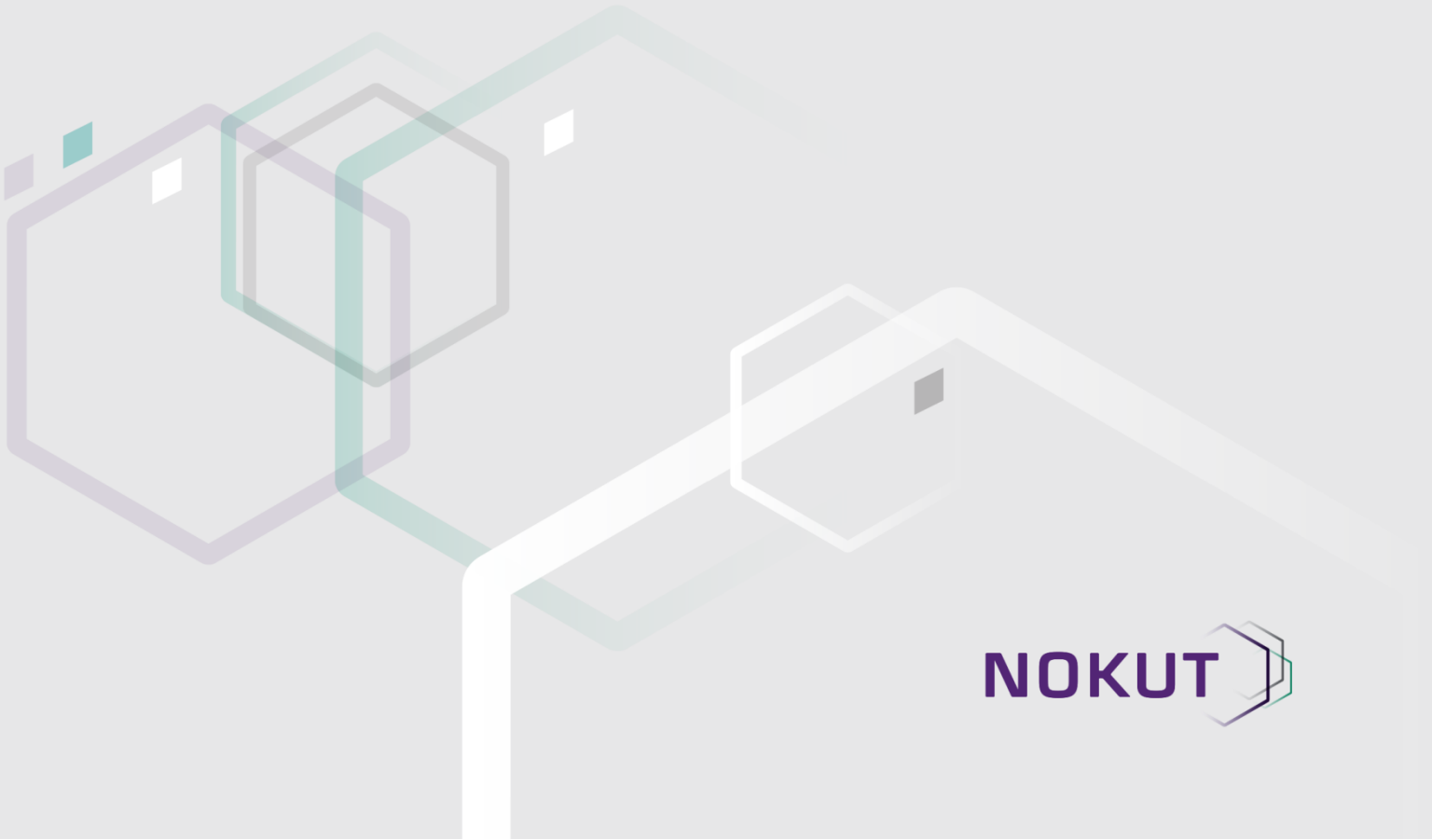
NOKUTs tilsynsrapporter

Cyber Security

Bachelorgradsstudium ved Noroff University College

Juni 2018



NOKUT kontrollerer og bidrar til kvalitetsutvikling ved lærestedene. Dette gjør vi blant annet gjennom å akkreditere nye utdanningstilbud. Institusjonene som gir høyere utdanning har ulike fullmakter til å opprette nye studier. Dersom en institusjon ønsker å opprette et utdanningstilbud utenfor fullmaktsområdet sitt, må den søke NOKUT om dette.

Institusjon:	Noroff University College
Studietilbudets navn:	Bachelorgradsstudium i Cyber Security
Grad/Studiepoeng	180 studiepoeng
Studieform	Campus/nettstudium deltid
Sakkyndige:	Førsteamanuensis Mass Soldal Lund, Forsvarets høgskole Professor Vladimir Oleschuk, Universitetet i Agder
Dato for vedtak:	26.06.2018
NOKUTs saksnummer	17/07577

Forord

NOKUTs tilsyn med norsk høyere utdanning omfatter evaluering av institusjonenes interne system for kvalitetssikring av studier, akkreditering av nye, og tilsyn med etablerte studier. Universiteter og høyskoler har ulike fullmakter til å opprette studietilbud. Dersom en institusjon ønsker å opprette et studietilbud utenfor sitt fullmaktsområde, må den søke NOKUT om dette.

Herved fremlegges rapport om akkreditering av bachelorgradsstudium i Cyber Security ved Noroff University College. Vurderingen som er nedfelt i tilsynsrapporten, er igangsatt på bakgrunn av søknad fra institusjonen. Denne rapporten viser den omfattende vurderingen som er gjort for å sikre utdanningskvaliteten i det planlagte studiet.

Bachelorgradsstudium i Cyber Security ved Noroff University College tilfredsstiller NOKUTs krav til utdanningskvalitet og er akkreditert i vedtak av 26. juni 2018.

Vedtaket er ikke tidsbegrenset

Øystein Lund
tilsynsdirektør

Alle NOKUTs vurderinger er offentlige og denne samt tilsvarende tilsynsrapporter vil være elektronisk tilgjengelige på våre nettsider www.nokut.no.

Innhold

1 Informasjon om søkerinstitusjonen 1

2 Saksgangen 1

3 Faglig vurdering 2

3.1 Oppsummering 2

3.2 Forutsetninger for akkreditering (§ 2-1 i studietilsynsforskriften) 2

3.3 Krav til studietilbudet (§ 2-2 i studietilsynsforskriften) 3

3.4 Krav til fagmiljø § 2-3 i studietilsynsforskriften 9

4 Samlet konklusjon 13

5 Institusjonens kommentar 15

6 Tilleggsvurdering 17

6.1 Vurdering av søkerinstitusjonens kommentar 17

6.2 Samlet konklusjon 19

7 Vedtak 19

8 Dokumentasjon 19

9 Presentasjon av den sakkyndige komiteen 19

1 Informasjon om søkerinstitusjonen

Noroff University College ble etablert i 1987 og tilbyr utdanning på videregående-, fagskole- og høyskolenivå. Høyskoledriften ble startet opp i 2012 og er lokalisert til Kristiansand. Styret er skolens øverste organ. Noroff tilbyr både campus- og nettbaserte studier og har fått følgende høyskolestudier akkreditert av NOKUT:

- Bachelorgradsstudium i Digital Forensics (180 studiepoeng), 2012
- Bachelorgradsstudium i Interactive Media med spesialiseringer i Animation og Games (180 studiepoeng), 2012
- Bachelorgradsstudium i Applied Data Science (180 studiepoeng), 2017.

