



Co-funded by the
Erasmus+ Programme
of the European Union



lmpi

licence master professionnel
en protection informatique

LMPI - N°573901-EPP-1-2016-1-IT-EPPKA2-CBHE-JP

“Licence, Master professionnels pour le développement, l’administration, la gestion, la protection des systèmes et réseaux informatiques dans les entreprises en Moldavie, au Kazakhstan, au Vietnam”

Dossier d'accréditation

Grade:	Ingénieur en sécurité informatique	Domaine:	061 Technologies de l'information et de la communication
Mention:	Études de licence		

Université:	Université Technique de Moldova	Département:	Ingénierie de logiciels et Automatique
Date de conception:	25.02.2018		

Rédacteurs:	Besliu Victor	Moraru Victor	Bulai Rodica
-------------	---------------	---------------	--------------

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



Co-funded by the
Erasmus+ Programme
of the European Union



**LMPI - Licence, Master professionnels pour le développement, l'administration,
la gestion, la protection des systèmes et réseaux informatiques
dans les entreprises en Moldavie, au Kazakhstan, au Vietnam**

Project N° 573901-EPP-1-2016-1-IT-EPPKA2-CBHE-JP

PROTOCOL OF PROJECT DOCUMENT VALIDATION

PROCES VERBAL DE VALIDATION DE DOCUMENT DU PROJET

Work Package/lot	3
Activity/Activité	3.3
Name of the activity/ Nom de l'activité	Accreditation files Licence/ Master
Name of the document/ nom du document:	Accreditation files Licence Accreditation files Master
Partner(s) concerne/partenaire(s) concerné(s)	P09 Technical University of Moldova P10 Alecu Russo Balti State University P11 Moldova State University P12 Academy of Economic Studies of Moldova
Referent EU University/université UE référente	P04 University of West Attica
Person validating the document/personne qui valide le document	
Name/nom	Panayotis Yannakopoulos
Function/fonction	Professor

Date:

21.06.2019

Signature:

I. Contexte

La cybersécurité et la sécurité des informations est accentuée par des phénomènes caractéristiques de la société d'aujourd'hui, tels que la globalisation et l'établissement de la société de l'information, les faiblesses de l'économie virtuelle liées à la nature immatérielle des valeurs du cyberspace, l'anonymat et de la nature transfrontalière, l'évolution de la criminalité électronique et sa dynamique.

La criminalité cybernétique coûte les économies du monde entier approximativement 600 milliards de dollars par an, soit 0,8% du PIB mondial selon une étude récente publiée par la société McAfee, spécialisée dans la protection contre les attaques informatiques et par le centre de réflexion Center for Strategic and International Studies (CSIS). Le domaine fait face à une pénurie croissante de professionnels qualifiés et de praticiens expérimentés dans la sécurité de l'information. Pour l'année 2022, près de 1,8 million de postes de sécurité informatique sont estimés mais ils ne devraient pas être couverts. La demande de main-d'œuvre est aiguë, immédiate et croissante. Dans ce contexte, la formation des spécialistes dans le domaine de la sécurité de l'information et des responsables de la sécurité des systèmes d'information est une priorité nationale, demandée à la fois par les médias gouvernementaux ainsi que par l'administration centrale ou locale mais aussi par le secteur privé - entreprises, banques, etc.

Le programme de licence vise à atteindre les objectifs suivants :

- Acquérir des connaissances sur les menaces, les vulnérabilités et les risques de sécurité propres aux systèmes d'information ;
- Vous familiarisez avec les dernières technologies avancées utilisées pour assurer la sécurité de l'information ;
- Apprendre des normes et des standards nationaux et internationaux dans le domaine de la sécurité de l'information ;
- Comprendre les méthodologies et les schémas d'audit, de certification et d'accréditation de la sécurité des produits et des systèmes d'information ;
- Identifier et résoudre les problèmes liés à l'acquisition, à la mise en œuvre et à l'exploitation de solutions de sécurité de l'information ;
- Développer des connaissances et des compétences en matière de gestion de la sécurité de l'information, des ressources techniques et humaines nécessaires à l'assurance d'informations ;
- Acquérir la capacité de diriger des groupes de travail ou des équipes de spécialistes en sécurité de l'information ;
- Développer des compétences pour la conception des études et des rapports techniques.

La licence en Sécurité de l'Information est basée sur l'expérience d'enseignement et de la recherche dans le domaine de la sécurité de l'information des enseignants de l'Université Technique de Moldavie. Des professeurs associés des autres universités ou professionnels avec une vaste expérience pratique, qui mènent leurs activités dans des structures commerciales et gouvernementales de sécurité nationale ou dans des entreprises privées seront également invités aux conférences et aux démonstrations pratiques.

L'enquête du projet Erasmus+ "Licence, Masters professionnels pour le développement, l'administration, la gestion, la protection des systèmes et réseaux informatiques dans les entreprises en Moldavie, au Kazakhstan, au Vietnam" a identifié une grande pénurie de professionnels qualifiés dans la sécurité de l'information et une forte demande en

spécialistes de haut niveau dans ce domaine, fait qui garantit l'insertion professionnelle des diplômés.

La licence en sécurité de l'information s'adresse aux diplômés des lycées possédant un BAC qui souhaitent devenir des spécialistes dans le domaine de la sécurité des informations. L'admission aura lieu conformément à la réglementation en vigueur, un concours annuel sera annoncé pour le recrutement de 25-50 étudiants, à ce qui concerne l'enseignement à distance, il n'y aura aucune restriction sur le nombre de places disponibles ou d'âge des candidats.

II. Descriptif général du curriculum

• II.1. Description des acquis de formation :

La sécurité de l'information est une spécialité qui implique des technologies, des personnes, des informations et des processus dans le but de permettre des opérations sécurisées dans un contexte incertain en analysant, testant, créant et en exploitant des systèmes d'information sécurisés. C'est une spécialité interdisciplinaire qui comprend des questions liées à la technologie, au droit, à la politique, aux facteurs humains, à l'éthique et à la gestion des risques.

Les acquis de formation	Descriptif
Les savoirs disciplinaires	Connaissance de l'entreprise, ses services/produits, sa structure, son organisation, son environnement juridique. Vision globale et complète des systèmes d'information e l'entreprise, des organisations similaires. Connaissance technique approfondie des concepts et techniques d'architecture des systèmes et réseaux, procédures d'exploitation et des standards d'échange des données employées, procédures de Sécurité informatique, systèmes d'exploitation et langages de programmation associés, bases de données.
Les compétences spécifiques	Les fondements scientifiques et techniques de la sécurité informatique. Les aspects organisationnels et informationnels de la SI. Les mesures de sécurité et de contrôle. Les méthodes et technologies pour développer des solutions de sécurité. L'architecture de sécurité et l'infrastructure Savoir-faire pratique et expérience rédactionnelle : actualités/brèves, articles de fond, dossiers. Maîtrise expérimentée «terrain» de l'outil informatique : architecture des systèmes et réseaux, procédures d'exploitation et des standards d'échange des données employées, procédures de sécurité informatique, systèmes d'exploitation (Solaris, Linux) et des langages de programmation associés. Maîtriser les outils bureautiques : traitement de texte, tableur, outil de présentation. Utilisation de logiciels spécifiques : outils de chiffrement de disques durs ou de serveurs, Pare feu (Firewalls), outils d'identification.

Les compétences transversales

"Leadership" et esprit d'entreprise. Adaptabilité et flexibilité. Analyse et synthèse. Communication orale et écrite. Conviction et Influence. Créativité, sens de l'innovation. Gestion de projet. Gestion de la performance. Orientation client. Rigueur et organisation. Sens relationnel. Travail et animation d'équipe.

