

## **DIPLOMA IN CYBERSECURITY & DIGITAL FORENSICS**

Mitigate cyber threats Singapore faces in our quest to be a smart nation. IT security professionals are in high demand to help Singapore succeed in this quest. With rapid growth in the area of Financial Technology, information security will be even more critical to protect our financial institutions, Join the fight against cybercrime with our Diploma in Cybersecurity & Digital Forensics (CSF).

In your first year, you will build a strong foundation in basic IT and security through modules such as Programming, Cyber Security Fundamentals, Front-end Development, Databases, Cryptography and Operating Systems Fundamentals.

In your second year, you will develop skills in the areas of network security, software security and digital forensics. You will learn to set up secure web servers, develop secure software applications and investigate cybercrimes. You will also learn how to secure codes and processes that go into developing applications, so that they are protected from external threats right from the start. This is called the Security Development Lifecycle, and is a highly valued skill in the industry.

In your final year, you will put your skills into practice by performing penetration tests on software, systems and networks, conducting in-depth forensic investigations on digital devices and networks, and analyzing malicious software or malware. You will get to do all these as well as work on information security projects in cutting-edge CSF labs.

What's more, you will attend masterclasses by information security professionals, and hone your skills in the real world with internships at the Ministry of Home Affairs and leading IT security organisations, such as Palo Alto Networks, SecureAge, Microsoft, NCS, CrimsonLogic, KPMG, Ernst & Young, CSIT and Ensign Infosecurity. You can also attain the highly sought-after CompTIA Security+ professional certification.

### **COURSE MODULES**

#### **LEVEL 1.1**

##### **Computing Mathematics**

This module introduces the basic concepts of relations and functions, matrices, statistical methods and relevant applications. The main emphasis is to develop students' ability in solving quantitative problems in computing mathematics, probability and statistics.

##### **Cyber Security Fundamentals**

This module provides an overview of the various domains of cyber security. It helps develop an understanding of the importance of cyber security in today's digital world. It aims to provide an appreciation of cyber security from an end-to-end perspective. It covers fundamental security concepts, tools and techniques in domains such as data, end-user, software, system, network, physical, organisation, and digital forensics. It also helps develop knowledge and skills in identifying common cyber threats and vulnerabilities, and to apply techniques to tackle these issues. In this module, students are assessed by coursework only.

##### **Enterprise Information Systems**

Companies today are adopting the use of technology not just to assist them in their day-to-day operations but also gain an advantage over their competitors. Many companies are implementing enterprise-wide information systems that provide them with platforms to integrate and coordinate their business processes. The use of enterprise information systems has become a necessity in multi-national companies (MNCs) as well as small and medium enterprises (SMEs). Within an enterprise information system, there is an intricate relationship between business strategy, organisational structure, business processes and technology resulting in challenges and issues during implementation.

This module introduces students to the different components that build up an enterprise information system. Different types of information systems are used for business processes, from communication and order processing to data analysis for decision making, and in almost all business functions ranging from marketing, sales, procurement, and human resource, to product development and manufacturing, accounting and finance.

## **Fundamentals for IT Professionals I**

This module provides an introduction to the field of IT by exploring the roles, professional practices, ethical expectations and career development paths of IT professionals. Through a guided inculcation of interpersonal and team work skills with strong team bonding spirit, the module aims to deepen students' commitment to the sector that the course prepares them for. In addition, students will be required to begin charting their career path in the IT industry by considering crucial aspects such as personal preferences and aptitude, job roles and responsibilities, skills needed and further education.

## **Programming I**

This module introduces the fundamentals of programming and how to develop programs using appropriate problem-solving techniques in a modular style. In this practice-oriented module, students are taught how to apply problem-solving skills using a top-down structured programming methodology and given ample practice in translating solutions into computer programs, then test and debug the programs.

Topics include data types, variables, expressions, statements, selection structures, loops, simple computation and algorithms, and the use of libraries. Students will also practise the use of pseudocodes, best practices of programming, debugging techniques with the help of tools, development of test cases, and suitable program documentation. In addition, they will study various areas where application software plays a prominent part in helping organisations solve problems. Students will be given ample opportunity for independent and self-directed learning.

