LEVEL 5 HIGHER INTERNATIONAL DIPLOMA

IN

CYBER SECURITY

CURRICULUM FOR CYBER SECURITY BASED ON CREDIT SYSTEM

PROGRAMME LEARNING OUTCOMES (PLO):

I. Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

II. Problem analysis Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

III. Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

IV. Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions Manage Construction Projects for Planning, Analyzing, Costing, Scheduling, Predicting and complete within the stipulated period and fund.

V. Modern tool usage Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations

VI. Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

VII. Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development, Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

VIII. Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design

documentation, make effective presentations, and give and receive clear instructions.

IX. Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments

X. Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change

PROGRAMME GUIDELINES	
PROGRAMME TITLE	**Level 5 Higher International Diploma in Cyber Security**
QUALIFICATION CODE	**701/7512/3**
LEVEL	**LEVEL – 4 & 5**
TOTAL CREDITS	**240**
TOTAL LEARNING HOURS	**2400 HOURS**
GUIDED LEARNING HOURS	**960 HOURS**

Total learning hour 2400 Hours

1 Credit = 10 hours of effort (10 hours of learning time which includes everything a learner has to do to achieve the outcomes in a qualification including the assessment procedures and practical's).

Guided Learning Hour for first year is 480 hours and second year is 480 hours.
Total Guided Learning Hours for Higher International Diploma in Cyber Security is 960 hours.

DIPLOMA IN CYBER SECURITY

COURSE STRUCTURE

YEAR	SEMESTER	UNIT SPECIFICATION	NO. OF. UNITS	UNIT CREDIT	CREDIT/YEAR
I	SEMESTER 1	Essential unit	1	20	120
		Essential unit	1	20	
		Essential unit	1	20	
	SEMESTER 2	Essential unit	1	20	
		Essential unit	1	20	
		Essential unit	1	20	
II	SEMESTER 3	Essential unit	1	20	120
		Essential unit	1	20	
		Essential unit	1	20	
	SEMESTER 4	Essential unit	1	20	
		Essential unit	1	20	
		Essential unit	1	20	
				TOTAL	**240**

FIRST YEAR	Essential unit carries	20 credit
	Essential unit carries	20 credit
	Essential unit carries	20 credit
SECOND YEAR	Essential unit carries	20 credit
	Essential unit carries	20 credit
	Essential unit carries	30 credit

LIST OF UNITS

S. No.	Subject Code	UNIT	UNIT SPECIFICATION	CREDIT
1	I/775/2021	Cyber Attacks	Essential unit	20
2	I/775/2022	Cyber Security Principles and Technologies	Essential unit	20
3	I/775/2023	Effect of Cyber Security Tools.	Essential unit	20
4	I/775/2024	Security Threats to E-Commerce	Essential unit	20
5	I/775/2025	Cyber security Challenges and Encryption Algorithms	Essential unit	20
6	I/775/2026	Advanced Encryption Standard Algorithms	Essential unit	20
7	I/775/2027	Emerging cyber threats and vulnerabilities	Essential unit	20
8	I/775/2028	Cyber security Awareness and Education	Essential unit	20
9	I/775/2029	Artificial Intelligence & Machine Learning in Cybersecurity	Essential unit	20
10	I/775/2030	Blockchain for cyber security	Essential unit	20
11	I/775/2031	Cybercrime Investigation & Digital Forensics	Essential unit	20
12	I/775/2032	Cyber-Physical Systems in cyber security	Essential unit	20

Semester : I
Year : 1
Credit : 60

UNIT CODE	UNIT	UNIT SPECIFICATION	CREDIT
I/775/2021	Cyber Attacks	Essential unit	20
I/775/2022	Cyber Security Principles and Technologies	Essential unit	20
I/775/2023	Effect of Cyber Security Tools.	Essential unit	20

Semester : II
Year : 1
Credit : 60

UNIT CODE	UNIT	UNIT SPECIFICATION	CREDIT
I/775/2024	Security Threats to E-Commerce	Essential unit	20
I/775/2025	Cyber security Challenges and Encryption Algorithms	Essential unit	20
I/775/2026	Advanced Encryption Standard Algorithms	Essential unit	20

Semester : III
Year : 2
Credit : 60

UNIT CODE	UNIT	UNIT SPECIFICATION	CREDIT
I/775/2027	Emerging cyber threats and vulnerabilities	Essential unit	20
I/775/2028	Cyber security Awareness and Education	Essential unit	20
I/775/2029	Artificial Intelligence & Machine Learning in Cybersecurity	Elective Unit	20

Semester : IV
Year : 2
Credit : 60

UNIT CODE	UNIT	UNIT SPECIFICATION	CREDIT
I/775/2030	Blockchain for cyber security	Essential unit	20
I/775/2031	Cybercrime Investigation & Digital Forensics	Essential unit	20
I/775/2032	Cyber-Physical Systems in cyber security	Essential unit	20

UNIT CODE : I/775/2021

UNIT TITLE : Cyber Attacks

CREDIT : 20

SPECIFICATION : Essential Unit

UNIT DESCRIPTION

The aim of the course is to provide students with a comprehensive understanding of cyber threats, vulnerabilities, and attack vectors, as well as strategies for prevention, detection, and response to cyber-attacks. Through theoretical knowledge, practical exercises, and case studies, students will develop the skills and knowledge necessary to protect digital assets, mitigate risks, and maintain the security of information systems and networks.