II.2. La décomposition du curricula en semestres

Premier semestre

#	Titre du cours/module	Type du cours	Nr. de credits	Forme de verification	Nr. d'heures		
					Cours	Lab/Se m	Total
UE1	Mathématiques 1	Obligatoire	6	E	45	45	90
UE2	Mécanique	Obligatoire	4	E	30	30	60
UE3	Infographie	Obligatoire	3	E	15	30	45
UE4	Programmation	Obligatoire	6	E	30	60	90
UE5	Philosophie	Obligatoire	4	E	30	30	60
UE6	Étique, communication et droit	Obligatoire	5	E	45	30	75
UE7	Langue étrangère	Obligatoire	2	E		30	30

Deuxième semestre

#	Titre du cours/module	Type du cours	Nr. de credits	Forme de verification	Nr. d'heures		
					Cours	Lab/Se m	Total
UE8	Mathématiques 2	Obligatoire	5	E	45	30	75
UE9	Physique	Obligatoire	6	E	45	45	90
UE10	Mathématiques spéciales	Obligatoire	6	E	45	45	90
UE11	Structure de données et algorithmes	Obligatoire	5	E	30	45	75
UE12	Les fondements économiques de la branche	Obligatoire	6	E	60	30	90
UE13	Langue étrangère	Obligatoire	2	E		30	30

Troisième semestre

#	Titre du cours/module	Type du cours	Nr. de credits	Forme de verification	Nr. d'heures		
					Cours	Lab/Se m	Total
UE14	Électronique	Obligatoire	5	E	45	30	75
UE15	Méthodes et modèles de calcul	Obligatoire	6	E	60	30	90
UE16	Analyse et synthèse des dispositifs numériques	Obligatoire	5	E	45	50	75
UE17	Analyse et conception d'algorithmes	Obligatoire	4	E	30	30	60

UE18	Langages formels et automates	Obligatoire	5	E	30	45	75
UE19	Programmation orientée objets	Obligatoire	5	E	30	45	75

Quatrième semestre

#	Titre du cours/module	Type du cours	Nr. de credits	Forme de verification	Nr. d'heures		
					Cours	Lab/Se m	Total
UE20	Architecture d'ordinateurs	Obligatoire	4	E	30	30	60
UE21	Cadre légal de la sécurité d'informations	Obligatoire	3	E	30	15	45
UE22	Réseaux d'ordinateurs	Obligatoire	4	E	30	30	60
UE23	Analyse et modélisation orientée objet	Obligatoire	6	E	45	45	90
UE24	Les bases de la sécurité d'information – Sécurité des systèmes informatiques	Obligatoire	4	E	30	30	60
UE25	Logiciels malicieux et antivirus	Obligatoire	5	E	45	30	75

Cinquième semestre

#	Titre du cours/module	Type du cours	Nr. De credits	Forme de verification	Nr. D'heures		
					Cours	Lab/Se m	Total
UE26	Management and Marketing	Obligatoire	6	E	45	45	90
UE27	Sécurité de l'activité vitale	Obligatoire	3	E	30	15	45
UE28	L'administration et l'audit de la sécurité d'informations	Obligatoire	5	E	45	30	75
UE29	Bases de données	Obligatoire	6	E	45	45	90
UE30	Programmation des applications mobiles	Obligatoire	5	E	45	30	75
UE31	Systèmes d'exploitation	Obligatoire	5	E	45	30	75

Sixième semestre

#	Titre du cours/module	Type du cours	Nr. De credits	Forme de verification	Nr. D'heures		
					Cours	Lab/Se m	Total
UE32	Cybercriminalité et techniques d'investigation	Obligatoire	4	E	30	30	60
UE33	Programmation réseaux	Obligatoire	4	E	30	30	60
UE34	Techniques et mécanismes de sécurité dans la conception des logiciels	Obligatoire	5	E	30	45	75
UE35	Méthodes cryptographiques de la protection d'information	Obligatoire	4	E	30	30	60
UE36	Reverse engineering	Obligatoire	4	E	30	30	60
UE37	Vérification et validation des logiciels	Obligatoire	5	E	30	45	75

Septième semestre

#	Titre du cours/module	Type du cours	Nr. De credits	Forme de verification	Nr. D'heures		
					Cours	Lab/Se m	Total
UE38	La conception des systèmes informatiques	Obligatoire	6	E	45	45	90
UE39	Méthodes et moyens techniques pour la protection d'information	Obligatoire	4	E	30	30	60
UE40	Internet of Things (IoT)	Obligatoire	5	E	45	30	75
UE41	Programmation d'applications distribuées	Obligatoire	5	E	45	30	75
UE42	Qualité du logiciel	Obligatoire	5	E	30	45	75
UE43 /1	Administration des réseaux d'ordinateurs	Au choix	5	E	30	45	75
UE43 /2	Administration et sécurité des réseaux informatiques	Au choix	5	E	30	45	75

Huitième semestre

#	Titre du cours/module	Type du cours	Nr. de credits	Forme de verification	Nr. d'heures		
					Cours	Lab/S em	Total
1.	Stage de fin d'études, conception du mémoire	Obligatoire	25	E			840
2.	Examen final		4	E			120
3.	Soutenance de la thèse de licence		1	E			30

II.3. Tableau de mise en corrélation entre compétences et unités d'enseignement :

Le tableau de mise en corrélation entre compétences et unités d'enseignement est présenté ci-dessous :

	C1	C2	C3	C4	C5
UE1		x	x		x
UE2		x	x		x
UE3		x	x		
UE4	x		x	x	x
UE5				X	x
UE6	x	x	x	x	x
UE7	x			x	
UE8	x		x	x	
UE9	x	x	x	x	x
UE10	x	x	x		
UE11		x	x		x

UE12	x	x		x	x
UE13			x		x
UE15	x		x		x
UE16	x	x	x		x
UE17	x		x		x
UE18	x		x	x	x
UE19	x		x		x
UE20	x	x	x		
UE21	x	x			x
UE22	x		x		x
UE23	x	x			x
UE24	x		x	x	
UE25	x		x		x
UE26	x	x	x	x	x
UE27	x		x		x
UE28	x	x			x
UE29			x	x	x
UE30	x	x	x		x
UE31	x	x	x		x
UE32	x		x		x
UE33	x		x		x
UE34	x		x		x
UE35	x	x		x	x
UE36	x		x		x
UE37	x	x			x
UE38	x		x		x
UE39	x		x	x	x
UE40	x		x		x
UE41	x		x		x
UE42	x	x	x		x
UE43/1	x	x	x	x	x
UE43/2	x	x	x	x	x

II.4. Le projet tutoré

Le projet tutoré s'inscrit pleinement dans la professionnalisation des étudiants. Il permet aux étudiants de s'engager sur un temps long dans un travail collaboratif (de groupe) qui œuvre à la réalisation d'un projet en réponse à une étude de cas proposée par l'encadrant universitaire et par le tuteur entreprise.

Le projet tuteuré comporte trois dimensions complémentaires :

- il implique en effet la conception, la mise en œuvre et l'évaluation d'un projet qui repose sur un problème validé en formation ;
- il se traduit par la rédaction d'un rapport satisfaisant à l'ensemble des exigences universitaires ;
- il donne lieu enfin à une soutenance comportant un exposé suivi d'un entretien avec le jury.