## **LEVEL 1.2**

### **Cryptography**

This module covers the essential concepts of Cryptography, including Public Key Infrastructure (PKI), Digital Signature and Certificate, and the various encryption/decryption algorithms. Students will understand how Symmetric and Asymmetric (Public-Key) cryptographic techniques are used to support different security implementations, and the encryption/decryption algorithms used in these techniques. The role of the Certificate Authority, how the digital certificates are generated, managed and distributed will also be covered in detail.

### **Databases**

Today's business organisations depend on information systems in virtually all aspects of their businesses. Corporate databases are set up to hold the voluminous business transactions generated by these information systems. This module introduces students to the underlying concepts of database systems and on how to model and design database systems that reflect business requirements. Students will be taught how to analyse data needs, model the relationships amongst the data entities, apply normalisation process to relations and create the physical database. Skills to be taught include data modelling technique, transformation of data model to relations, normalisation technique and SQL (Structured Query Language).

### **Front-End Development**

This module teaches the fundamental skills required to develop responsive websites that are optimised for mobile and desktop viewing. The students would attain skills and knowledge in programming languages such as HTML, CSS, JavaScript, jQuery, and AJAX which are used to develop interactive websites. This allows students to develop a website with interactive elements, providing them with a tangible product that they can develop into an interactive resume application and e-Portfolio website.

### **Operating Systems & Networking Fundamentals**

This module focuses on the fundamentals and principles of Operating Systems. It explains what general operating systems are and what they do. The module teaches concepts that are applicable to a variety of operating systems such as Windows and Linux. Students will learn about the different number and character representation methods such as binary, hexadecimal and ASCII. Concepts including processes, physical and virtual memory, files and directories, file systems, shell and OS commands will be covered.

The module also covers the terminology and technologies in current networking environments and provides a general overview of the field of networking as a basis for subsequent related modules in the course. The topics related to types of networks, network topologies, network technologies and layered protocol architecture will be taught. In addition, the students will also learn the OSI model as a reference model to understand data networks and understand the commonly used network systems such as Ethernet. The topic on TCP/IP as it forms most of the network architecture will be discussed in details. An overview of internetworking will also be presented to allow the

students to have a global picture of how local area networks and wide area networks are interconnected in the real world.

In this module, students are assessed by coursework only.

### Programming II

This module builds upon the knowledge and skills acquired in Programming 1 (PRG1). It aims to provide opportunities for the students to develop medium- scale applications based on the Object-Oriented (OO) approach. A suitable object-oriented high-level programming language will be used for students to continuously apply their problem-solving skills. The main concepts of OO and the implementation of applications using the OO approach will be taught in this module. The module may also cover the concepts of Abstract Data Types (ADTs) and the implementation of some selected ADTs using the OO approach.

Suitable sorting and search algorithms and the use of Application Protocol Interface (API) will be introduced when required. Other key topics include the introduction of system design concepts such as the class diagram. Software robustness and correctness, and good programming practices will be emphasised throughout the module. Independent and self-directed learning will also be encouraged.

### COURSE CURRICULUM

| Module Name                                 | Credit Units |
|---|--------------|
| <b>YEAR 1</b>                               |              |
| <b>Level 1.1 (25 hours per week)</b>        |              |
| Computing Mathematics                       | 4            |
| Cyber Security Fundamentals                 | 4            |
| Enterprise Information Systems              | 4            |
| Fundamentals for IT Professionals I         | 3            |
| Programming I                               | 4            |
| Innovation Made Possible ^                  | 3            |
| Sports & Wellness ^                         | 3            |
| <b>Level 1.2 (24 hours per week)</b>        |              |
| Cryptography                                | 4            |
| Databases                                   | 4            |
| Front-End Development                       | 4            |
| Operating Systems & Networking Fundamentals | 4            |
| Programming II                              | 4            |
| Communication Essentials^                   | 4            |

#### Notes:

^ For more details on Interdisciplinary Studies (IS) electives, please log on to [www.np.edu.sg/is/](http://www.np.edu.sg/is/)

#### IS Modules

The School of Interdisciplinary Studies (IS) delivers a broad-based curriculum, which nurtures a new generation of professionals with multidisciplinary skills and an innovative and entrepreneurial spirit to meet the challenges of a knowledge economy. IS offers both prescribed modules and electives to challenge boundaries. Prescribed modules develop students' competencies in core areas such as Communication, Innovation and Enterprise, Culture and Communication, and Personal Mastery and Development, while elective modules provide insights into Arts and Humanities, Business, Design, and Science and Technology.