UNIT LEARNING OUTCOMES

ULO1 - Understanding Cyber Threat Landscape and Attack Vectors
ULO2 – Able to know Implementing Cybersecurity Measures and Best Practices
ULO3 – Understanding Evaluating and Enhancing Cybersecurity Posture

MAPPING

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8	PLO9	PLO10
ULO1	M	M		M	M		M	M		M
ULO2	M			M		M		M		
ULO2	M	M		M	M			M		M

UNIT CODE : I/775/2022

UNIT TITLE : Cyber Security Principles and Technologies

CREDIT : 20

SPECIFICATION : Essential Unit

UNIT DESCRIPTION

The aim of the course is to provide students with a foundational understanding of the principles, concepts, and technologies underpinning cybersecurity. Through theoretical knowledge, hands-on practical exercises, and case studies, students will develop the skills and knowledge necessary to protect digital assets, mitigate cyber threats, and secure information systems and networks effectively.

UNIT LEARNING OUTCOME

ULO1 – Understanding Cyber Security Fundamentals.
ULO2 – Understanding Exploring Cyber Security Technologies and Tools
ULO2 – Able to Implementing Cyber Security Best Practices

MAPPING

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8	PLO9	PLO10
ULO1	M	M			M	M		M	M	M
ULO2			M	M			M	M		
ULO3		M			M			M	M	

UNIT CODE : I/775/2023

UNIT TITLE : Effect of Cyber Security Tools

CREDIT : 20

SPECIFICATION : Essential Unit

UNIT DESCRIPTION

The aim of the course is to explore the diverse range of cybersecurity tools available to organizations and individuals, understand their functionalities, and evaluate their effectiveness in mitigating cyber threats. Through theoretical exploration, practical demonstrations, and case studies, students will develop a nuanced understanding of how cyber security tools impact the security posture of organizations and contribute to overall cyber resilience.

UNIT LEARNING OUTCOME

ULO1 - Understanding Cyber Security Tool Landscape
ULO2 - Understanding Evaluating the Effectiveness of Cyber Security Tools
ULO3 – Able to Implementing and Optimizing Cyber Security Tools

MAPPING

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8	PLO9	PLO10
ULO1	M	M		M	M		M	M	M	M
ULO2	M						M		M	
ULO3	M	M	M	M	M	M			M	

UNIT CODE : I/775/2024

UNIT TITLE : Security Threats to E-Commerce

CREDIT : 20

SPECIFICATION : Essential Unit

UNIT DESCRIPTION

The aim of the course is to provide students with an in-depth understanding of the security challenges and risks faced by e-commerce platforms, along with the policies and standards aimed at mitigating these threats. Through theoretical knowledge, case studies, and practical exercises, students will develop the skills and knowledge necessary to implement effective security measures and ensure the integrity, confidentiality, and availability of e-commerce transactions and data.

UNIT LEARNING OUTCOMES

ULO1 - Understanding Security Threats to E-Commerce Platforms

ULO2 - Exploring E-Commerce Security Policies and Regulatory Compliance

ULO3 - Implementing Security Measures and Best Practices for E-Commerce Security

MAPPING

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8	PLO9	PLO10
ULO1	M	M		M	M		M	M		M
ULO2	M			M		M		M		
ULO3	M		M		M	M		M	M	

UNIT CODE	:	I/775/2025
UNIT TITLE	:	Cybersecurity Challenges and Encryption Algorithms
CREDIT	:	20
SPECIFICATION	:	Essential Unit

UNIT DESCRIPTION

The aim of the course is to provide students with a comprehensive understanding of the major cybersecurity challenges faced by organizations and the role of encryption algorithms in securing digital communications and data. Through theoretical knowledge, practical demonstrations, and case studies, students will develop the skills and knowledge necessary to address cybersecurity threats and implement encryption solutions effectively.