Plus précisément, il s'agira à travers ce dispositif pédagogique de permettre aux étudiants :

- d'approfondir leur champ de connaissances des secteurs et contextes de la communication publique;
- d'apprendre à gérer un projet de communication de manière autonome dans le cadre de travail en équipe ,
- de gérer le travail de groupe et le calendrier des activités ;
- de développer des capacités d'analyse, d'enquête et de recommandations ;

Le projet tutoré permet aux étudiants de :

- mettre en pratique les savoirs acquis au cours de la formation,
- travailler au sein d'une équipe sous contrainte de temps et de moyens,
- démontrer leurs capacités d'initiative, d'autonomie et de responsabilité,
- répondre à une demande réelle en analysant une situation et en proposant une solution adaptée.

Ses principales tâches des encadrants (tuteurs universitaire et entreprise) sont :

- valider dès le début la proposition de projet du groupe d'étudiants, notamment sa faisabilité ;
- orienter les étudiants vers des ressources ;
- donner des conseils en terme d'organisation ;
- valider la répartition des tâches au sein du groupe et la planification ;
- évaluer les rapports intermédiaires et les rendus finaux.

Le but principal du projet tutoré est : à partir d'une problématique clairement identifiée (une étude de cas), l'étudiant doit concevoir une réponse cohérente basée sur les connaissances acquises pendant les cours théoriques.

Les étudiants sont évalués sur leur capacité à proposer une solution crédible, réaliste, adaptée. Pour ce faire, il mobilise l'ensemble des connaissances théoriques acquises durant la formation. Ils réalisent l'ensemble des opérations liées à la conception et à la mise en œuvre de leur projet : identification, analyse, recherche des solutions possibles, choix d'une solution, critères et conditions de mise en œuvre, mise en œuvre, mesure d'efficacité, actions correctrices...

Les résultats du projet tutoré sont présentés sous forme d'un rapport écrit qui sera soutenu devant un jury composé de deux enseignants de l'équipe pédagogique et éventuellement du

tuteur en entreprise. La soutenance comprend successivement un exposé de l'étudiant suivi d'un entretien avec le jury, elle a pour objectif d'approfondir, compléter, enrichir le rapport.

L'étudiant est donc invité à construire un exposé, appuyé par un diaporama de présentation, qui ne soit pas une répétition du rapport, ni sur le fond, ni sur la forme. Il s'exprime pendant environ dix minutes. A la suite de sa présentation, une dizaine de minutes est consacrée à des questions-réponses avec le jury. Celles-ci peuvent porter sur l'exposé, le rapport, et plus largement sur les acquis de l'étudiant au terme de l'année.

L'entreprise fournit une appréciation qui se traduit par un bonus sur la note globale.

La délibération se fait hors de la présence de l'étudiant. En vue de permettre une harmonisation éventuelle des jurys, les notes ne lui sont pas communiquées à l'issue de la soutenance.

Le projet tutoré se déroule pendant le deuxième semestre d'études et il vaut 5 ECTS.

II.5. Le stage en entreprise

Les stages de fin d'études visent l'approfondissement des connaissances théoriques, l'acquisition des compétences pratiques de travail dans les organisations d'état, publiques ou privées. L'organisation des stages est réalisée en conformité avec les documents normatifs de l'UTM.

Le stage en entreprise est prévu pendant le troisième semestre et vaut 28 ECTS est sa durée est de 15 semaines. Une convention-type entre UTM est l'organisme d'accueil doit être signée avant le début du stage.

Les types d'entreprises d'accueil : institution bancaires et financières, entreprises de production, compagnie du domaine TIC, etc., l'emploi à occuper : expert en sécurité de systèmes d'information et des réseaux

Les modalités de suivi des stages en entreprise : le professeur référent du stage visite régulièrement le stagiaire et l'aide de mettre en place le travail proposé par le tuteur, le tuteur en entreprise propose les sujets et le cahier de charges pour le stage, surveille quotidiennement le travail du stagiaire, l'aide de surmonter les difficultés rencontrées, veille au respect des règlements en cours, etc.

A la fin du stage l'étudiant présente ses résultats sous forme d'un mémoire du stage in y incluant les résultats les plus pertinents ainsi que l'avis de son tuteur de stage.

Le nombre d'ECTS prévus pour le stage est en adéquation avec le contenu des autres enseignements, les compétences professionnelles visées et l'investissement en temps de travail nécessité par le stage. Une modulation des ECTS peut être opérée, selon sa nature (observation, application, responsabilité...), sa durée et sa période dans l'année. Une préparation à l'insertion professionnelle et à la recherche de stage est proposée dans les cursus.

Le jury de stage est constitué de deux membres au minimum dont au moins un enseignant de la formation. La participation d'un représentant de l'organisme d'accueil est vivement recommandée.

La note de stage comporte plusieurs évaluations : l'évaluation du rapport écrit et de la soutenance orale, l'évaluation par l'organisme d'accueil des compétences professionnelles et du comportement de l'étudiant. Une pondération peut être prévue entre ces différentes évaluations. Les différents aspects de ces évaluations figurent sur la convention de stage.

L'évaluation des stages réalisés dans le cadre de la licence relève de dispositions spécifiques qui doivent être précisées aux étudiants en début d'année universitaire.

II.6. Le stage à l'international

Le stage de fin d'études peut être organisé sous forme d'une mobilité à l'étranger sous financement dans le cadre des projets scientifiques en cours dont UTM fait part (Erasmus +, Horizon 2020 , AUF, etc.) ou par l'obtention des bourses et des grants proposés par des organismes internationaux (tel que AUF, ambassades, etc.). Dans ce but UTM a signé plus de 150 accords de coopération bilatérale avec des universités, des centres scientifiques et des entreprises des pays membres de l'Union européenne (Belgique, République tchèque, Allemagne, Grèce, France, Italie, Grande-Bretagne, Pologne, Portugal, Roumanie, Espagne, Suède, Hongrie), Canada, Biélorussie, Fédération de Russie, Turquie, Ukraine. UTM est membre d'organisations académiques internationales comme l'Agence Universitaire de la Francophonie (1996), le Réseau des universités de la mer Noire (1997), le Réseau international pour l'éducation en matière de sécurité nucléaire, etc.

Le contenu de ce stage, sa durée, le nombre d'ECTS attribués et les modalités de son évaluation sont similaires au stage en entreprise.

II.7. Les mobilités vers les entreprises étrangères (le cas échéant)

Des mobilités vers des entreprises étrangères ne sont pas directement prévues dans le cadre de cette licence, mais il est tout à fait possible de les organiser sous réserve d'un financement par un organisme externe, par un projet ou par l'entreprise elle-même.

III Modalités de contrôle des connaissances

La licence est constituée de 90 ECTS. La formation dispensée comprend des enseignements théoriques, méthodologiques et appliqués et un stage, ainsi qu'une initiation à la recherche.

Les études de licence sont structurées en semestres et en unités d'enseignement (UE) capitalisables

Dans chaque UE, les aptitudes et l'acquisition des connaissances sont appréciées par un contrôle continu et par un examen terminal. La forme du contrôle (épreuve écrite, orale, pratique, soutenance, etc.) est décidée par l'équipe pédagogique en fonction des spécificités de l'UE.

La prise en compte de l'assiduité aux TD/TP dans l'évaluation de l'UE est laissée à l'appréciation des membres de l'équipe pédagogique ou précisée dans les modalités de contrôle des connaissances spécifiques de la formation.

Une UE est acquise si sa moyenne est supérieure ou égale à 5/10. L'acquisition de l'unité d'enseignement emporte l'acquisition des crédits européens (ECTS) correspondants. Une UE capitalisée ne peut pas être repassée ultérieurement.