## **COURSE MODULES**

### **LEVEL 2.1**

#### **Fundamentals for IT Professionals II**

This module gives a course-based experience in which students can engage with the local community and industry. This includes participation in community service events or in Service-Learning projects that leverage students' discipline knowledge and skills to meet identified needs. Through iterative and guided reflection on the service experience, students gain a broader appreciation of their discipline and an enhanced sense of personal voice, empathy and civic responsibility. Industry talks and seminars are organised to keep students up-to-date on emerging trends so as to build up their interpersonal, team and networking skills with the community and industry.

#### **Networking Infrastructure**

This module covers basic Local Area Network (LAN) and Wide Area Network (WAN) infrastructures including physical cabling systems used for an enterprise network, and how hardware platforms such as switches, routers and servers are deployed in typical networks. The module also introduces students to major networking protocols such as Ethernet, RIP, PPP, OSPF and HDLC, network operating systems and applications that run on LANs/WANs. Students will learn to configure switches and routers, and will be taught the techniques to configure and troubleshoot LANs and WANs.

#### **Reverse Engineering Malware**

This module trains students in reverse engineering malicious software using system and network monitoring tools, a disassembler, and a debugger. The module focuses on teaching students the essential assembly language concepts, along with the use of an assembly language emulator, a disassembler, and a debugger. These assembly language concepts and tools are needed to examine malicious code and understand its execution flow, identify common assembly-level patterns in malicious code, identify suspicious API calls, and to bypass defensive mechanisms of the malware.

#### **Secure Software Development**

This module provides students with the knowledge of the secure software development lifecycle. It trains students to incorporate security throughout the entire process of software development. With the knowledge gained from this module, students would be able to design, code, test and deploy software with a security mindset. The module begins with training students on how to identify, gather and record security requirements for a software. Students will learn secure software design, where various security frameworks, considerations and methodologies are taught. Students will understand how software vulnerabilities can be exploited and how to address the risks. Students are trained to write secure code that is resilient against critical web application attacks. Finally, students are trained in secure software testing and how to securely deploy software.

#### **World Issues: A Singapore Perspective<sup>^</sup>**

This module develops a student's ability to think critically on world issues. Students will discuss a wide range of social, political and cultural issues from the Singapore perspective. It also looks at how city-state Singapore defied the odds and witnessed close to half a century of rapid economic growth, strong political ties and social harmony.

### **LEVEL 2.2**

#### **Data Structures & Algorithms**

This module aims to provide students with the knowledge and skills to analyse, design, implement, tests and document programs involving data structures. It teaches basic data structures and algorithms within the conceptual framework of abstract data types. The emphasis here is to use the class feature of an Object-oriented language platform to give the concrete implementation of various abstract data types.

#### **Digital Forensics**

This module gives an insight into the process of forensics investigation. It covers the various types of computer related crimes, techniques of gathering electronic evidence, and the recovering of deleted, damaged or encrypted data. Students will also make use of advanced forensic tools to perform forensic investigation. Besides the tools and techniques of investigation, students will be taught sound forensic investigation methodology and the proper handling of evidence. The module will also cover aspects of law and policies applicable to digital forensics.

### Malware Analysis Tools and Techniques

This module teaches a repeatable malware analysis methodology, which includes static analysis, code analysis, and behavioural analysis. Students are taught how to write a malware analysis report on a target malware. Students will be able to determine the malware's indicators of compromise needed to perform incident response triage. This module trains students to efficiently use network and system monitoring tools to examine how malware interacts with the file system, registry, network, and other processes in an OS environment. Students are also trained to decrypt and analyse malicious script components of web pages, identify and examine the behaviour of malicious documents, and apply memory forensics techniques to analyse complex malware and rootkit infections. This module carries a pre-requisite: Reverse Engineering Malware (REM).