Høyskolens interne system for kvalitetssikring av utdanningen ble godkjent av NOKUT i 2016. Noroff søkte om akkreditering av et bachelorgradsstudium i Cyber Security til søknadsfristen 15. september 2017. Søknaden har også blitt vurdert av NOKUT ved tidligere søknadsfrister under navnet Cyber Defence og fått avslag. Noroff fikk mulighet til å supplere søknaden av 15. september 2017 med oppdatert informasjon om fagmiljøet. Oppstart av saksbehandlingen ble dermed utsatt til januar 2018.

2 Saksgangen

NOKUT gjør en innledende vurdering for å avklare om grunnleggende forutsetninger for akkreditering er tilfredsstillende imøtekommet slik disse gjengis i NOKUTs studietilsynsforskrift[1]. For søknader som går videre, slik som den aktuelle søknaden denne rapporten dreier seg om, oppnevner NOKUT sakkyndige til faglig vurdering av søknaden. De må erklære seg habile og utfører oppdraget i samsvar med mandat for sakkyndig vurdering vedtatt av NOKUTs styre, og krav til utdanningskvalitet slik disse er fastsatt i studietilsynsforskriften.

I sin faglige vurdering, skal de sakkyndige konkludere med et tydelig ja eller nei på om utdanningskvaliteten samsvarer med kravene i studietilsynsforskriften. De sakkyndige blir også bedt om å gi råd om videre utvikling av studiet. Alle kriteriene må være tilfredsstillende imøtekommet for at NOKUT skal vedta akkreditering.

Dersom ett eller flere av kriteriene underkjennes av de sakkyndige, sendes den faglige vurderingen til søkerinstitusjonen som får tre uker til å kommentere denne. NOKUT avgjør deretter om institusjonens kommentarer skal sendes de sakkyndige for tilleggsvurdering. De sakkyndige får i slike tilfeller, to uker på å avgi tilleggsvurdering. NOKUTs direktør fatter deretter vedtak.

Om denne rapporten

Vi gjør oppmerksom på at NOKUTs tilsynsrapporter viser en kronologisk saksgang. Vår metode innebærer som beskrevet ovenfor en mulighet for at komiteen endrer sin konklusjon i løpet av vurderingsprosessen. Det er tilfelle i denne rapporten. Sluttkonklusjon finnes i del 7.

[1] http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20110127-0297.html

3 Faglig vurdering

Der det forekommer «vi» i dette kapitelet, er det et uttrykk for de sakkyndige. Nummereringen på hver overskrift henviser til tilsvarende bestemmelse i NOKUTs studietilsynsforskrift.

3.1 Oppsummering

Noroff University College (NUC) søker om akkreditering for Bachelorstudium i Cybersikkerhet. Studiet tilbys som et heltidsstudium for studenter ved NUCs hovedcampus i Kristiansand og satellittcampus i Oslo, og som nettstudium. Den sakkyndige komiteen anser dette for å være et studium med spesielt praktisk og operativt fokus og derfor skiller seg noe fra sammenlignbare studium i cyber- eller informasjonssikkerhet. Sakkyndig komité mener videre at fagområdets aktualitet gjør studiet slik det er beskrevet relevant både for arbeidslivet og for samfunnet generelt.

NUC har tidligere søkt om akkreditering for Bachelorstudium i Cyberforsvar (Cyber Defence). Selv om navnet er endret, er likhetene mellom søknadene så store at sakkyndig komite anser den nye søknaden for å i hovedsak være for det samme studiet. Denne uttalelsen er derfor i stor grad basert på uttalelsen gitt i forbindelse med søknad om akkreditering av Bachelorstudium i Cyberforsvar.

Sakkyndig komite anbefaler ikke akkreditering av studiet. Likevel er komiteen av den oppfatning at manglene ved søknaden i hovedsak er et spørsmål om dokumentasjon, og i mindre grad mangler ved studieplanen. Spesielt gjelder dette dokumentasjon rundt kvalifisering til masterstudier, dokumentasjon på ansettelser i fagmiljøet, samt utdanningsfaglig kompetanse og faglig ledelse.

3.2 Forutsetninger for akkreditering (§ 2-1 i studietilsynsforskriften)

3.2.1 Aktuelle krav i lov om universiteter og høyskoler

§ 2-1 (1) Aktuelle krav i lov om universiteter og høyskoler med tilhørende forskrifter skal være oppfylt.

Vurdering

Bachelor i Cybersikkerhet er en grunnutdanning og opptaket er derfor regulert av *Forskrift om opptak til høyere utdanning* (opptaksforskriften). Opptakskravene til utdanningen er generell studiekompetanse etter opptaksforskriften § 2-1 eller realkompetanse etter § 3-1. I tillegg er det krav om bestått Matematikk R1 eller Matematikk S1+S2. Studiet må etter komiteens vurdering være å regne for en informatikkutdanning og dette opptakskravet følger da etter forskriftens § 4-3.

For utenlandsstudenter er opptak etter opptaksforskriften § 2-2. Søkeren angir at studiet vil undervises på engelsk og det derfor ikke stilles spesielle krav til norskkunnskaper. Dette unntaket er det anledning til å gi etter forskriftens § 2-2 (5).

Aktuelle forskrifter er således oppfylt, og det er ingen rammeplan studiet må oppfylle.

Konklusjon

Ja, høyskolens redegjørelse er tilfredsstillende.

3.2.2 Informasjon om studietilbudet

§ 2-1 (2) Informasjon om studietilbudet skal være korrekt, vise studiets innhold, oppbygging og progresjon, samt muligheter for studentutveksling.

Vurdering

Sakkyndig komite har i vurdering av informasjon om studietilbudet vurdert *Study plan*, versjon 1.0 datert 14.09.2017, som er vedlagt søknaden. Studiets innhold og oppbygning med progresjon, læringsutbyttebeskrivelser, undervisningsmetoder og vurderingsmetoder er godt beskrevet. Alle kurs har fyldige kursbeskrivelser. Muligheter for studentutveksling er beskrevet, men lite konkrete. Studieplanen oppgir at ytterligere opplysninger om studentutveksling er å finne i NUCs LMS for opptatte studenter, men dette er ikke nyttig informasjon for potensielle studenter. Studieplanen har ingen informasjon om studiets relevans for videre studier.

Konklusjon

Ja, kravet er tilfredsstillende imøtekommet.

Høyskolen bør:

- Gi en mer detaljert beskrivelse av muligheter for studentutveksling i studieplanen
- Gi en beskrivelse av muligheter for videre studier i studieplanen.

