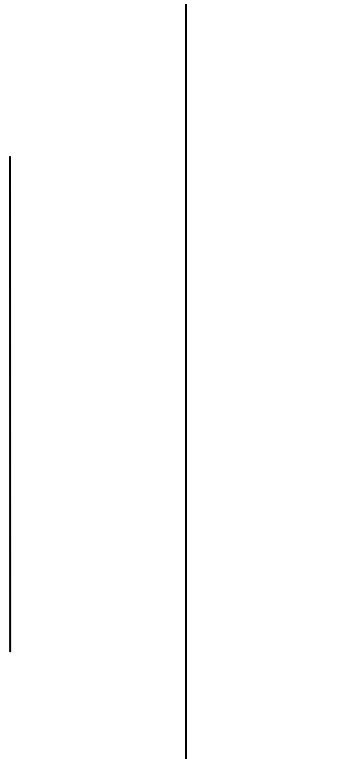




UNIVERSITY OF COMPUTER SCIENCES & SKILLS

Rzgowska 17a, 93-008 Łódź, Poland



**A complete course of study for
Bachelor of Computer Science (Network
Technology & Cyber Security)
(4 years)**

WYŻSZA SZKOŁA INFORMATYKI
I UMIEJĘTNOŚCI
93-008 Łódź, ul. Rzgowska 17 A (07)
tel. 42 27 50 100, fax 42 240 33 55
REGON 471544471, NIP 107-19-96-067

1. Introduction

This documentation constitutes the Program Outline for the Undergraduate Degree of the Bachelor of Computer Science (Network Technology & Cyber Security) affiliated to University of Computer Science and Skills, Lodz, Poland. The Program of studies is aligned with international standards of Undergraduate Higher Education and fulfils the criteria of the Harmonization of Higher Education. The modules are delivered interactively and are based on actual knowledge and research in this pathway. They equally introduce students to essential practice and embed internships.

Objective of this Program of studies is to introduce students to relevant theory and practice with a specific view on contemporary computer science. Therefore, all modules of this course and their content are oriented towards actual and future trends in this computer science and IT industry. That means the right balance between professional roles in organizational functions or in future self-employment. They also own an overarching understanding on how IT organizations function in a competitive environment.

Each individual module is designed to provide in-depth subject knowledge and also contributes to cross-functional understanding. The overall outcome of this Program of studies supports Graduates in their career development through the combination of academic knowledge and essential practice-orientation of highest standards. Emphasis of the Program of studies is Employability Impact.

This Program of studies is considered as relevant, rich and academically valid. Superior professional standards have been embedded accordingly.

2. Delivery of Teaching and Student Achievement

The Program of studies can be either delivered as full- or part-time studies. In addition to the formal contact hours students will be expected to engage in additional independent studies during and between the different modules. These independent studies are more intense, when the Program is taken as part-time studies. Individual and own studies are an essential element of study requirements, which strongly contribute to the successful outcome of the studies. The Bachelor of Computer Science (Network Technology and Cyber Security) is especially designed to improve candidates.

- Qualities in effectively and efficiently contributing to organizational progress

- Knowledge on the inter-functional and cross-disciplinary complexities within contemporary challenges
- Capacity to exercise good practice by application of profound standards in the computer science and IT related business
- Intellectual caliber and critical reflection
- Problem-solving skills being essential in and for complex environments
- Own motivation and that of others and through these develop principles for sustainable organizational competitiveness and viability.

2.1 General Delivery

These studies can be delivered as full-time or part-time studies. Practice-oriented internships complement teaching and learning.

In addition to formal contact hours students are expected to engage in independent studies, during and after taking the different modules. They are an essential study prerequisite.

Bachelor of Computer Science (Network Technology and Cyber Security) is a four years academic program which is 240 ECTS (4 years full-time). The standard period of studies comprises eight (8) semesters. The study plan has been designed into standard education, research, and activity based. The study plan consists of 50 hours of assisted lecture session, 15 hours of self-study, 19 hours of research and study and 84 hours of intern, assignment, project and field work. Internal activities like assignment, internship, field work and projects are evaluated internally and graded according to the grading specification.

2.2 Attendance

For all its presence studies University strongly feels that good attendance is necessary on students' part as an important element of successful studies. Consequently, the following requirements operate:

- Students are expected to attend all sessions.
- If a student cannot attend for any genuine reason (e.g., illness), they are expected to inform the tutor or course leader in due time.
- Persistent non-attendance will require an explanation, in person, initially with the course leader.

2.3 General Grading Scheme of the University

Through all modules and the dissertation, a consistent marking scheme applies.