Chaque semestre doit être validé par un jury. La validation d'un semestre permet l'acquisition de 30 ECTS. Le contrôle des connaissances des formations définit les modes de validation des semestres notamment les règles de compensation à l'intérieur du semestre et les règles de rattrapage.

L'année est validée lorsque chacun des deux semestres est validé. Il n'y a pas de compensation possible entre les semestres.

Le licence est délivré aux étudiants ayant validé toutes les UE constitutives d'un parcours type tel que défini par la maquette.

L'évaluation des mémoires est effectué par un jury de mémoire constitué d'au moins deux enseignants de la formation. L'évaluation du mémoire peut comporter plusieurs notes (mémoire, soutenance orale, etc.). Une pondération peut être prévue entre les différentes notes.

Les soutenances sont publiques sauf en cas de confidentialité.

IV Composition de l'équipe pédagogique

a) Le responsable pédagogique général du nouveau curriculum

Nom : **Bulai** Prénom : **Rodica** Fonction : **enseignant-chercheur** Université : **UTM**

b) Les responsables pédagogiques par unités d'enseignement

UE	Responsable d'UE	Université de rattachement
UE1	Maître de conf.,dr. Costaş Ana	UTM
UE2	Maître de conf.,dr. Balmus Ion	UTM
UE3	Maître de conf.,dr. Dîntu Serghei	UTM
UE4	Maître de conf., dr. Carcea Liviu	UTM
UE5	Maître de conf.,dr. Ţurcan Iuliu	UTM
UE6	Maître de conf.,dr. Braga Mihail	UTM
UE7	Maître de conf.,dr.,Vangheli Ion	UTM
UE8	Maître de conf.,dr. Costaş Ana	UTM
UE9	Enseignant-chercheur Ceban Gheorghe	UTM
UE10	Maître de conf.,dr. Tronciu Vasile	UTM
UE11	Maître de conf.,dr. Carcea Liviu	UTM
UE12	Enseignant-chercheur Dodu Aliona	UTM
UE13	Enseignant-chercheur Tăriță Stela	UTM
UE14	Maître de conf.,dr. Mironov Bettin	UTM
UE15	Maître de conf.,dr. Tutunaru Eleonora	UTM
UE16	Maître de conf.,dr. Sudacevschi Viorica	UTM
UE17	Enseignant-chercheur Catruc Mariana	UTM

UE18	Maître de conf.,dr. Cojuhari Irina	UTM
UE19	Maître de conf.,dr. Kulev Mihail	UTM
UE20	Maître de conf.,dr. Postovan Dumitru	UTM
UE21	Enseignant-chercheur Mocanu Veronica	Service de protection de données personnelles
UE22	Enseignant-chercheur Dinu Turcanu	UTM
UE23	Enseignant-chercheur Melnic Radu	UTM
UE24	Enseignant-chercheur Bulai Rodica	UTM
UE25	Enseignant-chercheur Mitev Constantin	Service TI du MAI
UE26	Enseignant-chercheur Grigoraș Maria	UTM
UE27	Enseignant-chercheur Benchici Mihai	UTM
UE28	Enseignant-chercheur Bulai Rodica	UTM
UE29	Maître de conf.,dr. Cotelea Vitalie	UTM
UE30	Enseignant-chercheur Antohi Ionel	UTM
UE31	Maître de conf.,dr. Besliu Victor	UTM
UE32	Maître de conf.,dr. Putere Alexandru	Service TI du MAI
UE33	Enseignant-chercheur Antohi Ionel	UTM
UE34	Maître de conf.,dr. Ababii Victor	UTM
UE35	Maître de conf.,dr. Besliu Victor	UTM
UE36	Enseignant-chercheur Catanoi Maxim	Endava
UE37	Enseignant-chercheur Catruc Mariana	UTM
UE38	Maître de conf.,dr. Chirev Pavel	UTM
UE39	Enseignant-chercheur Postaru Andrei	UTM
UE40	Enseignant-chercheur Turcanu Dinu	UTM
UE41	Maître de conf.,dr. Ciorba Dumitru	UTM
UE42	Enseignant-chercheur Catruc Mariana	UTM
UE43/1	Enseignant-chercheur Calin Rostislav	UTM
UE43/2	Enseignant-chercheur Calin Rostislav	UTM

c) Professeurs intervenant dans le curriculum

Nom prénom	Université	Disciplines enseignées	Nombre d'heures d'intervention	UE concernées
Bulai Rodica	UTM	Bases de données, Sécurité des systèmes informatiques	135	UE24, UE29

d) professionnels intervenant dans le curriculum

Nom prénom	Entreprise	Disciplines enseignées	Nombre d'heures d'intervention	UE concernées
Cernei Valeriu	BSD Management	L'administration et l'audit de la sécurité	75	UE28

		d'informations		
Putere Alexandru	Serviciul TI al MAI	Cybercriminalité et techniques d'investigation	60	UE32
Mitiev Constantin	Serviciul TI al MAI	Logiciels malicieux et antivirus	75	UE25
Catanoi Maxim	Endava	Reverse engineering	60	UE36
Mocanu Veronica	Centrul National de protectie a datelor cu caracter personal	Logiciels malicieux et antivirus	45	UE21

V Insertion professionnelle

La sécurité de l'information est le sujet très sollicité dans le contexte actuel où la cybercriminalité est devenue omniprésente dans tous les domaines. Pendant les cinq dernières années la demande de professionnels de la sécurité de l'information a augmenté de 3,5 fois plus vite que la demande des autres emplois informatiques et de 12 fois plus vite que tous les autres emplois. Aujourd'hui, les entreprises placent la sécurité de l'information parmi leurs principales priorités et environ 54% des organisations ont un responsable de la sécurité de l'information.

La classification des professions en République de Moldova approuvée le 03.03.2014 par le gouvernement contient, parmi les autres, le grand sous-groupe 25 "*Spécialistes des technologies de l'information et de la communication*" avec des groupes minoritaires 251203 "*Analyse pour la sécurité des systèmes d'information*"; 251403 "*Spécialiste des procédures et des outils de sécurité pour les systèmes d'information*"; 251903 "*Consultant pour la sécurité des systèmes informatiques*"; 252901 "*Ingénieur en sécurité de l'information*", ainsi que d'autres groupes et sous-groupes, tels que 2412 "*Spécialistes et consultants dans le domaine de la finance et de l'investissement*" - 241233 "*Agent de sécurité*"; 121113 "*Information Security Manager*" couvre les principales fonctions / professions des diplômés du programme de sécurité de l'information.

Tenant compte des compétences du programme de sécurité de l'information, les diplômés de la licence peuvent occuper d'autres fonctions que celles mentionnées : des ingénieurs de gestion de différents niveaux.

L'équipe pédagogique du programme Sécurité de l'information en accord avec la politique globale adoptée à l'UTM a mis en place une cellule d'aide à l'insertion, dispositif pour aider à l'insertion professionnelle des étudiants et des jeunes diplômés qui inclut la recherche de stage en entreprise, l'organisation périodique d'ateliers sur la technique de recherche d'emplois, une base de données sur les entreprises spécialisées dans le domaine a été mise en place. Chaque année un salon sur la recherche d'emplois est organisé à l'UTM avec la participation des entreprises et des professeurs du département visant l'établissement des contacts des étudiants et des jeunes diplômés avec le monde professionnel.

VI Le supplément au diplôme

Chaque diplômé obtient le diplôme en deux langues : en roumain et en anglais, et le supplément au diplôme, qui est également rédigé en roumain et en anglais. Le complément est structuré conformément aux recommandations de la Commission européenne et le Règlement sur l'organisation de l'examen final de baccalauréat à l'UTM approuvé par le Sénat. Il contient des informations sur les compétences acquises, les crédits d'études accumulés, les notes de promotion aux sujets étudiés, etc. Diplôme et supplément au diplôme programme d'études de licence correspondent aux modèles des diplômes et des suppléments dans l'enseignement supérieur approuvé par le ministère de l'éducation de Moldavie.