3.3 Krav til studietilbudet (§ 2-2 i studietilsynsforskriften)

3.3.1 Læringsutbytte og studiets navn

§ 2-2 (1) Læringsutbyttet for studietilbudet skal beskrives i samsvar med Nasjonalt kvalifikasjonsrammeverk for livslang læring, og studietilbudet skal ha et dekkende navn.

Studiets læringsutbyttebeskrivelse:
Knowledge
An understanding of theories, facts, principles, procedures in the subject area of cyber security.
The candidate …
K1
Has a broad knowledge of cyber defence and attack techniques, technologies and tools in order to implement appropriate technical and non-technical solutions to prepare for, defend against and recover from cyber intrusion.
K2 Is familiar with appropriate and current procedures and standards for managing cyber risks and threats, undertaking penetration testing and ensuring network security.
K3
Has knowledge of the legal and ethical issues and responsibilities pertaining to cyber security

activities with regard to the impact of the cyber intrusion on society, industry, national infrastructure and national security.
K4 Is familiar with current and emerging research and development in the field of Cyber Security and related disciplines.
K5 Is able to update their knowledge in the area of cyber security through academic study, research and professional development.
K6 Is familiar with the current and developing state of cyber criminality and cyber warfare threats, vulnerabilities and defensive tools and techniques.
K7
Has knowledge of the history and development of cyber security, cybercrime and cyber warfare, its impact on safety and security of digital environments and infrastructures, alongside the resulting effects on society.
K8 Is familiar with various computational tools, techniques and practices that underpin secure Computing

Skills
The ability to utilise knowledge to solve problems or tasks (cognitive, practical, creative and communication skills).
The candidate …
S1
Is able to critically assess the threat level to a digital environment and select and apply appropriate computer system security and penetration tools and techniques in order to secure a computer network.
S2
Can critically select and apply a range of analytical and methodological problem solving and investigative techniques including system profiling and vulnerability analysis, based on research and to be able to interpret the solutions and present results appropriately.
S3
Is able to reflect on their own academic practice and development as a security professional, identify areas for improvement and adapt to future cyber security tools, techniques, technology and threats.
S4 Is able to find, distil and evaluate relevant academic, commercial and non-commercial information assets then apply this information in resolving digital security problems.
S5 Is able to identify stakeholders of cyber security and defence-related issues and communicate, network and collaborate with these stakeholders according to their individual requirements.
S6 Can apply mathematical and software development theories, tools and techniques to computational challenges.

General Competence
The ability to utilise knowledge and skills in an independent manner in different situations.

The candidate …
G1
Is able to identify and appropriately act on complex ethical and social issues arising within academic and professional practice as a cyber security professional, whilst being aware of the greater implications of their actions and decisions.
G2 Is able to plan, execute and manage a variety of activities and cyber security-related projects over time, alone or as part of a collaborative team to successful conclusion and in accordance with relevant legal and ethical requirements and principles.
G3
Can distil and communicate cyber security-related theories, concepts, problems and solutions, with a variety of relevant stakeholders, through the selection and application of appropriate methods of communication.
G4
Can exchange opinions, experiences and ideas with others with background and/or experience in cyber security and defence, through the selection and application of appropriate methods of communication, thereby contributing to the development of good practice within the cyber security community of practice.

G5 Is familiar with, and can critically evaluate, current and evolving processes and disruptive technologies within the field of cyber security.
G6 Is able to identify appropriate stakeholders and communicate, network and collaborate with these stakeholders at an appropriate level while considering security and confidentiality.
G7 Is able to engage in critical self-reflection, and reflect upon relevant ethical and professional issues, as part of the lifelong learning strategy required of a cyber security professional.

Vurdering

Læringsutbyttebeskrivelsen gir en god beskrivelse av studiet, og reflekterer de kunnskaper, ferdigheter og den generelle kompetanse en vil kunne forvente at en kandidat tilegner seg gjennom et studium i cybersikkerhet der en relativt stor del av studiet er IKT/informatikk-utdanning. Læringsutbyttebeskrivelsene er også i tråd med de generelle læringsutbyttebeskrivelsene gitt i Nasjonalt kvalifikasjonsrammeverk for livslang læring, Nivå 6.2 Bachelor (1. syklus).

Søker har byttet navn på studiet fra Cyberforsvar (Cyber defence) til Cybersikkerhet (Cyber security). Dette er i samsvar med tidligere anbefalinger fra sakkyndig komite, og komiteen synes således at Cybersikkerhet er et dekkende navn for studiet. Samtidig er det mulig å argumentere for at «cybersikkerhet» viser til et breiere fagfelt enn «cyberforsvar» og det savnes derfor en redegjørelse for om det er et reint navnebytte eller om det også reflekterer endringer i studieplanen.

Konklusjon

Ja, kravet er tilfredsstillende imøtekommet.

3.3.2 Studietilbudets faglige oppdatering og relevans

§ 2-2 (2) Studietilbudet skal være faglig oppdatert, og ha tydelig relevans for videre studier og/eller arbeidsliv.

Vurdering

Studiet framstår som faglig oppdatert og relevant. Vedlagt studieplan viser oppdaterte pensumlister. Søknaden gjør ikke eksplisitt rede for rekrutering, men rekruttering har tidligere blitt vurdert av sakkyndige i forbindelse med denne søknaden. NUC har i tidligere søknader gjort rede for en egen markedsavdeling som jobber med markedsaktiviteter som reklame, informasjon til Samordna opptak, informasjon på websider og markedstiltak i sosiale medier.

Sakkyndig komité mener at fagområdets aktualitet gjør studiet slik det er beskrevet relevant for arbeidslivet og mener at NUC har argumentert godt for dette. Søknaden lister opp en rekke virksomheter NUC mener er mulige arbeidsgivere for uteksaminerte studenter. NUC viser til relevante stillingsannonser, men fra søknaden fremgår det bare at NUC har vært i kontakt med en av disse virksomhetene (NSM) for å undersøke om studiet faktisk vil dekke et behov hos dem.

NUC oppgir masterstudier ved partnerinstitusjoner (Teesside University, UK, University of South Wales, UK og Deakin University, Australia) og enkelte andre institusjoner som mulige videre studier i utlandet, og masterstudier ved Universitetet i Ager (UiA) eller NTNU som mulige videre studier i Norge. Sakkyndig komite mener det er sannsynlig at kandidater med Bachelor i Cybersikkerhet fra

NUC vil kunne få opptak på masterstudier ved UiA (Kristiansand) eller NTNU (Gjøvik), men mener NUC må undersøke dette før det ev. presenteres som et alternativ for potensielle studenter.

Konklusjon

Nei, studiet har ikke en tydelig faglig relevans for arbeidsliv og/eller videre studier.

Høyskolen må:

- Undersøke om bachelor i Cybersikkerhet kan gi opptak på masterstudier ved norsk høgskole eller universitet før dette presenteres som et alternativ for studentene.

3.3.3 Studietilbudets arbeidsomfang

§ 2-2 (3) Studietilbudets samlede arbeidsomfang skal være på 1500–1800 timer per år for heltidsstudier.