2.3.1 Marking Scheme

Grading can be based on theoretical discussion only, but in the case of applied sciences it can also respect pragmatism. I.e., depending on the assessment brief, practice-orientation of an assessment then is of equal acceptance and value, but that does not mean that submitted work can be without significant theoretical components I.e., all assessments must include sufficient theory and (except examinations) adopt sufficient literature of academic acceptability. The literature has to be academically acknowledged meaning that public sources are not approved.

2.3.2 Grading Policies

The possible range of grades consists of:

Obtained Percentage	Value
>90%	High Distinction
81 to 90%	Distinction
71 to 80%	Merit
61 to 70%	Pass with Satisfaction
50 to 60%	Pass
<50%	Fail = Retake of assessment

Table 1 Grading Policy

% of Mark Obtained	Grade point	Grade Symbol	Values	Explanation
90.00-100%	4.00	A+	High Distinction	Showing outstanding achievement
80.00-89.99%	3.83	A	Distinction	
75.00-79.99%	3.67	A-	Merit	show honors achievement of a higher-than average achievement of other students of the class
70.00-74.99%	3.33	B+	Pass with Satisfaction /Average	Show satisfactory performance with an average performance
65.00-69.99%	3.00	B		
60.00-64.99%	2.67	B-		
55.00-59.99%	2.33	C+	Pass	Showing percentage less than the average achievement of all students in the same class
50.00-54.99%	2.00	C		
45.00-49.00%	1.67	D+	Fail	Reset- Students can sit chance exam
40.00-44.99%	1.33	D		
00.00-39.99%	1.00	F	Fail	Retake-Students have to re-register for that exam

Table 2 Grade Point Table

2.3.3 Retake Regulations

Students, who have failed an assessment and/or module, are admitted to one retake. The maximum mark awarded to retakes is a Pass at 50%.

Should a student fail the re-assessment as well, they will have to repeat the module. During the whole Program of studies

- Each module can only be repeated once, and
- It only is possible to repeat three modules in total

Students failing a module twice or three modules in total will not be able to continue their studies to the intended degree.

2.3.4 Moderating Approval of Marks

To achieve consistent marking and as an implemented and proven control of quality, all assessments are subject to the moderating approval of the Examination Board as explained in the Undergraduate Student Handbook. This process guarantees that students will find an impartial, equal and fair marking process.

2.3.5 Student Handbook

Further essential elements of importance for this Program of studies are regulated and explained in the Undergraduate Student Handbook. Students are advised to read these carefully as a binding regulating part of the course's structure.

2.4 Award

Students who have passed all modules and the dissertation successfully, the University awards the Bachelor of Computer Science (Network Technology and Cyber Security).

Depending on the numerical average achieved in all modules, the Bachelor of Computer Science (Network Technology and Cyber Security) can be awarded as table 2.

In addition to their Bachelor Certificate, students will additionally receive a full Transcript. Students terminating their studies before completion or are not fulfilling the criteria (fails, academic misconduct) for obtaining the Bachelor Degree will obtain a Transcript stating subjects attended and the number of credits being awarded until the moment of termination.

3. Admission to the Bachelor of Computer Science (Network Technology and Cyber Security)

3.1 Admittance by Education

The Program of studies addresses candidates, who have finished school with a good College Degree, Baccalaureate, Diploma or equivalent other national qualification.

3.2 Work-based Entry Route

Applications from professionals without a college Degree or Baccalaureate or equivalent on national level, who can instead submit evidence of a credible professional education with their application, such as an apprenticeship or national equivalent, are equally encouraged to apply. Those candidates having sufficient work experience (e.g., gained in an apprenticeship) can only be admitted by providing evidence of such experience. These candidates are invited seeking advice with their local study center or the Registry of the University for further details and information for an individual assessment of their prior qualification.

3.3 Application Process

Applications must be made through the application form and are equally welcomed from individual candidates or from those being sponsored by employers. Only complete applications will be considered. The application form has to be accompanied by

- A certified copy of the latest School Degree (if applicable) and/or
- Written evidence of the existing professional education and/or experience
- Two photographs in passport size
- A copy of the passport

The registry of the University will issue a Letter of Acceptance for successful applicants enrolling and admitting the candidate to the Program of studies.

4 Course Outline

4.1 Mission of the Bachelor of Computer Science (Network Technology and Cyber Security)

The Bachelor of Computer Science (Network Technology and Cyber Security) is an Undergraduate Program of studies preparing candidates for qualified professional roles in IT organizations. The Program's purpose is to educate the responsible professional, who understands the general picture and wider implications by which organizations of this particular industry are driven.