Annexe 1 : Le partenariat avec les établissements de formation

1.1. Les universités concourant à la formation

Universités	Rôle dans la formation
ASEM	Enseignement des cours
USM	Enseignement des cours

Joindre les conventions.

1.2. Les collèges concourant à la formation

Collèges	Rôle dans la formation

Joindre les conventions.

Annexe 2 : Le partenariat avec les entreprises

2.1. Les entreprises concourant à la formation

Entreprises	Rôle dans la formation
Endava	Enseignement des cours, accueil de stagiaires
Pentalog	Accueil de stagiaires
BSD Management	Enseignement des cours, accueil de stagiaires

Joindre les conventions.

2.2. Autres entreprises soutenant la formation

Entreprises	Adresses
Fiscservisinform ÎS	
SA Moldotelecom	
ÎCS Red Union Fenosa SA	
SA Moldoincombank	
Dekart SRL	
EST Computers SRL	
MR Crystal System SRL	
BM Public SRL	
Centrul de guvernare	

electronică	
Centrul de Telecomunicații Speciale	
Banca națională a Moldovei	
Reliable Solutions Distributor	
Bitdefender, Romania	
Nec Corporation, Romania	

Joindre les lettres d'appui.

Annexe 3 : Fiche métier



Co-funded by the
Erasmus+ Programme
of the European Union



LMPI - N°573901-EPP-1-2016-1-IT-EPPKA2-CBHE-JP

“Licence, Master professionnels pour le développement, l’administration, la gestion, la protection des systèmes et réseaux informatiques dans les entreprises en Moldavie, au Kazakhstan, au Vietnam”

Fiche métier : Responsable de la Sécurité de l’Information

Intitulé du métier	Responsable de la Sécurité des Systèmes d'Information (RSSI) Manager de la Sécurité et des Risques de l'Information (MSRI) Délégué à la protection des données
Autres appellations (en)	Responsible for the Security of Information Systems Data Protection Officer
Mission	Le Responsable Sécurité de l'Information intervient comme expert métier sur les processus de l'entreprise sur des questions de sécurité. Il aide et conseille les entreprises à assurer la sécurité de leurs données et de leurs systèmes. Il assure le contrôle permanent de l'activité et définit les exigences de sécurité associées. Il définit la politique de gestion des risques de l'information dans l'entreprise, du déploiement et de l'animation du dispositif de gestion des risques.
Activités principales	Définir la gouvernance de la sécurité de l'information au sein de l'entreprise et dans l'entreprise élargie Définir et piloter le dispositif de sécurité (normes, outils, suivi des incidents, audits...) Identifier les risques et définir la politique de sécurité de l'information (audits, plan de prévention, plan de continuité d'activité, charte sécurité, choix technologiques...) Définir le plan de traitement des risques et les mesures de sécurité associées Assurer le respect des droits sur la protection des données personnelles Communiquer et former le personnel pour sensibiliser l'ensemble de l'entreprise aux questions de sécurité de l'information
Activités complémentaires	Assurer une veille technologique et réglementaire, benchmarker les bonnes pratiques
Secteur professionnel	Toutes les entreprises où les systèmes d'information sont utilisés.
Activités et tâches professionnelles	Protéger les données et la fiabilité du système informatique d'une entreprise, telle est la mission qui incombe à l'expert en sécurité informatique. Pour cela, l'expert en sécurité informatique est amené à

réaliser un diagnostic du système d'information d'une entreprise dans le but de déceler les éventuels points faibles; apporter différentes solutions de protection pour sécuriser les informations et les données d'une entreprise; mettre en place les différents processus de sécurité; garantir la pérennité des systèmes de sécurité; actualiser les systèmes de sécurité en fonction des nouvelles menaces et des dernières technologies.

Activités 1 Administrer les accès au réseau et aux données

Tâches

Analyser:

- Le fonctionnement de l'ensemble de l'entreprise
- Les besoins d'accès aux informations et au réseau de chaque service

Qualifier la typologie des contributeurs en fonction des accès autorisés:

- Contribution
- Validation
- Administration

Activités 2 Contrer les intrusions et les virus

Tâches

Éviter les piratages, vols, destruction de données:

- Achat de pare-feu, d'antivirus
- Mise en place de tunnels sécurisés
- Utilisation de la cryptographie

S'assurer de l'emploi des logiciels de protection par les salariés:

- Indicateurs de suivi ·
- Mécanismes d'alerte ·
- Analyse des logs

Mener des audits: ·

- Recensement des points faibles ·
- Rédaction des rapports ·
- Mise à jour des systèmes de protection ·
- Évolution de la structure du réseau

Activités 3 Mettre en place les processus de sécurité

Tâches

Assurer: ·

- Efficacité des sauvegardes ·
- Bon niveau de sécurité des serveurs ·
- Revue et validation des architectures en lien avec les services techniques

Créer des alertes: ·

- Notification de mise à jour ·
- Programmation d'échéance

Mettre en place les processus adaptés: ·

- Sauvegarde des données sur plusieurs serveurs ·
- Externalisation des données

Lutter contre: ·

- La sortie d'information de l'entreprise ·
- Les importations de données potentiellement dangereuses

Activités 4 Assurer la continuité de l'activité

	<p><i>Tâches</i></p> <p>Définir avec les différents services le plan de reprise d'activité en cas de:</p> <ul style="list-style-type: none"> • Sinistre (incendie, inondation) · • Mouvement social (grèves des transports, occupation des locaux) · • Acte malveillant (sabotage, terrorisme) <p>Assurer la continuité de l'activité d'un point de vue technique: ·</p> <ul style="list-style-type: none"> • Back up des serveurs · • Accès aux logiciels clés pour l'activité · • Locaux adaptés <p>Assurer la continuité de l'activité d'un point de vue humain: ·</p> <ul style="list-style-type: none"> • Recenser les métiers et les postes clés · • Mettre en place des back up · • Informer les personnes <p>Activités 5 Sensibiliser les utilisateurs aux risques</p> <p>Activités 6 Effectuer une veille technologique</p> <p><i>Tâches</i></p> <p>Identifier les évolutions nécessaires des réseaux et des systèmes de sécurité:</p> <ul style="list-style-type: none"> • Adaptations et ajustements • Modifications • Sécurité • Fonctionnalités et services <p>Anticiper les risques:</p> <ul style="list-style-type: none"> • Adaptation et formation • Renouvellement <p>«Benchmark» les réseaux:</p> <ul style="list-style-type: none"> • Bonnes pratiques • Références
<p>Compétences génériques</p>	<p>Exécution responsable des tâches professionnelles, dans des conditions restreintes et avec une assistance qualifiée</p> <p>CT1. Appliquer les principes, les normes et les valeurs de l'éthique professionnelle</p> <p>Se familiariser avec les rôles et les tâches spécifiques au travail d'équipe et la répartition des tâches pour les niveaux subordonnés</p> <p>CT2. Identifier, décrire et animer les activités organisées en équipe avec le développement des capacités de communication et de collaboration, ainsi qu'assumer les différents rôles (exécution et leadership)</p> <p>Sensibilisation au besoin de formation continue l'utilisation efficace des ressources et des techniques d'apprentissage pour le développement personnel et professionnel</p> <p>CT3. Démontrer l'esprit d'initiative et d'action pour mettre à jour votre propre culture professionnelle, économique et organisationnelle</p> <p><i>Savoir être</i></p> <p>Sens de la communication vis-à-vis de différents publics:</p>

