

LETTER OF OFFER – AI & CYBERSECURITY PROGRAMME 2024/2025

Issued by:

Masaryk University, Faculty of Informatics

Address: Botanická 554/68a, 602 00 Brno, Czech Republic

ID No.: 00216224

Bank account Nr.: 85636621/0100

Represented by: prof. RNDr. Jiří Barnat, Ph.D., Dean

Contact person:

(hereinafter referred to as “FI MU”)

and addressed to:

Foreign Training, HQ IDS

Room No. 1248

Hotel Ashoka

Chanakyapuri, New Delhi-110021

India

Represented by: Col KMN Kuttappa, Colonel, Foreign Training, HQ IDS.

Contact person:

(hereinafter referred to as “CFT”)

hereinafter jointly referred to as the “**parties**” and individually also as a “**party**”

I.

Subject of the Offer

1. The subject of this Offer is the participation of CFT nominated candidates in the “Long Term Course in Informatics with Specialization in AI and IT Security”, which is built of courses of accredited Master of Science (Magistr) programmes at FI MU. Hereinafter, the programme shall be referred to as AI-Sec Programme.
2. FI MU agrees to provide high quality training specified in the Article II of this Offer.

II.

Programme Courses

1. Content of the AI-Sec Programme

- *PA164 Learning and natural language*: Students will obtain knowledge about methods and tools for text mining and natural language learning. At the end of the course students should be able to create systems for text analysis by machine learning methods. Students are able to understand, explain and exploit contents of scientific papers from this area.
- *PV021 Neural Networks*: At the end of the course student will have a comprehensive knowledge of neural networks and related areas of machine learning. Will be able to independently learn and explain neural networks problems. Will be able to solve practical problems using neural networks techniques, both independently and as a part

of a team. Will be able to critically interpret third party neural-networks based solutions.

- *PA153 Natural Language Processing*: The course offers a deeper knowledge about the natural language processing using statistical algorithms and/or deep learning of neural networks. Working examples and applications are provided to illustrate selected methods. The students will learn about practical processing of texts. The students will be able to: understand text processing methods; design algorithms for classification of text, documents, sentences; understand the structure of question answering and machine translation systems; evaluate the quality of the natural language processing applications.
- *IA161 Practical Techniques of Natural Language Processing*: The course participants will have the opportunity to learn about, test and experiment with advanced techniques of natural language processing (NLP) and to develop an understanding of the limits of those techniques. The course aims to introduce current research issues, and to meet in practice with particular programming techniques used in language technology applications.
- *IV111 Probability in Computer Science*: At the end of the course student should have a broad knowledge and an ability of independent study of problems based on the probability theory and its computer science applications. Will be able to apply the results of the probability theory in practical examples. Should be able to learn independently new problems requiring knowledge of probability theory. Will be able to characterise basic principles of data compression and error correction. Should be able to apply information theory results in practice. Student is able: to define basic terms of the mentioned topics (e.g., random variable, expectation, variance, random process, Markov chain, channel capacity, code rate); to explain meaning on the terms on practical examples; to solve simple examples e.g. using linearity of expectation; to provide basic analysis on both discrete- and continuous-time Markov chains; to compute (conditional) expectation, mutual information, and entropy random variables with given probability distribution; to demonstrate basic proof mentioned during lectures.
- *IA174 Fundamentals of Cryptography*: The course covers theoretical foundations of cryptography, ranging from encryption and hashing primitives to more modern topics such as blockchain technologies. Students will learn why are the state-of-the-art cryptographic algorithms constructed in the way they are, and how to reason about their mechanics and security guarantees via the language of mathematics.
- *PV079 Applied Cryptography*: This course explores the issues of cryptography deployment issues, standards and applications. The course enhances students' working experience with up-to-date cryptosystems, and enables them to deploy cryptography effectively.
- *PA018 Advanced Topics in Information Technology Security*: This advanced-level course reviews selected topics in IT security in a greater depth. Students are expected to work on several assignments and a term project.
- *PV181 Laboratory of security and applied cryptography*: The aim of this lab course is to understand implementation details of cryptographic algorithms and protocols and be able to apply the gained knowledge in practice. At the end of the course students should be able to design and implement cryptographic applications independently, and possibly also with support of smartcards.