UNIT LEARNING OUTCOMES

ULO1 - Understanding Cybersecurity Challenges

ULO2 - Understanding Exploring Encryption Algorithms

ULO2 – Able to Implementing Encryption Solutions

MAPPING

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8	PLO9	PLO10
ULO1	M	M		M	M		M	M		M
ULO2	M			M		M		M		
ULO3	M	M		M	M		M			

UNIT CODE	:	I/775/2026
UNIT TITLE	:	Advanced Encryption Standard (AES) Algorithms
CREDIT	:	20
SPECIFICATION	:	Essential Unit

UNIT DESCRIPTION

The aim of the course is to provide students with an in-depth understanding of the principles, mechanisms, and applications of AES encryption algorithms. Through theoretical knowledge, practical exercises, and hands-on demonstrations, students will develop the skills and knowledge necessary to implement, analyze, and evaluate AES encryption algorithms in various cybersecurity contexts.

UNIT LEARNING OUTCOMES

ULO1- Understanding the Principles and Concepts of AES Encryption

ULO2- Understanding the Implementing AES Encryption Algorithms

ULO3- Analyzing and Evaluating AES Encryption Performance and Security

MAPPING

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8	PLO9	PLO10
ULO1	M	M		M	M		M	M		M
ULO2	M			M		M		M		
ULO3	M		M	M		M				

UNIT CODE : I/775/2027

UNIT TITLE : Emerging Cyber Threats and Vulnerabilities

CREDIT : 20

SPECIFICATION : Essential Unit

UNIT DESCRIPTION

The aim of the course is to provide students with an up-to-date understanding of the latest cyber threats and vulnerabilities facing individuals, organizations, and society. Through theoretical exploration, case studies, and practical exercises, students will develop the skills and knowledge necessary to identify, assess, and mitigate emerging cyber threats and vulnerabilities effectively

UNIT LEARNING OUTCOMES

ULO1- Understanding Emerging Cyber Threat Landscape
ULO2- Assessing and Mitigating Emerging Cyber Vulnerabilities
ULO3- Developing Proactive Cyber Defense Strategies

MAPPING

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8	PLO9	PLO10
ULO1	M	M		M	M		M	M		M
ULO2	M			M		M		M		
ULO3	M		M	M		M	M		M	

UNIT CODE : I/775/2028

UNIT TITLE : Cybersecurity Awareness and Education

CREDIT : 20

SPECIFICATION : Essential Unit

UNIT DESCRIPTION

The aim of the course is to equip students with the knowledge, skills, and attitudes necessary to promote cybersecurity awareness and education within organizations and society at large. Through theoretical understanding, practical exercises, and interactive learning methods, students will develop the capacity to recognize cyber threats, adopt safe online practices, and contribute to a culture of cybersecurity awareness and resilience.

UNIT LEARNING OUTCOMES

ULO1- Understanding the Importance of Cybersecurity Awareness

ULO2- Promoting Safe Online Practices and Behavior

ULO3-Creating Effective Cybersecurity Awareness Programs

MAPPING

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8	PLO9	PLO10
ULO1	M	M		M	M		M	M		M
ULO2	M			M		M		M		
ULO3	M		M	M		M	M			

UNIT CODE : I/775/2029

UNIT TITLE : Artificial Intelligence & Machine Learning in Cybersecurity

CREDIT : 20

SPECIFICATION : Essential Unit

UNIT DESCRIPTION

The aim of the course is to provide students with a comprehensive understanding of how artificial intelligence (AI) and machine learning (ML) techniques are applied to enhance cybersecurity capabilities. Through theoretical knowledge, practical exercises, and case studies, students will develop the skills and knowledge necessary to leverage AI and ML algorithms for threat detection, anomaly detection, and security automation in cybersecurity operations

UNIT LEARNING OUTCOMES

ULO1- Understanding the Foundations of AI and ML in Cybersecurity

ULO2- Applying AI and ML Techniques for Threat Detection and Anomaly Detection

ULO3- Implementing AI and ML Solutions in Cybersecurity Operations

MAPPING

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8	PLO9	PLO10
ULO1	M	M		M	M		M	M		M
ULO2	M			M		M		M		
ULO3	M	M			M		M			M

UNIT CODE : I/775/2030

UNIT TITLE : Blockchain for Cybersecurity

CREDIT : 20

SPECIFICATION : Essential Unit

UNIT DESCRIPTION

The aim of the course is to provide students with a deep understanding of how blockchain technology can be utilized to enhance cybersecurity measures. Through theoretical exploration, practical applications, and case studies, students will develop the knowledge and skills necessary to leverage blockchain's decentralized and immutable nature to address cybersecurity challenges effectively.

