Université de Bretagne-Sud

N° ……..

DIPLÔME D'UNIVERSITÉ
DU ☒ DIU ❑

Création
Modification ✠
Renouvellement
Suppression

Intitulé:
Diplôme d'Université:
"Organiser la cyberdéfense des TPE/PME, organismes publics & privés"

- **Composante responsable de la formation : ENSIBS**

- **Lieux de la formation** :
Campus de Tohannic et Groupement Départemental de la gendarmerie du Morbihan (Place de la Libération à Vannes)

- **Composante(s) associée(s) :**
à court / moyen terme l'IUT de Vannes

- **Autre(s) établissement(s) concerné(s) :**
  - Sans objet

- **Enseignants responsables :**
  - Julien Breyault
  - Julien Nachouki

Avis du Conseil de composante		En date du
Avis du CFVU		En date du

Avis du CA		En date du

Enseignant(s) responsable(s) *(maximum deux)* Responsable de la FC cyber	**Nom : Julien Breyault** **Composante de rattachement : ENSIBS**	**Statut : Enseignant titulaire** **Téléphone : 02 97 48 50 56** **E-mail : julien.breyault@univ-ubs.fr**
Responsable opérationnel de la formation	**Nom : Julien Nachouki** **Composante de rattachement : ENSIBS (pour la formation)**	**Statut : BIATSS** **Téléphone : 06.66.94.56.82** **E-mail : julien.nachouki@univ-ubs.fr**
Type de formation et de diplôme	Acquisition de nouvelles compétences ☒ Réorientation ☒ DU X	
Code NAF	6202	
Niveau de sortie	**Cycle universitaire** 1er cycle **Niveau selon la nomenclature du Ministère du travail** 5 (ancien niveau III)	
Objectif(s)	L'objectif de la formation est de faire du participant un référent cyberdéfense interne sur l'organisation de la Cyberdéfense au sein de l'entité et/ou des métiers. **Cibles :** **Dirigeants, Responsables des Systèmes d'Information (RSI/DSI), Responsables de la Sécurité des Systèmes d'Information (RSSI), voire responsables métiers avec forte dépendance cyber** **Compétences :** • Analyser les risques cyber • Mettre en place une politique de sécurité des systèmes d'information, • Mettre en place des plans de continuité et de reprise d'activité associés, • Comprendre les enjeux économiques, juridiques et organisationnels liés aux types d'informations traitées • Comprendre les menaces • Interagir avec les structures de sécurité étatiques (ANSSI, gendarmerie, cybermalveillance,…)	
	Précisez comment se situe la formation par rapport à l'offre de la composante, de l'université et extérieure à l'université.	

