Principes de Sécurité Informatique

TEM1006-NAIN_

Domaine : **Sciences** Grade académique : **Master en architecture des systèmes informatiques - Namur**
Niveau de certification : **7** Cycle : **Deuxième cycle** Année académique : **2026-2027** (Q1)

CRÉDITS ECTS	VOLUME HORAIRE
4	**50 h**

PRÉREQUIS	CO-REQUIS
Aucun	*Aucun*

IMPLANTATION	DIRECTEUR DE DÉPARTEMENT DU DOMAINE	RESPONSABLE DE L'UE	ENSEIGNANTS INTERVENANTS
Département technique de Namur	Willem Kuypers	Emmanuel DAUVIN	Emmanuel DAUVIN Thomas REMY

PROGRAMME D'ÉTUDES

Programme	Bloc	Caractère
IE-Master en architecture des systèmes informatiques	1	Obligatoire

Partie 1 Contribution de l'UE au profil d'enseignement du programme et acquis d'apprentissage spécifiques (AAS) sanctionnés par l'évaluation

CONTEXTUALISATION

UE prérequise : aucune

Cette UE contribue à l'atteinte des acquis d'apprentissage terminaux suivants :

• Résoudre selon une approche analytique et systémique des problèmes liés à des situations nouvelles ou présentant un certain degré d'incertitude

– Identifier, traiter et synthétiser les données pertinentes

– Rechercher les ressources nécessaires

– Transposer les résultats des concepts à la problématique ou situation traitée

– Argumenter les choix proposés

• Contribuer à des travaux de recherche et de développement

– Analyser une problématique de manière critique

– Identifier et proposer des solutions innovantes et/ou améliorations

• Communiquer dans un cadre professionnel avec les collaborateurs, les clients

– Rédiger des rapports, des cahiers des charges, fiches techniques ou manuels

– S'exprimer de manière adaptée en fonction du public

– Utiliser efficacement les outils de communication adéquats

• Agir de façon réflexive et autonome, en équipe, en partenariat

– Organiser son temps, respecter les délais

– Acquérir une capacité d'autocritique

– Actualiser ses connaissances et compétences

– Collaborer activement avec d'autres

– Animer et accompagner une équipe

– Assumer les responsabilités associées aux actes posés

• Innover, concevoir ou optimiser un système

– Intégrer l'ensemble des composantes d'un système à partir des résultats d'analyse

– Concevoir des procédures et des dispositifs

– Modéliser, dimensionner et optimiser des systèmes

• Gérer les ressources techniques et financières de systèmes

– Assurer un suivi

– Evaluer les processus et les résultats

– Proposer et appliquer les actions correctives

• Utiliser des procédures et des outils

– Exploiter les outils appropriés afin de résoudre une tâche spécifique

– Effectuer des tests, des contrôles et des mesures

– Effectuer des paramétrages, des réglages

– Respecter la déontologie et les règlementations en vigueur dans la profession

ACQUIS D'APPRENTISSAGE SPÉCIFIQUES (AAS)

Théorie

À la fin de cette formation, l'étudiant sera capable, dans le cadre de la stratégie d'entreprise, de comprendre, d'expliquer et d'appliquer en justifiant :

• La gouvernance de la sécurité des systèmes d'information.

• La gestion des risques cyber.

• La conformité aux normes, standards et règlements.

Laboratoires

Au terme de l'activité, l'étudiant sera capable de :

• Comprendre les principes de base de la fonction de Hash et de son utilisation pour les mots de passe ;

• Retrouver des informations clés dans des documents ou sur une image disque à l'aide d'outils Forensics ;

• Identifier et exploiter différentes vulnérabilités sur un système.

OBJECTIFS DE DÉVELOPPEMENT DURABLE

Document annexe à la fiche UE accessible via un lien explicitant en quoi le programme d'études s'inscrit dans une politique de développement durable. Une ou plusieurs UE spécifique(s) pourraient être ciblée(s) dans cette annexe.