- *PA228 Machine Learning in Image Processing*: The objective of the course is to introduce approaches for solving common image processing problems using machine learning methods. At the end of the course students should be able to: understand, use, and evaluate machine learning models in the area of image processing; know how to employ pre-trained models using transfer learning; how to deal with big datasets that do not fit available memory; and how to prepare data to get relevant results. -
- *PV254 Recommender Systems*: The goal of the course is to familiarize students with basic techniques and problems in the field of recommender systems. The course is project based - students have practical experience with development of a simple recommender system or with a partial evaluation of a realistic recommender system. At the end of the course students will understand the main types of recommender systems and their application domains; be able to apply the basic recommender techniques; be able to implement basic versions of recommender techniques; understand main aspects of evaluation of recommender systems and be able to analyze such evaluations.
- *MV013 Statistics for Computer Science*: The main goal of the course is to become familiar with some basic principles of statistics, with writing about numbers (presenting data using basic characteristics and statistical graphics), some basic principles of likelihood and statistical inference; to understand basic probabilistic and statistical models; to understand and explain basic principles of parametric statistical inference for continuous and categorical data; to implement these techniques to R language; to be able to apply them to real data.
- *PV182 Human Computer Interaction*: The course deals with the basics of human-computer interaction and user-centered design. The focus is on theoretical foundations and practical experience with techniques and tools, psychological aspects, user interface design criteria, interface design, and evaluation of prototypes followed by the human-centered design process. The goal is to provide an overview of theoretical foundations and practical experience with human-computer interaction techniques and methods, emphasizing the Human-Centered Design Process. The students will become familiar with interface design principles current trends in HCI and gain hands-on experience through practical exercises and a semester-long team project.
- *PV204 Security Technologies*: The aim of this subject is to understand details of smart cards security, secure authentication and authorization, security of hardware modules, trusted boot, analysis of malware and rootkits (both black-box and gray-box), reverse engineering of binary applications, multilevel security and file/disk encryption. Student should be able to apply the gained knowledge in a practice based on experience gained from laboratory a project work.
- *PA193 Secure coding principles and practices*: Language level vulnerabilities, secure programming techniques and approaches, input processing, code checking, security testing, integrity of modules, concurrent issues, random number generation and usage, security primitives, security code review.
- *PA168 Postgraduate seminar on IT security and cryptography*: The seminar participants will discuss a broad range of topics in IT security and cryptography in a greater depth. PhD and Master's students undertaking research in these and closely related areas are expected to report on their work.
- *PA197 Secure Network Design*: Basic design requirements and principles (basic network architecture and functions, general requirements on the security and

reliability). Network specific faults, threats, and attacks. Security architectures (Secure and resilient routing, secure DNS, secure channels, trusted network access, resilient architectures). Operational security management – how to design and manage reliable networks. Network monitoring and defence mechanisms (firewalls, IDS, netflow). Penetration testing. WiFi networks and security. (Wireless) personal area networks. Wireless Sensor Networks (WSN). Cryptographic aspects of WSN.

- **Other courses**, where the students will be free to select any courses listed for the current academic year at the webpages of FI MU.

III.

Letter of Offer and Acceptance Letter

1. The Letter of Offer from FI MU is based on a discussion of the Liaison Coordinators (see Section V below), with the following details:
 - a. 4 offered positions for students from CFT in the AI-Sec Programme.
 - b. Cost per participant for the AI-Sec Programme shall be 240'000 (two-hundred-and-forty-thousands) Czech korunas. The total cost is therefore 960'000 Czech korunas.
 - c. Starting date 9/9/2024 and final month of June 2025.
2. The Acceptance Letter must be received within two weeks of the issue date of a given Letter of Offer in order to take effect.
3. Letter of Offer and the corresponding Acceptance Letter based on the Appendix A of this Letter of Offer received within a month of the date of a given Letter of Offer then form a mutual written agreement.

IV.