Vurdering

Søknaden dokumenterer et arbeidsomfang på 1500 timer per år. Av dette er 435 timer (29 %) på førsteåret, 420 timer (28 %) på andre året og 350 timer (23 %) på tredjeåret organiserte læringsaktiviteter («guided education»). Det resterende er selvstudium og tid brukt til forberedelser til- og gjennomføring av vurderingsaktiviteter. Sakkyndig komite finner det totale omfanget og andelen organiserte læringsaktiviteter tilfredsstillende. Av de organiserte læringsaktivitetene ser det ut til at rundt 30 % er forelesinger mens den resterende tiden er satt av til lab og øvingstimer. Sakkyndig komité mener at andelen forelesninger burde kunne økes.

Konklusjon

Ja, kravet er tilfredsstillende imøtekommet.

Høyskolen bør:

- Vurdere å øke andelen forelesninger.

3.3.4 Studietilbudets innhold, oppbygning og infrastruktur

§ 2-2 (4) Studietilbudets innhold, oppbygging og infrastruktur skal være tilpasset læringsutbyttet for studietilbudet.

Vurdering

Studiet består av 16 obligatoriske emner og syv valgemner (studenter skal velge to av disse syv). Av disse er 12 allerede eksisterende emner som inngår i andre bachelorprogrammer.

Etter sakkyndig komités syn, er nivået i læringsutbyttebeskrivelsene på emnenivå passende for en bachelorgrad. Det er også komiteens syn at studiets innhold, i form av summen av de emnene som skal

inngå, er passende for å oppfylle de læringsbyttene som er beskrevet. Emnene i studieplanen følger en naturlig og god progresjon. Studentene skal etter studieplanen ikke skrive bacheloroppgave, men tredje året inneholder emnet «Final Degree Project» (20 studiepoeng fordelt over semester 5 og 6) der studentene må gjennomføre et større prosjekt og levere en prosjektrapport.

Komiteens vurdering er at i hvert fall ett av matematikkemnene (UC3PMC051: Pure Mathematics for Computing) er på et nivå som ikke kan aksepteres som kvalifiserende matematikk for å begynne på teknologimasterstudier i Norge (den har et innhold på nivå med videregående skole hvis en velger R1 og R2). Det er allikevel sakkyndiges vurdering at nivået totalt sett på emnene er slik at det er på bachelornivå.

NUC vil tilby Bachelor i Cybersikkerhet til studenter både ved hovedcampus i Kristiansand, en satellitt/desentralisert campus i Oslo og som nettstudium. NUCs lokaler i Kristiansand har grupperom, auditorier, kantine, PC-laboratorier, cybersikkerhet-laboratorium og spesialtilpassede arbeidsrom. Lokalene i Oslo har kantine, auditorium og fire klasserom, hvorav to utstyrt med stasjonære PCer, tre data-laboratorier og fire grupperom. Det finnes et fysisk bibliotek i Kristiansand med en satellitt i Oslo. Både campusstudenter og nettstudenter har tilgang til elektronisk biblioteksystem for ressurser fra ACM og Ebsco og Dawsonera.

Online-studenter og studenter ved Oslo-campus følger undervisningen gjennom et Virtual Learning Envionment (VLE). VLE består av et LMS, et system for streaming av forelesninger, et virtuelt laboratorium og en chat-tjeneste. Studentene kan følge forelesningene online og delta i praktiske øvinger via det virtuelle laboratoriet.

Samlet vurderer vi det slik at infrastrukturen er tilstrekkelig for at studentene kan ta del i undervisningen og oppnå de spesifiserte læringsutbyttene både ved hovdecampus i Kristiansand, desentralisert campus i Oslo og online. Vi vurderer det også som positivt av NUC legger opp til å ha deler av den faglige staben lokalisert til Oslo-campus.

Konklusjon

Ja, studietilbudets innhold, oppbygning og infrastruktur er tilpasset læringsutbyttet for studietilbudet.

- Vurdere å justere opp nivået på enkelte av matematikkemnene.

3.3.5 Undervisnings-, lærings- og vurderingsformer

§ 2-2 (5) Undervisnings-, lærings- og vurderingsformer skal være tilpasset læringsutbyttet for studietilbudet. Det skal legges til rette for at studenten kan ta en aktiv rolle i læringsprosessen.

Vurdering

Sakkyndig komité stiller seg positive til at NUC legger opp til ulike undervisningsformer med både forelesninger, øvingstimer og lab. Siden studiet kan sees som et spesielt praktisk rettet studium i cybersikkerhet vil øvinger og lab være avgjørende for at kandidatene tilegner seg relevante ferdigheter. Bruken av lab og øvinger, samt «studio»-fagene der studentene arbeider med selvstendige

prosjekter, legger til rette for at studentene vil ha en aktiv rolle i læringsprosessen. Komiteen merker seg likevel at NUC legger opp til relativt få forelesningstimer (se også punkt 3.3.3)

Sakkyndig komité ser det også som positivt at NUC legger opp til varierte vurderingsformer, at ulike typer vurderingsformer kombineres i hvert enkelt emne og at vurderingsformene også inkluderer vurdering av kandidatenes praktiske ferdigheter. Komiteen merker seg at det i liten eller ingen grad blir lagt opp til vurderingsformer som ikke er hjemmearbeid eller online-prøver; dvs. få eller ingen vurderingsformer der det beviselig er studentens eget arbeid som blir vurdert. Komiteen mener NUC burde vurdere å inkludere skriftlige eller muntlige eksamener med personlig oppmøte.

Konklusjon

Ja, studiets undervisnings-, lærings- og vurderingsformer er egnet til å oppnå læringsutbyttet slik det er beskrevet i planen.

Høyskolen bør:

- Vurdere å inkludere skriftlige eller muntlige eksamener med personlig oppmøte blant vurderingsformene.

3.3.6 Kobling til forsknings- og utviklingsarbeid

§ 2-2 (6) Studietilbudet skal ha relevant kobling til forskning og/eller kunstnerisk utviklingsarbeid, og faglig utviklingsarbeid.

Vurdering

NUC legger opp til bruk av vitenskapelige artikler som pensum i flere av emnene og bruk av vitenskapelig litteratur i selvstendige arbeider i «Studio»-emnene og «Final Degree Project». Komiteen anser dette for å være tilstrekkelig kobling til forskning og faglig utviklingsarbeid for et bachelorstudium.

Konklusjon

Ja, studiet har tilfredsstillende kobling til forskning og/eller kunstnerisk utviklingsarbeid og faglig utviklingsarbeid.

3.3.7 Studietilbudets ordninger for internasjonalisering

§ 2-2 (7) Studietilbudet skal ha ordninger for internasjonalisering som er tilpasset studietilbudets nivå, omfang og egenart.

Vurdering

NUC legger opp til bruk av internasjonal litteratur i studiet og arrangerer forelesinger fra internasjonale gjesteforelesere. NUC har godt utbygd infrastruktur for strømming av forelesinger. Denne kan utnyttes til å arrangere gjesteforelesninger uten at foreleseren må reise til Norge, noe som

forenkler arrangementet og øker tilgjengeligheten på internasjonale forelesere. Komiteen anser dette for å være tilstrekkelige ordninger for internasjonalisering for et bachelorstudium.