	<ul style="list-style-type: none"> • Diplomatie • Adaptabilité • Souplesse • Force de persuasion • Curiosité d'esprit • Vif intérêt pour les nouvelles technologies et leurs enjeux <p>Sens pédagogique :</p> <ul style="list-style-type: none"> • Goût pour l'échange • Aptitude à la communication vis à vis des utilisateurs variés • Capacité de vulgarisation des enjeux et des risques <p>Gestion du stress:</p> <ul style="list-style-type: none"> • Excellente gestion des situations d'urgence • Hiérarchisation pertinente des priorités <p>Intégrité prouvée:</p> <ul style="list-style-type: none"> • «Hacker éthique» (il cherche et repère les failles du système pour mieux les contrer); • Respect de la confidentialité • Rigueur <p>Sens de l'engagement :</p> <ul style="list-style-type: none"> • Implication et motivation • Goût pour le travail en équipe • Charisme et entraînement • Force de proposition
<p>Compétences spécifiques (professionnelle)</p>	<p>C1. Les fondements scientifiques et techniques de la SI</p> <p>C1.1 Identifier et définir les concepts, théories et méthodes de soutien aux sciences fondamentales et appliquées pour l'ingénierie de la sécurité de l'information</p> <p>C1.2 Expliquer les solutions d'ingénierie en utilisant les techniques, concepts et principes des sciences exactes et appliquées</p> <p>C1.3 Résoudre des problèmes dans les activités humaines en appliquant notamment des techniques et des méthodes de protection</p> <p>C1.4 Choisir les critères et les méthodes pour analyser les avantages et les inconvénients des méthodes et procédures appliquées pour résoudre les problèmes de sécurité</p> <p>C1.5 Modélisation de problèmes typiques en sciences appliquées à l'aide d'un instrument mathématique</p> <p>C2 Les aspects organisationnels et informationnels de la SI:</p> <p>C2.1 Identifier et définir les concepts, théories et méthodes utilisés pour effectuer des analyses axées sur la protection des personnes et des informations sur les systèmes opérant au niveau des organisations. C2.2 Expliquer les concepts, théories et méthodes utilisés dans l'analyse des systèmes fonctionnant au niveau organisations</p> <p>C2.3 Application de concepts, de théories et de méthodes de base pour la préparation des informations nécessaires au développement de systèmes de sécurité opérant au niveau des organisations</p> <p>C2.4 Choisir les critères et les méthodes d'évaluation de la qualité, des performances et des limites des systèmes de sécurité en fonction des</p>

besoins de l'organisation, y compris ceux requis pour définir un système de gestion de la qualité et de la sécurité

C2.5 Élaboration d'un projet (spécification du système) dans les conditions d'un système de gestion de la qualité et de la sécurité.

C3 Les mesures de sécurité et de contrôle

C3.1 Identifier et définir les concepts, procédures et méthodes de sécurité de l'information utilisée pour effectuer les mesures de contrôle découlant des besoins de l'activité humaine

C3.2 Expliquer les bonnes technologies pour mettre en œuvre les systèmes de sécurité requis dans les activités des organisations

C3.3 Utilisation des technologies modernes dans la définition de solutions de sécurité

C3.4 Utilisation de critères et de méthodes basés sur la technologie pour évaluer la conformité aux normes d'interopérabilité

C3.5 Développement de mesures de contrôle et de sécurité utilisant des technologies modernes pour la transmission, le stockage et le traitement des données en fonction des besoins d'une organisation

C4 Les méthodes et technologies pour développer des solutions de sécurité

C4.1 Identification et définition de concepts et de méthodes axés sur le développement, la mise en œuvre et l'utilisation de solutions de sécurité

C4.2 Explication des concepts et méthodes utilisés pour élaborer, mettre en œuvre et utiliser des mesures de contrôle et de sécurité

C4.3 Application des langages de programmation, environnements de modélisation et de développement, méthodologies de création de systèmes de sécurité

C4.4 Utilisation de critères et de méthodes pour évaluer le processus de développement de systèmes de sécurité en termes de qualité et de performance
C4.5 Développement et implémentation de logiciels de sécurité pour des problèmes concrets dans divers domaines de l'activité humaine

C5 L'architecture de sécurité et l'infrastructure

C5.1 Identification et définition du matériel architectural, des logiciels et des composants de communication, ainsi que de ceux qui sont nécessaires pour décrire une infrastructure de protection

C5.2 Expliquer l'interaction et le fonctionnement des composants architecturaux et de sécurité

C5.3 Application de méthodes de base pour spécifier des solutions architecturales et d'infrastructure pour des problèmes de sécurité typiques

C5.4 Utilisation de critères et de méthodes pour évaluer les caractéristiques fonctionnelles et non fonctionnelles des composants du système de sécurité

C5.5 Mise en place d'une solution architecturale et d'infrastructure basée sur les contraintes imposées par les projets de sécurité

Savoir faire

Pratique et expérience rédactionnelle:

	<ul style="list-style-type: none"> • Actualités/brèves • Articles de fond • Dossiers <p>Maîtrise expérimentée «terrain» de l'outil informatique:</p> <ul style="list-style-type: none"> • Architecture des systèmes et réseaux • Procédures d'exploitation et des standards d'échange des données employées • Procédures de Sécurité Informatique • Systèmes d'exploitation (Solaris, Linux) et des langages de programmation associés <p>Maîtriser les outils bureautiques:</p> <ul style="list-style-type: none"> • Traitement de texte, tableur, outil de présentation <p>Utilisation de logiciels spécifiques:</p> <ul style="list-style-type: none"> • Outils de chiffrement de disques durs ou de serveurs • Pare feu (Firewalls) • Outils d'identification
<p>Compétences transverses</p>	<p>"Leadership" et esprit d'entreprise. Promouvoir sa vision auprès des décideurs internes et externes, et encourager la prise d'initiative de ses équipes.</p> <p>Adaptabilité et Flexibilité. Évaluer l'impact des changements et proposer les réponses ou les solutions adéquates.</p> <p>Analyse et Synthèse. Identifier les informations / sources nécessaires à la réalisation des activités de l'entreprise et conduire une analyse critique. Présenter l'essentiel sur un sujet donné dans une logique de préconisation.</p> <p>Communication orale et écrite. Communiquer de façon habile et fine dans des situations complexes (message sensible, public difficile, situation imprévue...).</p> <p>Conviction et Influence. Identifier et décrypter les positions des différents interlocuteurs stratégiques internes et externes, repérer et toucher les bons relais d'influence auprès des personnes à convaincre.</p> <p>Créativité, sens de l'innovation. Concevoir et mettre en œuvre des solutions nouvelles et efficaces.</p> <p>Gestion de Projet. Diriger un projet majeur ou coordonner plusieurs projets opérationnels simultanément.</p> <p>Gestion de la performance. Mettre en place de nouveaux indicateurs pertinents en fonction des objectifs. Partager et promouvoir les meilleures pratiques en interne comme en externe.</p> <p>Orientation client. Être force de proposition par rapport au besoin exprimé tout en mobilisant les parties prenantes nécessaires (internes – externes).</p> <p>Rigueur et Organisation. Hiérarchiser et établir des priorités d'actions selon les enjeux des activités.</p> <p>Sens Relationnel. Adapter son comportement et son attitude en fonction de l'interlocuteur pour maximiser la qualité des échanges.</p> <p>Travail et animation d'équipe. Accompagner un ou deux collaborateurs sur une activité opérationnelle ou un projet de l'entreprise.</p>
<p>Connaissances</p>	<p><i>Savoirs</i></p>