### Server & Cloud Security

This module aims to teach students the concepts and knowledge related to securing web servers and cloud models. It covers topics such as how a web server is installed and optimized securely, the various methods of attacking web servers and the appropriate countermeasures. The specific tools used to test for vulnerabilities in web servers, their applications and databases will also be covered. Cloud security topics will cover introduction to the various delivery models of cloud computing ranging from Software as a Service (SaaS) to Infrastructure as a Service (IaaS). Each of these delivery models presents an entirely separate set of security conditions to consider. An overview of security issues within each of these models will be covered with in-depth discussions of risks to consider.

### Web Application Development

This module provides students with the knowledge and skills needed to develop web applications and web application protocol interface (API). Students will be introduced to an integrated development environment that will enable them to design and develop web applications and web API over the Internet. They will learn how to make use of web development technologies such as ASP.NET framework, jQuery for rich internet applications, data interchange formats such as JSON AJAX, source code version control systems such as GIT or SVN to develop effective web applications, and web API targeting both mobile web and unified web experience. This module aims to provide students with a good understanding of the web development architecture and service layer as well as the various issues related to Web Application Development.

### Web Application Pen-Testing

This module provides a thorough understanding of major web application vulnerabilities and their potential impact on people and organisations. The module teaches a repeatable web pen-testing methodology, which includes reconnaissance, mapping, discovery, and exploitation of web application vulnerabilities and flaws. Students are taught how to write a web application pen-test report. The module teaches students the pen-tester's perspective of web applications. It trains students on building a profile of the machines that host the target web application and come up with a map of the web application's pages and features. Students are also trained in web application attack tools and interception proxies that are used to discover and exploit key web application vulnerabilities.

## COURSE CURRICULUM

| Module Name  | Credit Units |
|--|--------------|
| <b>YEAR 2</b>                                      |              |
| <b>Level 2.1 (22 hours per week)</b>               |              |
| Career & Professional Preparation II               | 2            |
| Fundamentals for IT Professionals II               | 2            |
| Networking Infrastructure                          | 4            |
| Reverse Engineering Malware                        | 4            |
| Secure Software Development                        | 4            |
| Web Application Development <sup>#</sup>           | 4            |
| World Issues: A Singapore Perspective <sup>^</sup> | 2            |

**Level 1.2 (22 hours per week)**

|   |   |
|---|---|
| Data Structures and Algorithms            | 4 |
| Digital Forensics                         | 4 |
| Malware Analysis Tools and Techniques     | 4 |
| Server & Cloud Security                   | 4 |
| Web Application Pen-Testing               | 4 |
| Interdisciplinary Studies (IS) elective ^ | 2 |

**Notes:**

^ For more details on Interdisciplinary Studies (IS) electives, please log on to [www.np.edu.sg/is/](http://www.np.edu.sg/is/)

**IS Modules**

The School of Interdisciplinary Studies (IS) delivers a broad-based curriculum, which nurtures a new generation of professionals with multidisciplinary skills and an innovative and entrepreneurial spirit to meet the challenges of a knowledge economy. IS offers both prescribed modules and electives to challenge boundaries. Prescribed modules develop students' competencies in core areas such as Communication, Innovation and Enterprise, Culture and Communication, and Personal Mastery and Development, while elective modules provide insights into Arts and Humanities, Business, Design, and Science and Technology.

# The elective modules offered may change from year to year, depending on relevance and demand. They may also include modules available in other diplomas offered by the School.

## **COURSE MODULES**

### **LEVEL 3.1**

#### **Ethical Hacking**

This module aims to develop Penetration Testers for the information security industry. They will be taught to follow a process model to locate and establish targets, find vulnerabilities, and exploit the flaws to determine potential impact and business risk with the goal of helping the owner improve security practices.

Students will learn the techniques hackers use to hack a system, and the steps to secure it. Students will have hands-on practice on actual pen-testing that involves reconnaissance to map out IT infrastructure, scanning vulnerable systems, and developing attack vectors to exploit loopholes in a system. Students will also be taught the necessary countermeasures to mitigate risks of exploitation through system hardening, intrusion detection and prevention.

#### **Network Security**

This module provides an in-depth knowledge on network security in a defensive view. It covers various types of firewall technologies, Virtual Private Networks (VPNs), and Intrusion Detection/Prevention Systems (IDS/IPS). Students will have a chance to configure and deploy state-of-the-art networking devices in a typical computer network.