Konklusjon

Ja, studiet har ordninger for internasjonalisering relevant for studiets nivå, omfang og egenart.

3.3.8 Studietilbudets ordninger for internasjonal studentutveksling

§ 2-2 (8) Studietilbud som fører fram til en grad skal ha ordninger for internasjonal studentutveksling. Innholdet i utvekslingen skal være faglig relevant.

Vurdering

NUC har etablert en ordning for studentutveksling der studentene selv kan finne relevante kurs internasjonalt og søke om å få utveksling innplassert i studiet. NUC har etablert utvekslingsavtaler med Deakin University, Australia, og Teeside University, UK, som sikrer at ordningen for utveksling er reell. Samtidig er ikke ordningen avgrenset til disse samarbeidsinstitusjonene og studentene kan søke om utvekling til andre institusjoner dersom de selv lager avtale med vertsinstitusjonen. Kvalitetssikring i søknadsprosessen sørger for at utvekslingen er faglig relevant.

Konklusjon

Ja, studiet har ordninger for internasjonal studentutveksling relevant for studiets nivå, omfang og egenart.

3.3.9 Praksisavtaler

§ 2-2 (9) For studietilbud med praksis skal det foreligge praksisavtale mellom institusjon og praksissted.

Vurdering

Ikke relevant

3.4 Krav til fagmiljø § 2-3 i studietilsynsforskriften

3.4.1 Fagmiljøets sammensetning, størrelse og kompetanse

§ 2-3 (1) Fagmiljøet tilknyttet studietilbudet skal ha en størrelse som står i forhold til antall studenter og studiets egenart, være kompetansemessig stabilt over tid og ha en sammensetning som dekker de fag og emner som inngår i studietilbudet.

Vurdering

Utfra en sammenstilling komiteen har gjort av tilgjengelig informasjon i søknaden samt vedlagte CVer og tilsendt seinere informasjon på epost ser det ut til at fagmiljøet ved NUC har 15 tilsatte med erfaring og/eller utdanning på ph.d.- eller masternivå innenfor fagområder som kan regnes relevant for cybersikkerhet. Av disse er det 6 som har ph.d. og 9 har MSc (enten i informasjonssikkerhet eller har lang erfaring innen informasjonssikkerhet), alle i fast 100 %-stilling. I tillegg er 3 stillinger med ph.d. i informasjonssikkerhet under ansettelse (ikke signert kontrakter ennå). Det er nødvendig at disse stillingene kommer på plass for å sikre stabilitet over tid i fagmiljøet. Kompetansen i fagmiljøet dekker ellers et bredt spekter av tema innenfor cybersikkerhet.

NUC anslår at studiet vil ha 100 studenter når fullt operativt (opptak av 40 studenter i året, men med et forventet frafall gjennom studiet) fordelt på 50 campusstudenter og 50 online-studenter. Det er ikke angitt noen forventet fordeling mellom Kristiansand-campus og Oslo-campus, men gitt at kapasiteten på f.eks. Cyber Security lab ved de to campusene er lik vil vi legge til grunn at studentene vil være jevnt fordelt mellom campusene. Fagmiljøet knyttet til studiet skal utgjøre 8,5 årsverk. Av disse ser det ut til at ca. 2,5 årsverk skal være reservert Oslo-campus og 1,25 årsverk reservert oppfølging av Online-studenter, mens det resterende vil være tilknyttet Kristiansand-campus.

Komiteen regner det utfra dette for sannsynlig at fagmiljøet har tilstrekkelig størrelse i forhold til forventet antall studenter, og at fagmiljøets kompetanse dekker alle deler av studiet forutsatt at resterende ansettelser blir gjennomført. Fagmiljøet ved NUC besitter også kompetanse og erfaring med nettbasert læring. Faglig stab generelt får tilgang til ulike ressurser for nettbasert læring og formidling.

Konklusjon

Nei, fagmiljøets sammensetning, størrelse og samlete kompetanse er ikke tilpasset studiet slik det er beskrevet.

Høyskolen må:

- Snarest besette de planlagte stillingene for at fagmiljøet og den kompetansen det besitter skal være tilstrekkelig.

3.4.2 Fagmiljøets utdanningsfaglige kompetanse

§ 2-3 (2) Fagmiljøet tilknyttet studietilbudet skal ha relevant utdanningsfaglig kompetanse.

Vurdering

NUC har faglig ansatte med både formell og erfaringsbasert pedagogisk kompetanse. Men merknaden til kravet sier at søkerinstitusjonen også aktivt skal legge til rette for oppdatering og utvikling av denne kompetansen. Videre bør UHRs retningslinjer for pedagogisk basiskompetanse legges til grunn som en minimumsnorm. Sakkyndig komité kan ikke se at NUC har noen program eller ordning for oppdatering og utvikling av den utdanningsfaglige kompetansen, og som sikrer at alle ansatte har eller kan tilegne seg pedagogisk basiskompetanse.

Konklusjon

Nei, fagmiljøet tilknyttet studietilbudet har ikke relevant utdanningsfaglig kompetanse.

Høyskolen må:

- Dokumentere program eller ordning for å sikre at faglig ansatte har eller kan tilegne seg pedagogisk basiskompetanse og utvikling av denne kompetansen.

3.4.3 Faglig ledelse

§ 2-3 (3) Studietilbudet skal ha en tydelig faglig ledelse med et definert ansvar for kvalitetssikring og -utvikling av studiet.

Vurdering

Ut fra en sammenstilling komiteen har gjort av tilgjengelig informasjon i søknaden er det ikke tydelig definert hvem som har ansvar for faglig ledelse med et definert ansvar for kvalitetssikring og -utvikling av studiet (selv om vi kan anta hvem dette skal være).

Konklusjon

Nei, studietilbudet har ikke en tydelig faglig ledelse med et definert ansvar for kvalitetssikring og –utvikling av studiet.

Høyskolen må:

- Definere en tydelig faglig ledelse med et definert ansvar for kvalitetssikring og -utvikling av studiet.

3.4.4 Tilsatte i hovedstillinger

§ 2-3 (4) Minst 50 prosent av årsverkene knyttet til studietilbudet skal utgjøres av ansatte i hovedstilling ved institusjonen. Av disse skal det være ansatte med minst førstestillingskompetanse i de sentrale delene av studietilbudet. I tillegg gjelder følgende krav til fagmiljøets kompetansenivå:

a) For studietilbud på bachelorgradsnivå skal fagmiljøet tilknyttet studiet bestå av minst 20 prosent ansatte med førstestillingskompetanse

b) For studietilbud på mastergradsnivå skal 50 prosent av fagmiljøet tilknyttet studiet bestå av ansatte med førstestillingskompetanse, hvorav minst 10 prosent med professor- eller dosent kompetanse ansatte med førstestillingskompetanse.

c) For studietilbud på doktorgradsnivå skal fagmiljøet tilknyttet studiet bestå av ansatte med førstestillingskompetanse, hvorav minst 50 prosent med professorkompetanse.

