Hes·SO VALAIS WALLIS
Haute Ecole de Gestion
Hochschule für Wirtschaft

Hes·SO
Haute Ecole Spécialisée
de Suisse occidentale
Fachhochschule Westschweiz
University of Applied Sciences and Arts
Western Switzerland

Règlement d'études

Certificate of Advanced Studies HES-SO
en
Cyber Security

ARGUMENT *(Facultatif)*

Ce CAS constitue un approfondissement professionnel qui vise le développement de compétences spécifiques de tous les professionnels de l'informatique désireux de comprendre la sécurité sous l'angle des techniques et des stratégies.

HES-SO Valais-Wallis • TechnoArk 3 • 3960 Sierre
+41 58 606 90 43• www.hevs.ch

Article 1 Objet et titre

1.1 La Haute Ecole de Gestion & Tourisme de la HES-SO Valais-Wallis (ci-après HEG) organise un certificat de formation continue conformément au Règlement sur la formation continue de la HES-SO.

1.2 Le titre de ce certificat est « *Certificate of Advanced Studies HES-SO en Cyber Security*», pour les personnes ayant suivi et réussi l'entier de la formation, les 4 modules ainsi que le travail de certificat

1.3 Le/la participant-e ayant suivi une partie de la formation (un ou deux modules) reçoit une attestation de participation.

Article 2 Organisation et gestion du programme d'études

2.1 L'organisation et la gestion du programme d'études pour l'obtention du certificat sont confiées à un comité pédagogique, placé sous la responsabilité de la direction de la HEG. Un comité scientifique garantit l'adéquation de la formation aux besoins des terrains ainsi que de sa scientificité. Il se réunit au minimum une fois par année.

2.2 Le Comité pédagogique est composé de 2 membres, enseignant-e-s de la HES-SO et désigné-e-s par direction de la HEG.

2.3 Le Comité pédagogique avec le soutien du Comité scientifique assure la mise en œuvre du programme d'études ainsi que le processus d'évaluation des compétences acquises par les participant-e-s.

2.4 Les membres du Comité scientifique sont désignés par la direction de la HEG, sur proposition du comité pédagogique. La durée de leur mandat est de deux ans, renouvelable tacitement.

Article 3 Conditions et procédure d'admission

3.1 Le CAS en Cyber Security est ouvert aux titulaires d'un diplôme délivré par une haute école (titre de bachelor ou équivalent) et attestant d'une pratique professionnelle d'au moins 1 an.

3.2 Les personnes qui ne sont pas titulaires d'un diplôme de haute école peuvent être admises aux formations continues si elles démontrent leur aptitude à suivre ces dernières en suivant la procédure d'admission sur dossier décrite à l'alinéa 3.3.

3.3 Les personnes visées par une procédure d'admission sur dossier doivent attester de leur aptitude à suivre la formation choisie en fournissant au minimum un curriculum vitae, des attestations des formations suivies, des certificats de travail ainsi qu'une lettre de motivation. Le délai d'inscription est défini par le Comité pédagogique.

3.4 L'admission est décidée par la direction de la HEG sur préavis du Comité pédagogique après examen du dossier de candidature soumis en vertu de l'alinéa 3.3.

3.5 Le nombre de candidat-e-s admis-es par une procédure d'admission sur dossier ne doit pas excéder 40 % des effectifs d'une volée. Les hautes écoles fournissent annuellement un rapport au Rectorat de la HES-SO sur les procédures d'admission.

3.6 Les frais relatifs à l'admission sur dossier s'élèvent à CHF 100.–.

3.7 Les candidat-e-s ayant suivi une partie des modules qui désirent continuer la formation doivent s'inscrire aux modules manquants lors d'une prochaine session. Cette inscription doit intervenir au plus tard 2 ans après la fin du ou des premiers modules suivis.

3.7 Aucune reconnaissance d'acquis n'est prévue dans le cadre de ce CAS.

3.8 Lorsque le nombre de candidat-e-s à l'admission n'atteint pas la limite décidée par la direction du CAS, la date d'ouverture de la formation peut être reportée, voire annulée.

3.9 Le nombre de participant-e-s peut être limité par la direction du CAS, qui décide alors du nombre maximum de participants possibles. Les admissions sont attribuées en fonction du type du dossier selon les articles précédents, puis par ordre d'arrivée, les personnes ayant été refusées lors d'une session précédente étant prioritaires lors de la session suivante.