<p>nécessaires</p>	<p>Connaissance de:</p> <ul style="list-style-type: none"> • L'entreprise • Ses services/produits • Sa structure • Son organisation • Son environnement juridique <p>Vision globale et complète des systèmes d'information</p> <ul style="list-style-type: none"> • De l'entreprise • Des organisations similaires <p>Connaissance technique approfondie des:</p> <ul style="list-style-type: none"> • Concepts et techniques d'architecture des systèmes et réseaux • Procédures d'exploitation et des standards d'échange des données employées • Procédures de Sécurité Informatique • Systèmes d'exploitation et langages de programmation associés • Bases de données
<p>Compétences cœur de métier</p>	<p>Gouvernance SI</p> <ul style="list-style-type: none"> • Définir le modèle d'évaluation et d'évolution des processus <p>Architecture fonctionnelle SI</p> <ul style="list-style-type: none"> • Concevoir des cartographies fonctionnelles et applicatives <p>Architecture technique SI</p> <ul style="list-style-type: none"> • Analyser les acteurs et outils (matériel ou logiciel) du marché • Évaluer les solutions au regard du besoin • Conduire des audits de performance technique SI <p>Supervision et administration d'un Système d'Information</p> <ul style="list-style-type: none"> • Superviser des infrastructures informatiques et le patrimoine applicatif <p>Assistance à Maîtrise d'Ouvrage en cadrage projet</p> <ul style="list-style-type: none"> • Analyser les propositions techniques et fournir une aide au choix <p>Gestion des risques</p> <ul style="list-style-type: none"> • Cartographier les risques techniques et fonctionnels et estimer leur criticité • Piloter les risques projets (qualitatifs, budgétaires, contractuels et de planning) • Identifier les risques légaux (propriété intellectuelle, pénal...) pour l'entreprise et mettre en place les solutions juridiques de prévention • Réaliser une analyse de risques et d'impacts de mise en production • Réaliser une analyse de risque en utilisant des normes et des méthodes standard (méthode AMDEC, MARION, MEHARI, EBIOS, ISO 27005...) • Assurer le niveau de couverture des risques d'une entreprise, d'un projet... (assurances, plans d'actions...) • Déployer une démarche sûreté de fonctionnement • Gérer une crise <p>Gestion des contrôles, tests et diagnostics</p> <ul style="list-style-type: none"> • Analyser et comprendre l'origine d'un dysfonctionnement, incident ou accident (spécifications physiques du produit, processus...) <p>Gestion d'entreprise</p> <ul style="list-style-type: none"> • Arbitrer entre plusieurs orientations stratégiques, tactiques ou opérationnelles <p>Résolution de problèmes complexes</p>

	<ul style="list-style-type: none"> • Analyser une situation problématique dans un environnement complexe • Élaborer et déployer une méthodologie de résolution • Élaborer des préconisations, proposer des solutions et scénarii d'amélioration <p>Formation et transmission de connaissances</p> <ul style="list-style-type: none"> • Synthétiser une méthodologie ou des connaissances à capitaliser et transmettre <p>Gestion réglementaire et contractuelle</p> <ul style="list-style-type: none"> • Connaître les réglementations en vigueur dans sa spécialité ou son secteur <p>Veille, analyse et gestion documentaire</p> <ul style="list-style-type: none"> • Réaliser une veille technologique sur son domaine d'activité • Analyser des documents techniques <p>Anglais</p> <ul style="list-style-type: none"> • Converser en anglais en contexte professionnel • Utiliser un vocabulaire technique en anglais • Comprendre de la documentation technique en anglais • Écrire en anglais les livrables, notes, e-mails... nécessaires à la réalisation des activités
Conditions d'accès	Licencié en Informatique ou Ingénieur Licenciât avec une spécialisation en Sécurité Informatique.

Annexe 4 : L'accord de collaboration avec ICS Endava S.R.L.

ACORD DE COOPERARE

Mun. Chişinău

Septembrie 2016

Prezentul Acord este încheiat între:

1. **ICS ENDAVA” S.R.L.**, reprezentată prin Vasile Nedelciuc, având funcția de Director, cu sediul în Chişinău, Moldova, Str. Sfatul Tarii, nr. 15, posesoarea certificatului de înregistrare nr. IDNO 1002600023471, codul fiscal nr. 7800076, având contul nr. MFO RNCBMD2X504, denumita în continuare **Partener**

și

2. **Universitatea Tehnică a Moldovei**, reprezentată de domnul Ion Balmuş conf. univ., dr., decan al facultății Calculatoare, Informatică și Microelectronică, cu sediul bd.Stefan cel Mare,168, MD-2004, Moldova, Chisinau, codul fiscal nr.1007600001506, codul bancar AGRNMD2X723, Banca beneficiara BC Moldova-Agroindbank SA, fil.Chisinau-Centru cu sediul bd.Stefan cel Mare,168, MD-2004,Moldova,Chisinau denumită în continuare **Universitate**

denumite în continuare Părți, care au convenit să semneze prezentul acord cu intenția realizării următoarelor obiective:

- să colaboreze în vederea ridicării nivelului de pregătire al specialiștilor în domeniul tehnologiilor informaționale;
- să avizeze și să propună îmbunătățiri ale programelor de studii în conformitate cu cerințele pieței IT;
- să ofere posibilitatea desfășurării unor stagii de practică (internship) în cadrul ÎCS Endava SRL pentru studenți și colaboratori ai Universității Tehnice din Moldova, selectați de ÎCS Endava SRL în conformitate cu cerințele și posibilităților acesteia.

Articolul 1. Obiectul Acordului de colaborare îl reprezintă stabilirea unui parteneriat reciproc avantajos între Părți în scopul ajustării procesului de formare profesională a studenților Universității la necesitățile pieței muncii, prin corelarea asistenței științifico-consultative cu cea practică.

Articolul 2. Drepturile și angajamentele Universității:

- punerea la dispoziție a programelor de studii la disciplinele de specialitate și revizuirea acestora, după necesitate, conform recomandărilor propuse de către Partener;
- crearea condițiilor privind implicarea specialiștilor Partenerului la predarea unor lecții privind ultimele evoluții în domeniile legate de dezvoltarea de software și cerințele de bază pentru angajare la companiile din domeniul TIC;
- înaintarea propunerilor privind efectuarea de către studenți a stagiilor de practică și supravegherea sistematică a procesului de stagiere a studenților;
- recomandarea, la solicitarea Partenerului, a celor mai performanți absolvenți sau viitorilor absolvenți ai Universității în vederea includerii acestora în procesul de selectare pentru angajare în câmpul muncii, inclusiv prin participarea Partenerului la Târgurile locurilor de muncă vacante, organizate regulat de către Universitate;

- organizarea, cu participarea specialiștilor Partenerului, a meselor rotunde pentru familiarizarea studenților și cadrelor didactice cu activitatea acestora, cu posibilități de stagiere a studenților și de angajare la lucru după absolvire.