Contemporary professionals must also respect high standards of ethics and moral, which are indispensable elements within the demand for sustainable management meeting the multiple challenges of economy and society. In today's complex environment professionals have to respect the objectives of multiple constituents and a variety of stakeholders with differing interests.

Internalizing these criteria into the studies enhances Graduates' employability and career opportunities within IT related organizations significantly. The Program of studies supports Graduates to differentiate themselves from employees, whose capabilities are limited to professional experience alone.

The Bachelor of Computer Science (Network Technology and Cyber Security) provides candidates with superior knowledge being fully concentrated on best practice and future developments, but focuses on modern organizational challenges, forces, and values driving these. The course combines knowledge on organizations and introduces the understanding of key management practice skills and respects professional standards of the IT related industry.

4.2 Strategic Aims

Shared aims unite all modules of the Bachelor of Computer Science (Network Technology and Cyber Security). These objectives are:

- To introduce to and use theory, practice-oriented insights and demonstrations to enhance candidates' intellectual caliber, professional and future leadership skills, and problem-solving capacity.
- To communicate sophisticated understandings of present and future problems and challenges typically found in contemporary IT related organizations and to identify scope for general and particular improvements.
- To analyze and foster appropriate professional roles contributing to managing the contemporary IT related organization. It further informs about the wider corporate responsibilities by using sophisticated approaches to drive organizational development and to meet the needs of demanding customers and guests, and multiple organizational constituents and contexts.
- To explore scope and content of organizational and functional effectiveness being focused on turbulent markets, organizational sustainability and progress within the permanently changing environment in a national, international, and global context.

4.3 Learning Outcomes of the Program of Studies

The Bachelor of Computer Science (Network Technology and Cyber Security) Program of studies develops profound knowledge of contributing to the management of the contemporary organization. It is specifically designed for meeting the concept of Employability Impact.

The particular intended learning outcomes are:

- Introduce critical thinking and analytical approaches to theories and best practice of contemporary hospitality organizational contexts by analyzing the internal and external environment.
- Further the ability to read, understand, and make sense of the specific organizational needs for sustainable organizational progress in the IT related industry.
- Develop the capacity to evaluate and critically analyze how organizational functions effectively and efficiently interact for performance improvements.
- Apply own high standards of moral and ethical behavior contributing to that of an organization.
- The aims for each of the individual modules that make up the Bachelor of Computer Science (Network Technology and Cyber Security) are set out in the individual module specifications of Chapter 5.

4.4 Standard Period of Studies

The duration of this Program of studies is structured to be accomplished within four (4) years of studies but may be extended to a maximum of six (6) years on request. Extensions are subject to a student's application and must be approved by a local study center and/or the University.

5. Bachelor of Computer Science (Network Technology and Cyber Security)

5.1 Introduction to the Program

Bachelor of Computer Science (Network Technology and Cyber Security) is focused a unique opportunity to learn about specialist security techniques and use real-world networking equipment in a security context. Students are also educated about market-leading Cisco Routing & Switching Techniques, security appliances, ethical hacking techniques, vulnerability analysis, and penetration testing and data encryption technology. This program has been designed to equip the individual with global knowledge of network and security.

5.2 Program Facts

Program Name	Bachelor of Computer Science (Network Technology & Cyber Security)
Program Duration Years	4 years
Semester Duration (Months)	6 Months
Intake Months	January/ September

No. of Semesters	8
Level	Bachelor
Field of Study	Computer Science
ECTC Credits	240 ECTC

Table 3 Program Facts

5.3 Program Objective:

The objectives of the course are aimed at:

- Computer systems and network, establishes link between people and businesses on a global scale. Business and industry are dependent on diverse network technologies and there is a high demand for professionals for designing as well as efficiently managing network systems.
- Our technology-infused course comprises technology, security and networking modules and thus offers diverse job opportunities for students. We also emphasize on the installation, operation, security and maintenance of computer systems as well as networks as far as business and industry is concerned.
- The course will equip the students with the essential skills for designing, implementing and managing systems effectively to ensure that people benefits from the use of these systems. This learning will also help the students to manage, design, implement, configure and operate secure networks on a professional footing and identify the threats to network security and formulate and implement defense strategies and mechanisms.

5.4 Entry Requirement

- 12 (Science and Management) / Diploma in IT
- Pass Foundation programs in Business & Computing Foundation; or
- Pass STPM; or secured at least second division in the 10+2, PCL or equivalent program equivalent
- Pass A level with 5 credit (English & 4 other subjects); or equivalent to Government agency

5.5 Learning activities and assessment

The examination will be conducted and monitored by the University, in presence of the representative from university. To successfully complete a subject/ module, the student has to achieve Pass marks in both internal assessments as well as final examination.