Vurdering

Utfra tilgjengelig informasjon i søknaden samt vedlagte CVer og tilsendt seinere informasjon på epost ser det ut til at fagmiljøet ved NUC har 15 tilsatte med erfaring og/eller utdanning på ph.d.- eller masternivå innenfor fagområder som kan regnes relevant til cybersikkerhet. I tillegg er 3 stillinger med ph.d. i informasjonssikkerhet under ansettelse (ikke signert kontrakter ennå). I skrivende stund utgjør fagmiljøet knyttet til studiet totalt 5,5 årsverk, hvorav 2,2 (40 %) er utført av ansatte med førstestillingskompetanse. Når de siste 3 ansettelsene er på plass skal fagmiljøet utgjøre 8,5 årsverk hvorav 5,2 (61 %) med førstestillingskompetanse. I det tilfellet at de 3 vakante stillingene blir besatt av personer uten førstestillingskompetanse vil andelen årsverk med førstestillingskompetanse være 26 % (2,2 av 8,5 årsverk). Det vil si at de kvantitative kravene er oppfylt. 100 % av årsverkene tilknyttet studiet utføres av ansette med hovedstilling hos NUC.

Konklusjon

Ja, fagmiljøet oppfyller de kvantitative kravene.

3.4.5 Fagmiljøets forsknings- og utviklingsarbeid

§ 2-3 (5) Fagmiljøet tilknyttet studietilbudet skal drive forskning og/eller kunstnerisk utviklingsarbeid, og faglig utviklingsarbeid, og skal kunne vise til dokumenterte resultater med en kvalitet og et omfang som er tilfredsstillende for studietilbudets innhold og nivå.

Vurdering

Deler av undervisningspersonellet ved NUC er aktive forskere som kan vise til vitenskapelig produksjon seinere år. Det meste ser ut til å være på NVI-nivå 0 og 1, men komiteen anser produksjonen til å være tilstrekkelig for bachelorgradsnivå (første syklus), og temaene det publiseres innenfor å være relevante for studiet. Videre legger studiet opp til bruk av vitenskapelige artikler som

pensum i flere av emnene og bruk av vitenskapelig litteratur i selvstendige arbeider. Komiteen anser dette for å være tilstrekkelig nivå på forskning og faglig utviklingsarbeid for et bachelorgradsstudium.

Konklusjon

Ja, kravet er tilfredsstillende imøtekommet.

3.4.6 Fagmiljøets eksterne faglige deltakelse

§ 2-3 (6) Fagmiljøet tilknyttet studietilbud som fører fram til en grad skal delta aktivt i nasjonale og internasjonale samarbeid og nettverk som er relevante for studietilbudet.

Vurdering

Nasjonalt deltar NUC i ulike klustere med teknologibedrifter, blant annet DIGIN IT som samler IKT-bedrifter på Sørlandet, som også inkluderer Universitetet i Agder. Komiteen anser dette som tilstrekkelig deltagelse i faglige nettverk på nasjonalt nivå.

På internasjonalt nivå oppgir NUC å ha tegnet samarbeidsavtaler om student og ansatte-utveksling med følgende utenlandske institusjoner: Teesside University, University of South Wales og Norwich University (alle Storbritannia) og Deakin University, Australia. Ansatte ved NUC har personlige kontakter i internasjonale forskingsmiljøer og deltar på internasjonale konferanser.

Konklusjon

Ja, fagmiljøet deltar aktivt i nasjonale og internasjonale samarbeid og nettverk relevante for studiet.

3.4.7 Praksisveiledere

§ 2-3 (7) For studietilbud med obligatorisk praksis skal fagmiljøet tilknyttet studietilbudet ha relevant og oppdatert kunnskap fra praksisfeltet. Institusjonen må sikre at praksisveilederne har relevant kompetanse, og erfaring fra praksisfeltet.

Vurdering

Ikke relevant

4 Samlet konklusjon

På bakgrunn av den skriftlige søknaden med tilhørende dokumentasjon, konkluderer den sakkyndig komiteen med følgende:

Komiteen anbefaler ikke akkreditering av bachelorstudium i Cyber Security ved Noroff University College.

Følgende krav er vurdert som ikke godkjent:

- § 2-2 (2) Studietilbudet skal være faglig oppdatert, og ha tydelig relevans for videre studier og/eller arbeidsliv.
- § 2-3 (1) Fagmiljøet tilknyttet studietilbudet skal ha en størrelse som står i forhold til antall studenter og studiets egenart, være kompetansemessig stabilt over tid og ha en sammensetning som dekker de fag og emner som inngår i studietilbudet.
- § 2-3 (2) Fagmiljøet tilknyttet studietilbudet skal ha relevant utdanningsfaglig kompetanse.
- § 2-3 (3) Studietilbudet skal ha en tydelig faglig ledelse med et definert ansvar for kvalitetssikring og -utvikling av studiet.

Følgende krav må innfris for å oppnå akkreditering:

- Undersøke om bachelor i Cybersikkerhet kan gi opptak på masterstudier ved norsk høgskole eller universitet før dette presenteres som et alternativ for studentene.
- Snarest besette de planlagte stillinger for at fagmiljøet og den kompetansen det besitter skal være tilstrekkelig.
- Dokumentere program eller ordning for å sikre at faglig ansatte har eller kan tilegne seg pedagogisk basiskompetanse og utvikling av denne kompetansen.
- Definere en tydelig faglig ledelse med et definert ansvar for kvalitetssikring og -utvikling av studiet.

Videre har komiteen gitt følgende råd for videre utvikling:

- Gi en mer detaljert beskrivelse av muligheter for studentutveksling i studieplanen
- Gi en beskrivelse av muligheter for videre studier i studieplanen.
- Vurdere å øke andelen forelesninger.
- Vurdere å inkludere skriftlige eller muntlige eksamener med personlig oppmøte blant vurderingsformene.
- Vurdere å justere opp nivået på enkelte av matematikkemnene.

5 Institusjonens kommentar

Noroff University College **Kristiansand, 12/6/2018**

Bachelor in Cyber Security

Viser til mottatte rapport med saksnummer 17/07577.

Vi vil få takke komiteen og Nokut for en god rapport med klare og tydelige krav og anbefalinger til oss.

Vi vil i det videre adressere de enkelte krav med våre kommentarer og beskrivelse av hvordan vi etterkommer disse.

I mottatt rapport fremkommer følgende MÅ punkter/krav:

- Undersøke om bachelor i Cybersikkerhet kan gi opptak på masterstudier ved norsk høgskole eller universitet før dette presenteres som et alternativ for studentene.

- Snarest besette de planlagte stillinger for at fagmiljøet og den kompetansen det besitter skal være tilstrekkelig.

- Dokumentere program eller ordning for å sikre at faglig ansatte har eller kan tilegne seg pedagogisk basiskompetanse og utvikling av denne kompetansen.

- Definere en tydelig faglig ledelse med et definert ansvar for kvalitetssikring og -utvikling av studiet.

– Etter mottak av rapporten har vi kontaktet UiA for nærmere utredning av mulighet for opptak til program på Master nivå for fremtidige uteksaminerte studenter. I dialog med UiA er det avtalt 2 videre prosesser.