Article 4 Conditions financières

4.1 Les frais de la formation pour l'ensemble du CAS sont présentés en annexe du présent règlement.

4.2 Le paiement de l'écolage s'effectue à 30 jours dès réception de la facture.

4.3 Les annulations se font par écrit. Le timbre postal ou la date de l'e-mail font foi. Les annulations opérées par écrit jusqu'à 15 jours avant le début du cours n'engendrent aucun frais. Entre 14 jours et 6 jours avant le début du cours, la HEG exige un montant correspondant à 10% de la finance de cours. Dès 5 jours avant le début du cours, le prix total du cours est dû.

4.4 La finance de cours reste intégralement due en cas de désistement d'un participant, sauf motif grave, dûment établi. En pareil cas, la finance de cours, augmentée des frais administratifs, est calculée proportionnellement au nombre d'heures de cours effectivement données jusqu'au moment de l'annonce écrite de l'arrêt par le participant

4.5 Si le/la participant-e prolonge sa formation au-delà de la durée maximale prévue, des frais d'écolage supplémentaires seront perçus.

4.6 En cas de travail de remédiation à un module, celui-ci sera facturé CHF 300.-

4.7 En cas de travail de répétition à un module, celui-ci sera facturé CHF 600.-.

4.8 En cas de non règlement ou de règlement partiel, la HES-SO Valais se réserve le droit de refuser au participant le document de validation (attestation, certificat), et le droit de se présenter à la défense de certificat. Les étudiants se retrouvant dans cette situation auront la possibilité, après paiement, de réaliser leur défense. Dans ce cas, la HES-SO Valais facturera les frais nécessaires à la couverture de cette journée supplémentaire d'expertise.

Article 5 Forme et durée des études

5.1 La formation CAS en Cyber Security est dispensée en emploi. Elle correspond à 15 crédits ECTS et comprend 5 modules, dont le Travail de Certificat, réparti sur 12 mois. La durée maximale des études est de 24 mois.

5.2 Le module Travail de Certificat se déroule après l'obtention des 4 modules précédents.

5.3 Le/la responsable du CAS peut, sur préavis du Comité scientifique, autoriser un-e participant-e qui en fait la demande écrite à prolonger pour de justes motifs la durée de ses études

5.4 Le plan d'études fixe les enseignements dispensés dans le cadre des modules thématiques et le nombre de crédits ECTS attachés à chaque module ainsi qu'au travail de fin d'études. Il est approuvé par la direction de la HEG.

5.5 Il est possible de ne suivre qu'un ou deux modules.

Article 6 Principes d'organisation modulaire

6.1 La formation est organisée selon un système modulaire avec attribution de crédits ECTS en référence au système européen de transfert et d'accumulation

de crédits ECTS ainsi qu'à la best practice et aux recommandations de la Conférence Suisse des HES.

6.2 Les modalités d'attribution des crédits ECTS sont organisées selon le guide « de l'utilisateur de l'ECTS » de la Commission Européenne en vigueur.

6.3 Un crédit ECTS correspond à un volume de travail de 25 à 30 heures de la part de l'étudiant-e. Ces heures regroupent aussi bien les cours présentiels, les travaux à distance, les travaux personnels, ainsi que de la part d'expérience professionnelle.

6.4 Chaque module fait l'objet d'un descriptif de module.

Article 7 Evaluation

7.1 Chaque module fait l'objet d'une évaluation. Les évaluations ont pour but d'apporter la preuve que les participant-e-s ont assimilé la matière dispensée dans le cadre des modules.

7.2 Les évaluations sont organisées par la direction du CAS en Cyber Security et peuvent être composées de plusieurs éléments comme un examen par écrit ou par oral, un exposé, un travail écrit ou encore une confirmation de participation active aux travaux menés durant le cours. Ces éléments sont précisés dans le descriptif de module.

7.3 Les personnes habilitées à attribuer les notes sont les personnes qui enseignent ou qui interviennent en tant qu'expert.

7.4 Le/la participant-e doit obtenir la mention "acquis" pour chaque module. L'évaluation se base sur une échelle allant de 1.0 à 6.0. Les notes égales ou supérieures à 4.0 correspondent à « acquis », les notes inférieures à 4.0 à « non acquis »

7.5 En cas d'obtention d'une note allant de 3.5 à 3.9 suite à la réalisation d'un module ou suite à la réalisation d'un travail de fin d'étude, un travail complémentaire (de remédiation) est demandé, selon des modalités fixées par le responsable de la formation. Une remédiation réussie équivaut à une note de 4.0. Une remédiation non réussie équivaut à une note de 3.0.

7.6 En cas d'obtention d'une note égale ou inférieure à 3.4 suite à la réalisation d'un module, suite à la validation d'un travail de fin d'étude, ou suite à une remédiation non réussie, un nouveau travail de validation est demandé (répétition). L'évaluation se fait sur une échelle allant de 1.0 à 6.0. Si lors de la répétition, le/la participant-e obtient une note supérieure à 4, le module est réussi. Si la note obtenue est égale ou inférieure à 3.9, il s'agit d'un échec définitif au module et à la formation.