<table>
<tr><td>Opportunités et originalités</td><td colspan="3">Précisez les besoins des milieux professionnels.
L’ANSSI a défini comme prioritaire le besoin de former la cible et de labelliser les formations en définissant un cahier des charges et en donnant une labellisation (en cours)
En effet, les organisations les plus sensibles aux cyber-menaces sont les PME, les TPE et les collectivités territoriales. Que cela soit par manque de compétences, de moyens humains, financiers ou encore de temps, ces organismes ne disposent pas des solutions organisationnelles et techniques cyber nécessaires pour assurer la pérennité de leurs activités. La Gendarmerie nationale, qui constitue des cellules cyber afin de les conseiller, a été le premier groupe formé en 2021-2021
La formation est proposée à partir de 2021 plus largement aux interlocuteurs des gendarmes que sont les responsables informatiques des PME/TPE, administrations et collectivités sur la partie organisationnelle uniquement.
On pourrait proposer une “seconde étape” en validant les blocs de compétences en commun avec la LP Cyber de Vannes pour ceux qui recherchent un diplôme de niveau 6</td></tr>
<tr><td>Capacité d’accueil</td><td>12</td><td>Seuil d’ouverture</td><td>8</td></tr>
<tr><td>Conditions d’inscription</td><td colspan="3">Précisez les pré-requis, les conditions d’admission (diplôme, financement, entreprise pour un stage ou sujet de mémoire de recherche par exemple) ainsi que, le cas échéant, les modalités (dossier, entretien, test…)
Le stagiaire doit avoir suivi le MOOC ANSSI : « SecNum académie »</td></tr>
<tr><td>Durée totale de la formation</td><td colspan="3">87,5 heures, soit 12,5 jours</td></tr>
<tr><td>Modalités de formation</td><td colspan="3">Formation continue</td></tr>
<tr><td>Frais de formation (hors apprentissage)</td><td colspan="3">Formation continue avec financement : 2000 euros par stagiaire pour les individuels (et tarif négocié autour de 1600€ avec Gendarmerie pour leur prochain groupe)</td></tr>
<tr><td colspan="4">Organisation détaillée des enseignements : voir annexe 1
Indiquez en annexe l’équipe pédagogique pressentie, programme, volume horaire, stages)</td></tr>
<tr><td>Moyens</td><td colspan="3">Précisez les moyens disponibles, les équipements le cas échéant.
Salle de TD (C4 PRO ENSIBS)
Plate-forme de simulation Cyber Range (Cyber Security Center, ENSIBS)
Application e-portfolio pilote cyberdéfense</td></tr>
<tr><td colspan="4">Modalités de contrôle des connaissances : voir annexe 2
Matières, nature et durée de l’épreuve, coefficients
Le contrôle continu sera privilégié – voir annexe 2 pour les détails</td></tr>
<tr><td>Évaluation financière</td><td colspan="3">Voir fichier budgétaire</td></tr>
<tr><td>Procédure</td><td colspan="3">Précisez les différentes formes d’évaluation (par exemple : indicateurs, évaluation par les étudiants, par les enseignants, par les professionnels…) ainsi que leur périodicité. Il est possible de renvoyer à une annexe.</td></tr>
</table>

d'évaluation de la formation	• Fiche d'évaluation standardisée à l'issue de chaque cours • Conseil de perfectionnement avec les différents intervenants et organisations impliqués à l'issue des soutenances du portfolio
Partenariats	Précisez les partenaires et leurs rôles respectifs • Gendarmerie Nationale (sont à l'origine du besoin) • CPME, MEDEF du Morbihan • Mairie de Saint Avé • Agence Nationale de la Sécurité des Systèmes d'Information (labellisation SecNum-FC en cours et par le biais du cours EBIOS-RM en cours de labellisation SecNum-FC également) • Cybermalveillance.gouv.fr via son intervention
Observations particulières	Groupe mixte gendarmes / TPE / PME / administrations / collectivités prévu
Date d'ouverture *(ou de modification)*	Modification à partir de septembre 2021
Ouverture demandée pour	1 an renouvelable

Le 17/5/2021,

Bloc	Modules (heures)	coef	Mode éval
Gouvernance et conformité (34h)	• Mettre en place une démarche de sécurité (4h) • Mettre en place une PSSI (Politique de Sécurité des Systèmes d'Information) (12h) • Mettre en place un PCA (Plan de Continuité d'Activité) (5h) • Mettre en place un PRA (Plan de Reprise d'Activité) (5h) • Organiser la gestion de crise (4h) • Viser la certification ISO27001 (4h)	6	**Contrôle continu** Travail rendu et/ou QCM
Analyser les risques cyber (17,5h)	Mise en œuvre (17,5h)	3	
Protéger les SI (20h)	• Comprendre les enjeux économiques et organisationnels d'une entreprise liés à leurs informations classifiées (2h) • Comprendre la typologie et motivations des acteurs de l'insécurité et de la sécurité économique (3h) • Utiliser les renseignements de sources opérationnelles, techniques, humaines :méthodologies et protections (OSINT, …) (3h) • Mettre en place des moyens de protections contre les techniques de manipulation (6h) • Comprendre et interagir avec les structures de sécurité françaises (ANSSI,Gendarmerie, renseignement, …) (2h) • Exercice de synthèse (4h)	6	
Intégrer les obligations et responsabilités juridiques cyber (16h)	• Comprendre et agir dans un contexte de droit international complexe (4h) • Se mettre en conformité avec le RGPD : principes fondamentaux, cas pratiques, rédaction d'un registre de traitement de données, contrats et clauses contractuelles, … (8h) • Anticiper les conséquences juridiques d'une cyberattaque, assurance cyber(4h)	3	

Compensation entre matières et entre blocs possible