– Vurdering om opptak på eksisterende Master i Informasjonssystemer. Her har vi oversendt studieplan til fakultetsleder og fagmiljøet for detaljvurdering. Vedlagt, vedlegg A-1, ligger uttalelse fra UiA som bekrefter opptaksmulighet.

– Vi har videre blitt informert om at det arbeides med etablering av Masterprogram i Cyber Security med oppstart 2019 som antas av UiA til å kunne være passende for våre fremtidige studenter. Det planlagte Master programmet er tiltenkt å ha 2 spesialiseringer. I samtale med UiA er de også interessert i å se på muligheter for hvordan vi sammen kan styrke fagmiljøet i regionen og ha mer synergieffekter mellom institusjonene.

Vi iverksetter tilsvarende prosess med bl.a. NTNU slik at vi får avklart og bekreftet relevante Master programmer, også der, som passende for våre studenter før vi markedsfører og anbefaler alternativer.

– Etter mottak av rapporten har vi engasjert ytterligere to spesialister med førstekompetanse innen to av kjerneområdene i vår utdanning, Computer Science og Penetrasjonstesting, med dertil hørende praktiske sikkerhetsekspertise. I tillegg har vi i samarbeid med vårt partneruniversitet Teesside University avtalt at de supporterer oss med ytterligere kompetanse i oppstarten om nødvendig. Første året er en felles leveranse med våre øvrige IT Bachelorprogrammer, således har vårt personell med

førstekompetanse, ett akademisk år på å forberede de faglige kursene i Cyber Security som skal leveres i år 2 og år 3.

Vedlagt ligger kontrakt og CV for: Dr Isah Jawal, vedlegg B-1 og B-2 Dr Konstantinos Xynos, vedlegg B-3 og B-4

Her følger en oppdatert oversikt som viser at alle fagområder med krav om førstekompetanser er dekket av det samlede fagmiljøet (En person er utsatt til August, men denne er bare en tilleggsressurs/overlappende kompetanse for allerede dekket førstekompetanse innen penetrasjonstesting): (Vi har ikke lagt ved CV´er som er tidligere innsendt, men disse kan gjerne ettersendes om ønskelig)

– Noroff har avtale med UiA om at ansatte kan registrere seg og delta på deres kurs i Universitetspedagogikk. Det er nå en god stund siden vi hadde ansatte med behov for dette og har således forespurt om å få en fornyet bekreftelse på dette og avventer tilbakemelding. Denne bekreftelsen kan ettersendes om ønskelig.

Videre tilbyr vi flere ulike etter og videreutdannelsestilbud for våre ansatte hvor ettårig pedagogisk utdanning er et av alternativene. Dette har 3 ansatte benyttet seg av hittil.

Vedlagt, som vedlegg C-1, ligger også en oversikt over vårt eget 5 ECTS kurs, «Online Tutoring and mentoring», som alle ansatte har tilgang til, både som nyansatte men også i ettertid.

Noroff er medlem i Abelia som blant annet har et eget forum for fagskoler hvor blant annet Høyskolen Kristiania, Westerdals og Noroff Høyskole er medlemmer. Senest på siste styremøte ble det fremlagt et initiativ som fremmes på nasjonalt nivå i forhold til å utarbeide og tilby pedagogisk utdanningsløp med fokus på pedagogikk i praktiske leveranser. Dette finner vi passende for våre fagmiljøer tilknyttet bachelorprogram hvor praktisk kompetanse og anvendelse av teknologi er en viktig faktor. Første pilot er tiltenkt levert våren 2019, og Rektor for Noroff Høyskole har allerede meldt Noroff på som deltaker som stiller med kandidater til dette utdanningsløpet.

– Noroff har nylig tilsatt Dr Beathe Due som Pro Rektor hvor et av hovedfokusområdene er akademisk leveranse og faglig utvikling. I tillegg innehar Professor Iain Sutherland, Dekan rolle for fakultetet som programmet Cyber Security er del av. Rektor, Prorektor og Dekan for fakultetet vil sammen med Professor i Cyber Security, Johan Van Niekerk, utgjøre den faglige ledelsen i Noroff Høyskole relatert til det omsøkte tilbudet.

Ved oppstart av omsøkte tilbud vil også næringslivs-tilknytning bidra til å opprettholde relevans og fremme faglig utvikling.

I det daglige vil Professor i Cyber Security inneha det faglige ansvaret og gjennom forskning, nettverk og med støtte fra kolleger, samt rektoratet, være i stand til å ivareta faglig leveranse og utvikling.

Noroff har også mottatt flere gode anbefalinger til forbedring av programmet. Disse tar vi med oss i det videre forberedelsesarbeidet for leveranse samt i informasjonsmateriellet vi utarbeider til våre nettsider og kommende studenter.

Ta gjerne kontakt om det er ønskelig med ytterligere informasjon eller redegjørelse.

Ernst Sundt

Rektor

Vedlegg:

A-1 – Bekreftelse fra UiA på tilgang til Mastergradsprogram
B-1 – CV Isah Lawal
B-2 – Kontrakt Isah Lawal
B-3 – CV Konstantinos Xynos
B-4 – Kontrakt Konstantinos Xynos
C-1 – Kursbeskrivelse «Online Tutoring and Mentoring».

6 Tilleggsvurdering

6.1 Vurdering av søkerinstitusjonens kommentar

§ 2-2 (2) Studietilbudet skal være faglig oppdatert, og ha tydelig relevans for videre studier og/eller arbeidsliv.

Høyskolen må:

- *Undersøke om bachelor i Cybersikkerhet kan gi opptak på masterstudier ved norsk høgskole eller universitet før dette presenteres som et alternativ for studentene.*

Vurdering

Søker oppgir i sitt tilsvar at de har gått i dialog med Universitetet i Agder (UiA) for å få vurdert mulighetene kandidater med Bachelor i Cyber Security fra NUC har for opptak til Masterstudier ved UiA. En uttalelse fra UiA vedlagt tilsvaret viser at kandidatene er kvalifiserte for opptak på Master i informasjonssystemer under forutsetning av at de tar et 7,5 studiepoeng kurs i samfunnsvitenskapelig metode i løpet av første studieår. Uttalelsen viser også at det er sannsynlig at kandidatene også kan være kvalifiserte til opptak på Masterstudier i IKT. Videre skal UiA ha opplyst søker om at et Masterstudium i cyber security er under planlegging og at det muligheter for at kandidater med Bachelor i Cyber Security fra NUC vil være kvalifiserte for opptak til dette.

Søker oppgir at de vil iverksette en tilsvarende dialog med NTNU. Sakkyndig komite finner redegjørelsen tilfredsstillende.

Konklusjon

Ja, høgskolens redegjørelse er tilfredsstillende.

- Høgskolen bør opprettholde dialogen med UiA om mulighetene for opptak til Masterstudier og søke opprette en tilsvarende dialog med NTNU.