7.7 Une remédiation et/ou une répétition sont indiquées sur le bulletin de note.

7.8 Les crédits ECTS sont attribués ou refusés en bloc pour chaque module ainsi que pour le travail de certificat.

7.9 Lorsque la personne en formation n'a pas répondu aux exigences de validation du module ou du travail de certificat selon les critères définis, elle peut bénéficier d'une seule remédiation et/ou répétition sur le même objet.

Article 8 Fréquentation

8.1 Pour obtenir le certificat ou l'attestation délivré à la fin de la formation, les étudiant-e-s doivent avoir fréquenté au moins 80% des cours dispensés.

Article 9 Présence à l'évaluation

9.1 Les examens ou autres formes d'évaluation ont un caractère obligatoire. Le/la participant-e qui ne peut pas se présenter à une étape d'évaluation pour raisons justifiées (maladie, accident, service militaire ou autres raisons majeures) doit informer la direction du CAS en Cyber Security en produisant les documents adéquats dans un délai maximum de trois jours après l'évaluation. Un rattrapage sera organisé en fonction des disponibilités.

9.2 Le/la participant-e qui, sans excuse valable, ne se présente pas à une étape d'évaluation obtient la note 1. La décision est communiquée par la direction du CAS en Cyber Security par écrit au/à la participant-e

9.3 Tout retard prévisible doit être annoncé à la direction du CAS en Cyber Security avant la date de l'étape d'évaluation, pour qu'il soit accepté ou refusé.

Article 10 Travail de fin d'études

10.1 Les études CAS se terminent par un travail de certificat. Le sujet du travail doit être validé par la direction du CAS en Cyber Security.

10.2 Le/la participant-e peut présenter le travail de fin d'études lorsque les modules précédents de la formation fréquentée sont réussis, mais au plus tard 12 mois après la fin du dernier module.

10.3 La quantité de travail à fournir pour le travail de certificat (CAS) correspond à 2 crédits ECTS, soit 50 à 60 heures de travail environ.

10.4 Les principes d'évaluation suivent les mêmes principes que ceux indiqués sous l'article 7.

Article 11 Fraudes

Toute fraude, plagiat ou tentative de fraude dans les travaux d'évaluation, les examens et l'élaboration du travail de CAS entraîne la non acquisition des crédits ECTS correspondants ainsi que l'échec définitif au module même s'il s'agit de la première tentative. Les crédits obtenus lors des modules précédents sont cependant validés, par contre le/la participant-e est exclu-e du reste de la formation. Le montant payé reste acquis à l'école.

Article 12 Conditions de réussite

La formation CAS en Cyber Security est réussie lorsque le/la participant-e a statisfait aux conditions cumulatives suivantes :

a) Avoir obtenu l'intégralité des crédits ECTS

b) Avoir suivi régulièrement les cours selon l'art.8.

c) Avoir réglé la totalité des montants dus.

Article 13 Exclusion

13.1 Sont exclu-e-s de la formation les participant-e-s qui :

a) n'ont pas obtenu les crédits nécessaires à l'obtention du titre dans la durée maximale des études prévue à l'art. 5 ;

b) n'ont pas suivi régulièrement les cours selon l'art. 8.

c) subissent un échec définitif à l'évaluation d'un module de la formation;

d) ne se sont pas acquitté-e-s de l'écolage dans le délai imparti.

13.2 Peuvent également être exclu-e-s à titre de sanction disciplinaire et selon le degré de gravité de la faute, les participant-e-s qui enfreignent les règles et usages en vigueur.

13.3 Les décisions d'exclusion sont prononcées par la direction du CAS. L'exclusion de la formation entraîne une interdiction de reprise des études dans ladite formation pendant une durée de deux ans.

Article 14 Confidentialité

Les participants qui le souhaitent peuvent signer le document « politique de confidentialité » de la HEG qui détermine les conditions de traitement des différents travaux réalisés pendant les études CAS en Cyber Security. Aucun autre document régissant la confidentialité des travaux ne sera signé.

Article 15 Voie de réclamation et de recours

En cas de litige, le règlement relatif à la procédure de réclamation et de recours de la HES-SO Valais-Wallis est applicable.

Tous les autres règlements ou directives en vigueur au sein de la HES-SO Valais/Wallis sont pleinement applicables à la formation si rien n'est prévu dans le présent règlement.

Les présentes directives entrent en vigueur le 30.10.2020 et s'appliquent à tous les participant-e-s dès leur entrée en vigueur.

Le for juridique est à Sion.

Sion, le 30.10.2020

La direction du CAS en Cyber Security