Students will be taught skills to identify the internal and external threats against a network and to propose appropriate security policies that will protect an organisation's information. Students will also learn how to implement successful security policies and firewall strategies in this module.

#### **Fundamentals for IT Professionals III**

This module provides a stepping stone to the students in their IT career. Students are given an insight into the infocomm industries and are kept updated with the latest skill sets required in their IT career path. They also have the opportunity to be exposed to various institutes of higher learning to further acquire their skill sets.

## **ELECTIVE MODULES**

#### **Capstone Project**

In this module, students are required to complete a substantial project that is the culmination of their education in the School of InfoComm Technology. The project can be a real-world problem proposed by a client, or it can be proposed by students in pursuit of their personal interests.

#### **Governance & Data Protection**

This module examines the relevant frameworks to ensure that information assets are protected within an organisation. It includes the processes and policies for administering and managing a company's IT systems that follow the compliance framework. Concepts on risk management process, risk analysis and mitigation will also be introduced. Students will learn to evaluate risks against the company's critical assets and deploy safeguards to mitigate them. Control frameworks such as PCI (Payment Card Industry), ISO 17799/27002, and COBIT will be covered.

#### **Mobile Device Security & Forensics**

This module covers techniques and tools in the context of a forensic methodology to extract and utilise digital evidence on mobile devices. Students will learn how to use current forensic tools to preserve, acquire & examine data stored in a mobile device. The module covers basic SIM Card examination and cell phone forensics on multiple platforms such as iPhone, Android & Windows Mobile. The module takes a practice-oriented approach to performing forensics investigation on mobile phones. This module carries a co-requisite: Digital Forensics.

#### **Network Forensics**

Network equipment, such as web proxies, firewalls, IDS, routers, and even switches, contain evidence that can make or break a case. This module provides students with the knowledge and skills to recover evidence from network-based devices. It will begin with an introduction of different network devices and the type of data that are useful from a forensic point of view. It then moves on to the most common and fundamental network protocols that the forensic investigators will likely face during an investigation. These include the Dynamic Host Configuration Protocol (DHCP), Network Time Protocol (NTP) and Microsoft Remote Procedure Call (RPC) protocol. The students will learn a variety of techniques and tools to perform sniffing and log analysis on the network. Commercial and Open Source tools will be used to perform deep packet analysis while SIEM tools such as Splunk will be used to perform log analysis on network

devices.

### LEVEL 3.2

#### Internship or Project

This module provides students with the opportunity to apply the knowledge and skills gained to develop an IT solution to solve a practical problem. Students may undertake an in-house industry-driven project or a real-life IT project in a local or overseas organisation. These projects may include problem definition, requirements analysis, design, development and testing, delivery and presentation of the solution. Through the project, students will learn to appreciate the finer points of project planning and control issues relating to IT project development.

### COURSE CURRICULUM

| Module Name                               | Credit Units |
|---|--------------|
| <b>YEAR 3</b>                             |              |
| <b>Level 3.1 (22 hours per week)</b>      |              |
| Ethical Hacking                           | 4            |
| Network Security                          | 4            |
| Capstone Project or 2 Elective Modules #  | 8            |
| Fundamentals for IT Professionals III     | 2            |
| Interdisciplinary Studies (IS) elective ^ | 2            |
| <b>ELECTIVE MODULES #</b>                 |              |
| Governance & Data Protection              |              |
| Mobile Device Security & Forensics        |              |
| Network Forensics                         |              |
| <b>Level 3.2</b>                          |              |
| Internship or Project                     | 22           |

#### Notes:

^ For more details on Interdisciplinary Studies (IS) electives, please log on to [www.np.edu.sg/is/](http://www.np.edu.sg/is/)

#### IS Module

The School of Interdisciplinary Studies (IS) delivers a broad-based curriculum, which nurtures a new generation of professionals with multidisciplinary skills and an innovative and entrepreneurial spirit to meet the challenges of a knowledge economy. IS offers both prescribed modules and electives to challenge boundaries. Prescribed modules develop students' competencies in core areas such as Communication, Innovation and Enterprise, Culture and Communication, and Personal Mastery and Development, while elective modules provide insights into Arts and Humanities, Business, Design, and Science and Technology.

# The elective modules offered may change from year to year, depending on relevance and demand. They may also include modules available in other diplomas offered by the School.