§ 2-3 (1) Fagmiljøet tilknyttet studietilbudet skal ha en størrelse som står i forhold til antall studenter og studiets egenart, være kompetansemessig stabilt over tid og ha en sammensetning som dekker de fag og emner som inngår i studietilbudet.

Høyskolen må:

- *Snarest besette de planlagte stillingene for at fagmiljøet og den kompetansen det besitter skal være tilstrekkelig.*

Vurdering

Søker oppgir i sitt tilsvar en oppdatert oversikt som viser at alle fagområder med krav om førstekompetanser er dekket av det samlede fagmiljøet (en person er utsatt til august, men som de påpeker denne er en tilleggsressurs/overlappende kompetanse for allerede dekket førstekompetanse innen penetrasjonstesting).

Sakkyndig komite finner ordningen passende og redegjørelsen tilfredsstillende.

Konklusjon

Ja, høgskolens redegjørelse er tilfredsstillende.

§ 2-3 (2) Fagmiljøet tilknyttet studietilbudet skal ha relevant utdanningsfaglig kompetanse.

Høyskolen må:

- *Dokumentere program eller ordning for å sikre at faglig ansatte har eller kan tilegne seg pedagogisk basiskompetanse og utvikling av denne kompetansen.*

Vurdering

Søker oppgir i sitt tilsvar at de har avtale med Universitet i Agder (UiA) om at ansatte ved NUC kan følge UiAs kurs i universitetspedagogikk. Videre oppgir søker om at de selv tilbyr et 5 sp kurs i «Online Tutoring and mentoring» som alle ansatte har tilgang til.

Sakkyndig komite finner ordningen passende og redegjørelsen tilfredsstillende.

Konklusjon

Ja, høgskolens redegjørelse er tilfredsstillende.

§ 2-3 (3) Studietilbudet skal ha en tydelig faglig ledelse med et definert ansvar for kvalitetssikring og -utvikling av studiet.

Høyskolen må:

- *Definere en tydelig faglig ledelse med et definert ansvar for kvalitetssikring og -utvikling av studiet.*

Vurdering

Søker oppgir i sitt tilsvar at en sentral professor og dekan for fakultetet som programmet Cyber Security er en del av, sammen med en sentral professor i Cyber Security, vil utgjøre den faglige ledelsen i NUC relatert til det omsøkte studietilbudet. Ved oppstart av det omsøkte studietilbudet vil også næringslivstilknytning bidra til å opprettholde relevans og fremme faglig utvikling. I det daglige

vil professoren i Cyber Security inneha det faglige ansvaret. Vi finner ordningen passende og redegjørelsen tilfredsstillende.

Konklusjon

Ja, høgskolens redegjørelse er tilfredsstillende.

6.2 Samlet konklusjon

På bakgrunn av den skriftlige søknaden med tilhørende dokumentasjon, supplerende informasjon og søkerinstitusjonens kommentar konkluderer den sakkyndig komiteen med følgende:

Komiteen anbefaler akkreditering av Bachelor i Cyber Security ved Noroff University College.

7 Vedtak

NOKUT vurderer at vilkårene i NOKUTs forskrift om tilsyn med utdanningskvaliteten i høyere utdanning (studietilsynsforskriften) av 9. februar 2017 nå er oppfylt.

Vi akkrediterer derfor utdanningen *Cyber Security*(180 studiepoeng) ved Noroff University College. Akkrediteringen er gyldig fra vedtaksdato.

8 Dokumentasjon

17/07577- 4 Noroff University College- Ny versjon av søknad om akkreditering av bachelorgradsstudium i Cyber Security

17/07577- 14 Tilleggsinformasjon vedrørende søknaden i Cyber Security – Noroff University College.

17/07577-16 Tilsvar på utkast til rapport- Noroff University College- Akkreditering av bachelorgradsstudium i Cyber Security.

9 Presentasjon av den sakkyndige komiteen

- **Førsteamanuensis Mass Soldal Lund, Forsvarets høgskole**

Lund er førsteamanuensis i informasjonssikkerhet ved Forsvarets høgskoles ingeniørutdanning i Lillehammer. Lund er emneansvarlig for «Utvikling av forsvarbare informasjonssystem» og er også delaktig i planleggingen og gjennomføringen av Cyber Defence Exercise som gjennomføres årlig. Før han kom til Forsvarets høgskole jobbet Lund i ti år som forsker ved SINTEF IKT. Der forsket han på

bruk av modeller i systemutvikling og software testing, og bruk av risikoanalyse og modeller i informasjonssikkerhet. Lund er medforfatter for en lærebok om sistnevnte tema. Forskningen hans ved Forsvarets høgskole fokuserer på temaene defensive cyberoperasjoner og maritim cybersikkerhet. Hovedfag og doktorgrad har Lund fra Universitetet i Oslo. I sitt doktorgradsarbeid i informatikk jobbet Lund med formelle metoder i systemutvikling (theoretical computer science). Han har også fullført et studium i høgskolepedagogikk. Soldal Lund har tidligere vært sakkyndig for NOKUT og har vært med på å vurdere en tidligere søknad om et tilsvarende studium fra Noroff.

- **Professor Vladimir A. Oleshchuk, Universitetet i Agder**

Oleshchuk har en ph.d. i Computer Science (1988) fra Taras Shevchenko National University i Kiev, Ukraina. I årene 1981-1987 har han besatt ulike stillinger ved forskningsinstitusjoner i Ukraina. I 1987–1992 var han ansatt som førsteamanuensis ved Universitetet i Kiev. Siden 1992 har han vært ansatt ved Universitetet i Agder (tidligere Høgskolen i Agder). I 2004 ble han tilsatt som professor i Computer Science – information security ved Institutt for informasjons- og kommunikasjonsteknologi, Fakultet for teknologi og realfag samme sted. Oleshchuk underviser i sikkerhetsrelaterte emner, matematikk og programmering på bachelor/master/ph.d. Han har også vært veileder for flere enn 40 studenter på master og ph.d-nivå.

De viktigste temaene i Oleshchuks forskning kan relateres til aktiviteter som sikkerhet, personvern og sikkerhet for trådløse systemer og deres applikasjoner til e-helse, trådløse sensornettverk, P2P-systemer og mobile systemer. Hvordan man anvender formelle metoder for å håndheve sikkerhet som tekstanalyse og dataanalyse for å bevare personvern er også et sentralt tema. Oleshchuk kan vise til over 100 vitenskapelige artikler innenfor disse fagområdene. Utover sin undervisnings og forskerkarriere har Oleshchuk bl.a. jobbet som ekstern konsulent, vært deltager i flere evalueringer, vært reviewer for en rekke internasjonale tidsskrift og vært opponent i flere ph.d. disputaser både i Norge og i utlandet. Over en rekke år har Oleshchuk vært sakkyndig for SKVC (tilsvarende NOKUT i Litauen) innen informatikk, IKT og matematikk både som medlem og som komitéleder. Oleshchuk har også tidligere vært sakkyndig for NOKUT i vurderingen av en søknad om akkreditering av et ph.d-studium i Information Security ved Høgskolen i Gjøvik (2008). Han har også vært med på å vurdere en tidligere søknad om et tilsvarende studium fra Noroff.