- Mixture of formal lectures, tutorials & Seminars and Practical sessions.
- Supervised Group works, Course Works.
- Regular Assignments, Assessments in the form of practical coursework, lab tests, written exams
- Case study, presentation, project works
- Evaluation of learning outcome will vary according to the need of the modules

Type of Assessment	Components of Assessment	Weightings of Components (%)
Written test (50%)	Final University Examination	50
Course Work (50%)	Test –Mid-Term Examination	10
	Written Assignment-1 (1000 words)	10
	Written Assignment-2 (1000 words)	10
	Project Work/Case Study	10
	Quizzes	5
	Attendance	5
	Total	100

Table 4 Types of Assessment for the Program

5.6 Graduation Certificate

After successful completion of the course the University will provide the graduation certificate to the students. Only the students who will garner the cumulative grade point average of 2.0 will be eligible for graduation. Students who cannot achieve the benchmarked summative assessment will be given a chance to repeat the specified items. Students are awarded with The Certificate of the Bachelor of Computer Science (Network Technology and Cyber Security) being officially recognized and part of the official Process of Harmonization of Higher Education.

This way, Graduates are equipped with outstanding knowledge and skills in Hospitality Management, but also the right officially and widely recognized documentation for their degree on international level.

5.7 Career Opportunities

After successful completion of the course, students can make their career as the following area and post

- Network Engineer
- Network Support Specialist
- Network Administrator System Administrator
- Security Engineer, Network Consultant
- Ethical Hacker
- Security Administrator
- Network Communication Engineer
- Security Consultant
- Penetration Tester
- Computer Science Teacher
- Information Security Specialist
- Network Design Engineer

5.8 Module Structure

Semester 1

Course Code	Course Title	ECTS Credits
CSC-101	Introduction to IT	6
CSC-102	Programming Fundamental using C	6
CSC-103	Data Communication & Networking	6
MTH-151	Computational Mathematics I (Continuous)	6
ENG-175	Communication English	6
	Total	30

Semester 2

Course Code	Course Title	ECTS Credits
MTH-152	Computational Mathematics II (Discrete)	6
ENG-176	Technical & Professional Communication	6
CSC-104	Object Oriented Programming (C++ / Java)	6
CSC-105	Database Management System	6
CSC-106	Digital Electronics & Logic Design	6
	Total	30

Semester 3

Course Code	Course Title	ECTS Credits
MTH-253	Numerical Method	6
CSC-201	Data Structure & Algorithm	6
CSC-202	Network Analysis & Design	6
CSC-203	Routing and Switching Essentials	6
CSC-204	Organization & Management	6
	Total	30

Semester 4

Course Code	Course Title	ECTS Credits
CSC-205	Probability & Statistics	6
CSC-206	Network Operating System	6
CSC-207	Network & System Administration	6
CSC-208	Client Server Computing	6
CSC-209	Wireless and Mobile Communication	6
	Total	30

Semester 5

Course Code	Course Title	ECTS Credits
CSC-301	Network Security	6
CSC-302	Network Programming	6
CSC-303	Research Methodology	6
CSC-304	Fundamentals of Project Management	6
CSC-305	Network Management	6
	Total	30

Semester 6

Course Code	Course Title	ECTS Credits
CSC-306	Server Administration	6
CSC-307	Broadband Networks	6
CSC-308	Ethical hacking	6
CSC-309	Project I	6
	Elective I	6
	Total	30

Semester 7

Course Code	Course Title	ECTS Credits
CSC-401	Cyber Security & IOT	6
CSC-402	Artificial Intelligence	6
CSC-403	IT Acts and Cyber law	6
CSC-404	Project Dissertation – II	6
	Elective II	6
	Total	30

Semester 8

Course Code	Course Title	ECTS Credits

CSC-409	Organization Behavior and HRM	6
CSC-410	Industrial Training	12
	Elective III	6
	Elective IV	6
	Total	30
	Grand Total	240

Elective Courses

Subject Code	Subject	Group
CSC-310	Distributed Networking	Elective -I
CSC-311	E-Governance	
CSC-312	Data Center Design and Management	
CSC-313	Linux for system Administration	
CSC-405	Cryptography	Elective - II
CSC-406	E-Commerce	
CSC-407	Net Centric Design	
CSC-408	Security Audit	
CSC-411	GIS	Elective -III
CSC-412	Advance Java Programming	
CSC-413	Information Security	
CSC-414	Cyber Forensics	
CSC-415	Advanced Networking with IPv6	Elective-IV
CSC-416	Cloud Computing	
CSC-417	Introduction to Programming with Python	
CSC-418	Criminal Evidence and Procedures	