DIPLOMA IN CYBERSECURITY & DIGITAL FORENSICS

In today's digital world, cybersecurity is crucial to protect organisations from cyber-attacks. 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, Databases, Cryptography and Operating Systems & Networking Fundamentals.

In your second year, you will develop skills in the areas of networking infrastructure, software security and digital forensics, which will aid you in developing secure software applications and conducting investigations on cybercrime.

In your final year, you will put your skills into practice by performing vulnerability assessment and penetration tests on software, systems and networks, securing networks, and analysing malware. Finally, apply your skills through a capstone project or take up a myriad of electives.

Plus, you can hone your skills in the real world with internships at leading companies and government organisations, such as Centre for Strategic Infocomm Technologies, Palo Alto Networks, SecureAge, Microsoft, NCS, CrimsonLogic, KPMG, PwC, Ernst & Young, SingTel, V-Key, Group-IB, DT-Asia, SP Group, Cyber Security Agency of Singapore and Ensign InfoSecurity. You can also attain the highly sought-after CompTIA and EC-Council certifications such as Security+ and Certified Ethical Hacker – all this to give you a head start in your career!

YEAR 1 COURSE MODULES

LEVEL 1.1

Cyber Security Fundamentals
This module provides an overview of the various domains of cyber security. It helps to 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 to develop knowledge and skills in identifying common cyber threats and vulnerabilities, and to apply techniques to tackle these issues.

Programming 1
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.

Design Principles
This module introduces students to basic elements and principles of design. Students will practice visual communication and self-branding through aesthetic use of line, shape, form, color, texture, typography, scale, contrast, rhythm and balance. Students will be trained in the usage of digital design tools and application of modern industrial practices to communicate the concepts, designs and solutions.

Data Science Fundamentals
This module provides an overview of Data Science, its importance in the world of data and how it affects the competitiveness of organisations. Learners will learn about the different areas within Data Science and the core pillars essential to practise in the area. Students will also be introduced to Design Thinking. Indicative topics include Introduction to Data Science, Big Data and Analytical Design Thinking.

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.

Fundamentals for IT Professionals 1
This module provides a broad introduction to the field of ICT by exploring the roles, professional practice, ethical expectations and career development paths of IT professionals. Through a guided inculcation of interpersonal and teamwork 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 ICT industry by considering crucial aspects such as personal preferences and aptitude, job roles and responsibilities, skills needed and further education.

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 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 the normalisation process to relations and create the physical database. Skills taught include data modelling technique, transformation of data model to relations, normalisation technique and SQL (Structured Query Language).

Front End Development
This module teaches skills such as HTML, CSS and JavaScript, required to develop responsive websites and web applications. The skills acquired will help students to better understand client-side web application attacks, a prelude to developing secure web applications and web application pen testing, which are covered in the subsequent modules in this course.

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. Topics related to types of networks, network topologies, network technologies and layered protocol architecture will be taught. In addition, the

students will also learn about the OSI model as a reference model to understand data networks and commonly used network systems such as Ethernet. The topic of TCP/IP, which forms most of the network architecture will be discussed in detail. 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.

Programming 2
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.

YEAR 1 COURSE CURRICULUM

Module Name	Credit Units
Level 1.1 (21 hours per week)	
Cyber Security Fundamentals	2
Programming 1	5
Design Principles	2
Data Science Fundamentals	2
Computing Mathematics	4
Fundamentals for IT Professionals 1	2
Health & Wellness^	1
Innovation Made Possible^	3
English Language Express*	NA
Level 1.2 (21 hours per week)	
Cryptography	4
Databases	4
Front End Development	2
Operating Systems & Networking Fundamentals	4
Programming 2	4
Communication Essentials^	3

Notes:
^ For more details on Interdisciplinary Studies (IS) electives, please log on to www.np.edu.sg/is
* For selected students only

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.

Official (Closed) - Non Sensitive

School of InfoComm Technology

YEAR 2 COURSE MODULES

LEVEL 2.1

Electives Module 1#

Electives Module 2#

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.

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 will 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 about secure software design, and various security frameworks, considerations and methodologies. They will understand how software vulnerabilities can be exploited and how they can address these risks. Students will also be trained in writing secure code that is resilient to critical web application attacks, as well as in secure software testing and how to securely deploy software.

LEVEL 2.2

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 recovery 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. They 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 will also be 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.

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 optimised 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.

Official (Closed) - Non Sensitive

School of InfoComm Technology

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 to build 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**.**

Fundamentals for IT Professionals 2
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 with emerging trends and develop their interpersonal, team and networking skills with the community and industry.