Articolul 3. Drepturile și angajamentele Partenerului:

- furnizarea materialelor publicitare proprii în scopul familiarizării corpului profesoral și a studenților cu privire la activitatea Partenerului, inclusiv prin plasarea informației pe portalul web al Universității și pe panourile informaționale plasate la facultate sau la catedrele de profil;
- suportarea, după caz, a cheltuielilor legate de organizarea unor cursuri de instruire speciale cu studenții selectați de către Partener pentru angajarea ulterioară a acestora la lucru;
- înaintarea, după caz, a propunerilor privind perfecționarea programelor de studii la specialitățile IT;
- oferirea posibilității de efectuări de către studenții selectați de către Partener a stagiilor de practică, supraveghind și validând activitatea acestora;
- selectarea din rândul studenților de la specialitățile IT a celor mai performanți pentru eventuala lor angajare, inclusiv prin participarea la Târgurile locurilor de muncă organizate de către Universitate;
- acceptarea stagerii unor cadre didactice ale Universității, care corespund cerințelor Partenerului, în cadrul ÎCS Endava SRL.

Articolul 4. Cesiunea Acordului

Una dintre părțile prezentului Acord poate transmite unei terțe persoane, total sau parțial, drepturile și obligațiile ce i se cuvin prin acest Acord, numai dacă a obținut acordul scris prealabil al celeilalte părți.

Articolul 5. Forța majoră

Forța majora exonerează de răspundere partea care o invocă, cu condiția ca aceasta să notifice cealaltă parte în termen de cel mult 5 zile de la data la care a intervenit cauza de forță majoră, termen care se decalează corespunzător în cazul în care, prin natura ei, situația de forță majoră împiedică inclusiv comunicarea. Efectul este suspendarea obligației părții în cauză de îndeplinire a prestațiilor asumate în prezentul Acord a căror executare este împiedicată, sub condiția dovedirii situației de forță majora în condițiile legii. În înțelesul prezentului Acord “forța majoră” înseamnă orice eveniment imprevizibil și insurmonabil (în afara puterii de control a părților), care se petrece în perioada de derulare a Acordului și care împiedică pe una din părți, în mod obiectiv, să își îndeplinească obligațiile din Acord, cum ar fi, de exemplu, conflicte armate, actele de terorism, dezastrele naturale și alte asemenea, fără a include însă grevele, modificarea cursurilor de schimb, creșterea fiscalității sau înrăutățirea situației socio-economice. În caz de forță majoră, întregul Acord încetează sau negociază după cum vor stabili părțile pe cale amiabilă.

Articolul 6. Încetarea Acordului

Prezentul Acord încetează în conformitate cu art. 4 din prezentul contract sau în baza acordului părților și în celelalte cazuri prevăzute de lege și de prezentul contract.

În cazul în care oricare dintre părți nu-și îndeplinește sau își îndeplinește necorespunzător obligațiile asumate prin prezentul Acord, partea care se considera prejudiciată va transmite celeilalte părți o

notificare, ce constituie și punerea în întârziere, semnalând încălcarea constatată și termenul de remediere, neremedierea sau remedierea neadecvată în acel termen sau dreptul părții care a făcut notificarea să declare, printr-o nouă notificare, încetarea Acordului prin rezoluțiune unilaterală.

Articolul 7. Dispoziții finale

- Relațiile dintre Părți vor fi guvernate de principiul echității, bunei voințe și dezvoltării relațiilor de colaborare durabilă.
- Prezentul Acord de colaborare se întocmește pe un termen de 1 an, prelungirea lui realizându-se prin consensul Părților.
- Modificările și completările în prezentul Acord de colaborare se vor efectua prin consensul Părților.
- Eventualele litigii între Părți vor fi soluționate pe cale amiabilă.
- În cazul reorganizării, schimbării locului de reședință, a numerelor de telefon, fax sau a altor date prezentate în Acordul de colaborare, Părțile vor informa despre aceasta cealaltă parte în termeni utili.

Articolul 8. Acordul de colaborare este redactat în două exemplare originale, câte unul pentru fiecare Parte și intră în vigoare din momentul semnării ei de către Părți.

ÎCS ENDAVA SRL
Director, Vasile Nedelciuc

Universitatea Tehnică a Moldovei
Decan FCIM conf. univ., dr. Ion Balmuș



Annexe 5 : L'accord de collaboration avec l'Université Alexandru Ioan Cuza de Iasi, Romania



ACORD DE COLABORARE
pentru desfășurarea de activități de cercetare comune
în domeniile: CHIMIE, ȘTIINȚELE VIETII ȘI ALE PĂMÂNTULUI ȘI
INFORMATICA

între

UNIVERSITATEA "Alexandru Ioan CUZA" IAȘI-ROMÂNIA
Biroul pentru Studii Doctorale Universitare
și
UNIVERSITATEA TEHNICĂ A MOLDOVEI
Departamentul "Școli Doctorale"

CAP. I. PARTILE

CSUD al Universității "Alexandru Ioan CUZA", cu sediul în Iași, Blvd. Carol I nr. 22, Iași, reprezentat prin Directorul Consiliului pentru Studiile Universitare de Doctorat, prof.univ.dr. Ovidiu CĂRJĂ, având ca domeniu principal de activitate coordonarea studiilor doctorale,

și

Departamentul "Școli Doctorale" al Universității Tehnice a Moldovei, cu sediul în Chișinău, bl Ștefan cel Mare, 168, biroul 303, reprezentat prin doamna Galina Marusic, conf. univ. dr., șef departament, având ca domeniu principal de activitate organizarea și desfășurarea studiilor superioare de doctorat,

convin prin prezentul protocol să colaboreze pe baza de parteneriat activ pentru organizarea mobilităților doctoranzilor din cadrul UTM în scopul realizării cercetărilor științifice prin utilizarea laboratoarelor de cercetare științifică din cadrul *Universității "Alexandru Ioan CUZA".*

CAP. II. PRINCIPII DE COLABORARE

- transparența și profesionalism în valorificarea cunoștințelor și a experienței în domeniul fiecăruia de activitate;
- confidențialitate, în schimbul de informații și păstrarea secretului profesional.

CAP. III. PARTEA FINANCIARĂ

Pe durata derulării activităților la Universitatea "Alexandru Ioan CUZA" din Iași, România, doctorandul va putea beneficia de:

- acoperirea cheltuielilor de tur-retur din partea UTM;
- acoperirea cheltuielilor privind cazarea din partea Universității "Alexandru Ioan CUZA" din Iași.

Pe durata derulării activităților la UTM, Republica Moldova, doctorandul va putea beneficia de:

- acoperirea cheltuielilor de tur-retur din partea UAIC Iași;
- acoperirea cheltuielilor privind cazarea din partea UTM Republica Moldova.

CAP. IV. DURATA MOBILITĂȚII

Mobilitatea doctoranzilor poate fi desfășurată cu o durată maximă de 10 zile calendaristice pe un an de studii.

CAP. V. DISPOZIȚII FINALE

Prezentul ACORD de colaborare are caracterul unui document cadru și acoperă întreaga activitate de realizare a obiectivelor comune convenite.

Prezentul ACORD poate fi modificat sau completat cu acordul scris al părților semnatare ori de câte ori acestea convin asupra amendamentelor propuse.

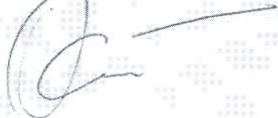
Acordul are valabilitate de un an, cu prelungire automată pentru noi perioade de câte un an, dacă nici una din părți nu notifică celeilalte părți cererea de încetare a valabilității sale.

Încheiat în doua exemplare, ambele cu valoare de original, câte un exemplar pentru fiecare parte.

Universitatea "Alexandru Ioan CUZA" din Iași,
Iași, România

RECTOR,
prof. univ. dr. Vasile ISAN

Director CSUD,
Prof. univ. dr. Ovidiu CĂRJĂ



Universitatea Tehnică a Moldovei

RECTOR,
prof. univ. dr. hab. Viorel BOSTAN

Șef departament "Școli Doctorale",
conf. univ. dr. Galina MARUSIC