Price of Work and Payment Conditions

1. The Contracting Parties have agreed that the total price for each run of a designated programme specified in Article II and performed under conditions agreed in this Agreement amounts will be specified in Czech korunas in the amendments set in Article III.
2. The CFT agrees to pay this price upon invoices issued by FI MU. The date of issue of the invoice is also the date of the taxable transaction.
3. The Parties have agreed that an invoice shall be due within 45 days after the date of issue at FI MU, where FI MU guarantees the invoice delivery to the CFT contact address (email and postal addresses) within 15 business days of the invoice issue.
4. The total price agreed in Article III shall be invoiced in two payments. The first payment of half of the total price will be invoiced within one month of the start of the program.
5. The second payment of half the total price will be invoiced within one month of the end of the program completion in June of the specific program run.
6. If CFT shall be in default with the payment of the Price agreed in the Article IV.1, the FI MU shall be entitled to require from CFT the penalty equal to 0,05 % from the due amount for each such day of default.
7. The provision regarding the penalty shall in no way affect the right of the Contracting

Parties in respect to indemnity.

V.

Liaison Coordinators

1. Each Party nominates a Liaison coordinator who shall act as a contact person for all matters concerning this Agreement.
2. The Liaison coordinator on behalf of FI MU is XXXXXXXXXXXX, the Liaison coordinator on behalf of CFT is XXXXXXXXXXXX.

VI.

Admission to the courses

1. Candidates will meet the following selection criteria for the Special Long Term programme of FI MU:
 - 1/ Completed Bachelor or Master degree in Computer Science / Computer Engineering / Computer Communications / Mathematics.
 - 2/ Extensive knowledge of Computer Science & Engineering
 - 3/ Basic knowledge of Cryptography and Computer Security
 - 4/ Academic track record, performance and English proficiency.
2. The participating students will be selected and admitted by FI MU on the recommendation of CFT.
3. The deadline for sending in the completed applications for eligible candidates shall be no later than May 20, 2024.
4. FI MU shall inform CFT of its final admission decisions within a month of the application of the candidates being made available to FI MU.
5. Students shall be subject to the rules, regulations and discipline of the FI MU. While registered in the courses within the programmes concerned, they will be registered as students of FI MU.

VII.

Dispute Resolution and Governing Law

1. Any dispute arising out of this Agreement shall be referred for resolution in the first instance to the liaison coordinators referred to in clause V.
2. If the dispute has not been settled sixty days after referral to them or within such other period as the parties may agree in writing, all disputes that may arise in connection with this present Agreement or the breach thereof shall be adjudicated exclusively by the Czech courts.
3. The contracting parties are aware of the requirements under the Czech Act no. 340/2015 Coll., on Special Conditions for Effectiveness of Some Contracts, Disclosure of These Contracts and on Registry of Contracts (Registry of Contracts Act), and if it is necessary according to this Act to publish this agreement, the contracting parties agree with its

publication in the registry of contracts, as well as with the publication of any agreements (amendments), which supplement, change, replace or cancel this agreement. The contracting parties agree that the publication of the agreement in accordance with the above-mentioned Act is ensured by FI MU.

VIII.
Final provisions

1. The Parties declare that the laws of the Czech Republic are applicable to this Letter of Offer and the resulting agreement and to the legal relationship between the Parties resulting from it.

**Masaryk University,
Faculty of Informatics**

In Brno on 17. 5. 2024

prof. RNDr. Jiří Barnat, Ph.D.,
Dean

**Appendix A: ACCEPTANCE LETTER– CYBERSECURITY PROGRAMME
2024/2025**

On behalf of CFT and with respect to the “LETTER OF OFFER – AI & CYBERSECURITY PROGRAMME 2024/2025”, from Masaryk University, Faculty of Informatics, dated May 17, 2024, I hereby confirm acceptance of the proposal from the Letter of Offer regarding the training in the “Long Term Course in Informatics with Specialization in AI and IT Security” and confirm that the conditions as stated in that Letter of Offer are accepted on our side without any modifications.

Foreign Training, HQ IDS (CFT)
Room No 1248
Hotel Ashoka
Chanakyapuri, New Delhi-110021
India

In New Delhi on _____

Col KMN Kuttappa