Partie 2 Description de l'unité d'enseignement

OBJECTIFS

À définir

CONTENU

Théorie

• Principes fondamentaux de la sécurité des systèmes d'information.

• Principes de gouvernance de la sécurité des systèmes d'information, politiques de sécurité.

• Gestion des risques cyber en entreprise.

• Normes et standards de cybersécurité, audit et conformité (p.ex. ISO27000, PCI-DSS, ..).

Laboratoires

• Framework utilisé dans la sécurité informatique

• Password cracking et fonction de hachage

• Computer Forensics

• Cyber Threat Intelligence

SOURCES ET RÉFÉRENCES

Théorie

L'accès institutionnel à la plateforme de documentation de la NBN permet d'accéder aux normes ISO.

SUPPORTS DE COURS

Activité d'apprentissage	Support
AAIN1006-A — Théorie	*À définir*
AAIN1006-B — Laboratoires	Slides, outils et ressources fournis par le professeur via Moodle

Partie 3 Méthodologie mise en œuvre et éventuel découpage de l'UE

DESCRIPTION DES ACTIVITÉS D'APPRENTISSAGE (AA) AU REGARD DE LEUR STATUT

Activité d'apprentissage	Heures	Langue d'enseignement	Langue d'évaluation
AAIN1006-A — Théorie	25 h	Français	Français
AAIN1006-B — Laboratoires	25 h	français	français

MÉTHODES D'ENSEIGNEMENT ET D'APPRENTISSAGE

Activité d'apprentissage	Méthodes d'enseignement et d'apprentissage

AAIN1006-A — Théorie	*À définir*
AAIN1006-B — Laboratoires	Exposés Travaux en autonomie

DÉTERMINATION DE LA COHÉRENCE PÉDAGOGIQUE EN CAS DE REGROUPEMENT D'AA FAISANT L'OBJET D'UNE ÉVALUATION DISTINCTE

À définir

Partie 4 Évaluation de l'unité d'enseignement

STRUCTURE DU DISPOSITIF GÉNÉRAL D'ÉVALUATION (EN LIEN AVEC LE PROGRAMME D'ÉTUDES)

Évaluation intégrée : non

UE remédiable.

Évaluation : session de janvier (Q1) et seconde session (Q3).

Note de l'UE : moyenne pondérée des notes des activités d'apprentissage :

• AAIN1006-A – Théorie : 50 %

• AAIN1006-B – Laboratoires : 50 %

MÉTHODOLOGIE DE CONSTRUCTION DE LA NOTE FINALE DE L'UE

Se référer à l'évaluation des activités d'apprentissage.

LA PONDÉRATION DE L'ÉVALUATION DE L'UE À DES FINS DE DÉLIBÉRATION LORS DU CALCUL DE LA MOYENNE

Au sein du programme d'études, lors du calcul de la moyenne, la pondération de l'évaluation de l'unité d'enseignement est effectuée sur base des crédits affectés à cette unité d'enseignement et évalués

MODALITÉS D'ÉVALUATION PAR ACTIVITÉ D'APPRENTISSAGE

Activité d'apprentissage	Modalités d'évaluation
AAIN1006-A — Théorie	*À définir*
AAIN1006-B — Laboratoires	**SEPTEMBRE - JANVIER** **TRAVAUX :** Rapport à réaliser par groupe et à remettre durant le quadrimestre - pondération : 50% **EXAMEN :** Examen oral pour valider les connaissances sur base des rapports rendus - pondération : 50% **SEPTEMBRE - JANVIER** **TRAVAUX :** / **EXAMEN :** Correction des rapports et défense orale de ceux-ci de manière individuelle - pondération: 100%

MODALITÉS CONCRÈTES D'ÉVALUATION

Une mention sur la fiche informera les étudiants du fait que les précisions sur les épreuves seront disponibles sur Moodle au plus tard 6 semaines avant l'évaluation.