for a Second Major in InfoSec are as follows:

To provide an information security programme within NUS for non-computing students;
To contribute to the national focus on growing the pool of cyber security professionals in Singapore; and
To produce graduates who are able to understand information security issues and practices from an inter-disciplinary point of view.

Student Learning Outcomes

The Second Major in InfoSec 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 ability to function effectively in teams to accomplish a common goal.
4. Recognition of the need for and an ability to engage in continuing professional development.
5. An ability to use the current techniques, skills, and tools necessary for information security practice.

Admission Requirements

For direct admission, students applying for the Second Major in InfoSec must meet the entry requirement:

For diploma holders: Diploma with at least an A2 grade in GCE O-level Elementary Mathematics or at least a B4 grade in GCE O level Additional Mathematics.
For A-Level Holders: H2 pass in Computing or Mathematics or Physics; OR a good pass in H1 Mathematics.

Existing students from cohort 2018/19 or later may apply into the Second Major in InfoSec after completing CS2040/C/S, and CS2107 with B+ or above in each of the modules.

Structure

The second major in InfoSec to be structured as follows:

Computing Foundation = 20 MCs
Information Security Foundation = 8 MCs
Capstone Project = 8 MCs
Information Security Electives = 12 MCs

In total, the 48 MCs requirement for graduation are broken down as follows:

Core modules = 36 MCs
Elective modules = 12 MCs

The table below shows the programme structure in details.

<table>
<thead>
<tr>
<th>Modules</th>
<th>MCs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computing Foundation</strong></td>
<td>20</td>
</tr>
<tr>
<td>CS1010 Programming Methodology or its equivalent</td>
<td>4</td>
</tr>
<tr>
<td>CS2040/C/S Data Structures and Algorithms</td>
<td>4</td>
</tr>
<tr>
<td>CS2100 Computer Organisation</td>
<td>4</td>
</tr>
<tr>
<td>CS2105 Introduction to Computer Networks</td>
<td>4</td>
</tr>
<tr>
<td>CS2106 Introduction to Operating Systems</td>
<td>4</td>
</tr>
<tr>
<td><strong>Information Security Requirements</strong></td>
<td>16</td>
</tr>
<tr>
<td>CS2107 Introduction to Information Security</td>
<td>4</td>
</tr>
<tr>
<td>CS3235 Computer Security</td>
<td>4</td>
</tr>
<tr>
<td>IFS4205 Information Security Capstone Project</td>
<td>8</td>
</tr>
<tr>
<td><strong>Information Security Electives</strong></td>
<td>12</td>
</tr>
</tbody>
</table>
Complete 12 MCs of modules from one of the following group, with at least 4 MCs at level-3000 or above.

**Group I: Data and Software Security**
- CS2102 Database Systems
- CS2113 Software Engineering & Object-oriented Programming
- CS4239 Software Security

**Group II: Foundation of Information Security**
- CS1231S Discrete Structures
- CS3236 Introduction to Information Theory
- CS4236 Cryptography Theory and Practice

**Group III: Information Systems and Security Management**
- IS1103/X IS Innovations in Organisations and Society
- IS3103 Information Systems Leadership and Communication
- IS4231 Information Security Management

### Grand Total

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>48</td>
</tr>
</tbody>
</table>

1. Students who are waived from completing CS1010 or its equivalent must complete another 4 MCs of modules listed under the Information Security electives.
2. **CS2100 Computer Organisation can be replaced by EE2024 Programming for Computer Interfaces or (EE2028 Microcontroller Programming and Interfacing and its prerequisite EE2026 Digital Design).**
3. EE3204/E **Computer Communication Networks I** or EE4204/E **Computer Networks** can be used in place of CS2105.
4. CG2271 **Real-Time Operating Systems** can be used in place of CS2106.
5. MA1100 and CS1231 can be used in place of CS1231S. Students without A-level mathematics are required to complete MA1301 **Introductory Mathematics** before completing CS1231.
6. MA42641 Coding and Cryptography can be used in place of CS4236

### Continuation and Graduation Requirements

The Second Major in InfoSec is a non-Honours major programme.

Students must complete CS2040/CS2040C, and CS2107 with a grade of at least B+ or above in each of the modules to continue the Second Major in InfoSec programme.

The Second Major in InfoSec will be awarded to students who completed the 48 MCs second major requirement. Students will need to complete the primary major requirements to graduate. Students who did not complete the Second Major in InfoSec requirement but completed the Minor in InfoSec requirement will be awarded the Minor in InfoSec.
Double Counting Framework for Double Major Programme

For 2014 cohort and beyond, 16 MCs of the 48-MC second major can be double counted with the primary major/programme requirements.