YEAR 2 COURSE CURRICULUM

Module Name	Credit Units
Level 2.1 (18 hours per week)	
Elective Module 1#	4
Elective Module 2#	4
Networking Infrastructure	4
Secure Software Development	4
World Issues: A Singapore Perspective^	2
Level 2.2 (18 hours per week)	
Digital Forensics	4
Malware Analysis Tools and Techniques	4
Server & Cloud Security	4
Web Application Pen-Testing	4
Fundamentals for IT Professionals 2	2

Notes:
^ For more details on Interdisciplinary Studies (IS) electives, please log on to 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. # Please refer to Year 3 for the elective modules' descriptions. 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.

Official (Closed) - Non Sensitive

School of InfoComm Technology

COURSE MODULES YEAR 3

LEVEL 3.1

Capstone Project or any two elective modules#
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.

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 in-depth knowledge of network security from 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.

Fundamentals for IT Professionals 3
This module provides a stepping-stone for students in their IT career. They will gain insights into the infocomm industry and keep abreast of the latest skill sets required in their IT career path. They will also have the opportunity to be exposed to various institutes of higher learning to further hone their skill sets.

ELECTIVE MODULES

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

Official (Closed) - Non Sensitive

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.

Data Structures & Algorithms
This module aims to provide students with the knowledge and skills to analyse, design, implement, test and document programmes involving data structures. It teaches basic data structures and algorithms within the conceptual framework of abstract data types. The emphasis is on using the class feature of an Object-oriented language platform to give the concrete implementation of various abstract data types.

Deep Learning

This module introduces the fundamentals of Deep Learning and its applications and provides students with essential context and background knowledge around Artificial Intelligence and its subset, Deep Learning. Students will learn about relevant models such as Neural Networks and experience the practical applications of these models in areas such as computer vision and natural-language processing. These models will be implemented using leading softwares and associated libraries.

Developing Cloud Applications
This module covers the analysis of business and technical requirements of a cloud-based system, implementation of a cloud strategy with appropriate programming tools, deployment, and testing and debugging of the cloud application. Analysis of business requirements to determine how they can be mapped into a cloud environment is discussed in this module. The module extends its discussion to cloud computing design patterns, best practices, cloud migration issues and considerations. Students are exposed to a cloud computing platform such as Windows Azure to get extensive hands-on practice to build, migrate, host and scale web applications and services through the vendor's data centres.

Machine Learning
This module introduces the fundamentals of Machine Learning (ML) and its applications. Students will be provided the essential context and background knowledge of Machine Learning. Students will gain exposure to both supervised and unsupervised learning models such as Linear & Logistic Regression, Decision Tree, K-means Clustering and more. Using leading software and associated libraries, learners will be able to implement and train Machine Learning models to address business challenges.

Mobile Applications Development
This module focuses on the design and development of applications for mobile devices like hand phones, personal digital assistants (PDAs) and handheld computers. Due to the nature of these handheld devices, issues such as memory storage, user interface and data input methods require more careful consideration. At the end of this module, students will be able to develop applications that can run on mobile devices and interact wirelessly with server-side programmes.

Cloud Architecture & Technologies
This module gives insight into the key concepts and technologies of cloud computing which include cloud characteristics, service models (SaaS, PaaS, and IaaS), deployment models (Public cloud, Private cloud, Community cloud, and Hybrid cloud), and the features of cloud computing technologies. It also covers the cloud computing architecture, emerging trends and issues such as clouds for mobile applications, cloud portability and interoperability, scalability, manageability, and service delivery in terms of design and implementation issues.

The module discusses the benefits and challenges of cloud computing, standards of cloud computing service delivery, and Service Level Agreement (SLAs) for cloud services. Hands-on activities are included to expose students to various cloud computing services offered by major cloud computing providers such as Amazon Web Services (AWS), Google App Engine (GAE), and Microsoft Windows Azure.

Official (Closed) - Non Sensitive

School of InfoComm Technology

LEVEL 3.2

Internship/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.

YEAR 3 COURSE CURRICULUM

Module Name	Credit Units
Level 3.1 (22 hours per week)	
Capstone Project / 2 Elective Modules #	8
Ethical Hacking	4
Network Security	4
Fundamentals for IT Professionals 3	2
Project ID: Connecting the Dots (IS)^	4
ELECTIVE MODULES # Governance & Data Protection Mobile Device Security & Forensics Network Forensics Data Structures & Algorithms Deep Learning Developing Cloud Applications Machine Learning Mobile Applications Development Cloud Architecture & Technologies	
Level 3.2 (20 hours per week)	
Internship or Project	20

Notes:
^ For more details on Interdisciplinary Studies (IS) electives, please log on to 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.