UNIT LEARNING OUTCOMES

ULO1- Understanding the Fundamentals of Blockchain Technology

ULO2- Exploring the Applications of Blockchain in Cybersecurity

ULO3-Implementing Blockchain Solutions for Cybersecurity Challenges

MAPPING

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8	PLO9	PLO10
ULO1	M	M		M	M		M	M		M
ULO2	M			M		M		M		
	M	M			M		M			M

UNIT CODE : I/775/2031

UNIT TITLE : Cybercrime Investigation & Digital Forensics

CREDIT : 20

SPECIFICATION : Essential Unit

UNIT DESCRIPTION

The aim of the course is to equip students with the knowledge, skills, and techniques required to investigate cybercrimes and analyze digital evidence effectively. Through theoretical understanding, practical exercises, and hands-on experience with forensic tools, students will develop the capabilities to identify perpetrators, gather evidence, and present findings in a court of law.

UNIT LEARNING OUTCOME

ULO1 - Understanding Cybercrime Investigation Principles

ULO2 - Mastering Digital Forensics Techniques

ULO3- Conducting Effective Cybercrime Investigations

MAPPING

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8	PLO9	PLO10
ULO1	M	M	M	M			M	M	M	M
ULO2		M				M			M	
ULO3	M	M			M	M	M	M		

UNIT CODE : I/775/2032

UNIT TITLE : Cyber-Physical Systems in Cybersecurity

CREDIT : 20

SPECIFICATION : Essential Unit

UNIT DESCRIPTION

The aim of the course is to provide students with a comprehensive understanding of the security challenges and solutions related to cyber-physical systems (CPS). Through theoretical knowledge, practical exercises, and case studies, students will develop the skills and knowledge necessary to secure interconnected systems that bridge the digital and physical worlds.

UNIT LEARNING OUTCOMES

ULO1- Understanding the Fundamentals of Cyber-Physical Systems (CPS

ULO2- Analyzing Security Risks and Threats in Cyber-Physical Systems

ULO3- Implementing Security Measures and Solutions for Cyber-Physical Systems

MAPPING

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8	PLO9	PLO10
ULO1	M	M		M	M		M	M		M
ULO2	M			M		M		M		
ULO3	M		M	M		M	M			

ASSESSMENT METHODS AND TECHNIQUES FOR DIPLOMA IN CYBER SECURITY

Assessment technique	Type of Assessment	Description	Formative or Summative
Case studies	Oral/ Problem based/ Practical	Students are required to work through a case study to identify the problem(s) and to offer potential solutions; useful for assessing students' understanding and for encouraging students to see links between theory and practice. Case studies could be provided in advance of a time-constrained assessment.	**Formative**
Concept maps	Written/ Oral	Students map out their understanding of a particular concept. This is a useful (and potentially quick) exercise to provide feedback to staff on students' understanding.	**Formative**
'Doing it' exam	Written	An exam which requires students to do something, like read an article, analyze and interpret data etc.	**Formative / Summative**
Field report	Written/ Oral	Students are required to produce a written/ oral report relating to a field/ site visit.	**Formative**
Laboratory books / Reports	Practical/ Written	Students are required to write a report for all (or a designated sample) of practical's in a single lab book. A sample of lab books will be collected each week to mark any reports of labs done in previous weeks; this encourages students to keep their lab books up to date. Each student should be sampled the same number of times throughout the module with a designated number contributing to the assessment mark.	**Summative**
Multiple choice questions (MCQs)	Written	Can be useful for diagnostic, formative assessment, in addition to summative assessment. Well-designed questions can assess more than factual recall of information, but do take time to design.	**Formative / Summative**
Online discussion boards	Written	Students are assessed on the basis of their contributions to an online discussion for example, with their peers; this could be hosted on a virtual learning environment (VLE).	**Formative**
Open book exams	Written	Students have the opportunity to use any or specified resources to help them answer set questions under time constraints. This method removes the over-reliance on memory and recall and models the way that professionals manage information.	**Summative**
Oral presentations	Oral / Written	Students are asked to give an oral presentation on a particular topic for a specified length of time and could also be asked to prepare associated	**Summative**

		handout(s). Can usefully be combined with self- and peer-assessment.	
Problem sheets	Written	Students complete problem sheets, e.g. on a weekly basis. This can be a useful way of providing students with regular formative feedback on their work and/or involving elements of self- and peer assessment.	**Formative**
Research projects / Group projects	Written/ Practical/ Oral/ Performance/ Problem based/ Work placement	Potential for sampling wide range of practical, analytical and interpretative skills. Can assess wide application of knowledge, understanding and skills.	**Formative / Summative**
Short answer questions	Written	Useful to assess a wide range of knowledge/skills across a module.	**Summative**
Simulations	Practical/ Written/ Oral/ Problem-based	Text or virtual computer-based simulations are provided for students, who are then required to answer questions, resolve problems, perform tasks and take actions etc. according to changing circumstances within the simulation. Useful for assessing a wide range of skills, knowledge and competencies.	**Formative**
Viva voce	Oral	Often used for assessing 'borderline' degree classifications but also useful to explore students' understanding of a wide range of topics. Depending on class size however, they can be time consuming for staff.	**Summative**