Kristiania

Programbeskrivelse

Bachelor i cybersikkerhet

Heltid

Stedbasert

180 studiepoeng

Gyldig fra 2024

Studiet er akkreditert av styret: 11.12.2020
Studiet ble re-akkreditert av styret: 18.10.2022
Programbeskrivelsen er godkjent i Lokalt utdanningsutvalg ved School of Economics, Innovation and Technology: 23.10.2023 (LU/SEIT-sak 34/23)

Innholdsfortegnelse

1 Innledning

Etter hvert som utviklingen gjør oss mer og mer avhengig av teknologi, og alle systemer på tvers av kloden snakker sammen, blir vi også mer sårbare ovenfor kriminelle og andre ondsinnede aktører. Cybersikkerhet innebærer å sikre informasjonsteknologi og systemene for operasjonsteknologi mot angrep fra kriminelle hackere, fiendtlige statsmakter og andre trusselaktører. I dette studieprogrammet lærer du å sikre systemer, teste sikkerheten i systemet ved å forsøke å bryte deg inn – og teknikker for å oppdage en inntrenger i et datasystem.

Du får en grundig innføring i sikring av skyløsninger, nettverk, skadevare, kryptering, hacking, penetrasjonstesting, risikoanalyser, hendelseshåndtering, overvåkning, etterforskning og sikkerhetsarkitektur. Studenter ved dette emnet vil også få en grundig forståelse for tingenes internett ("Internet of Things" - IoT) og hvilke sikkerhetsutfordringer dette gir for privatpersoner, samt operasjonell teknologi som styrer alt fra flyplasser til atomkraftverk – og hvilke katastrofale konsekvenser det kan få hvis hackere klarer å ødelegge disse systemene.

For å oppnå denne kompetansen trenger du en dyp teknisk forståelse for hvordan datamaskiner fungerer, hvordan nettverk og nettverksprotokoller er bygget opp, og hvordan dataprogrammer og systemer er utviklet fra høynivå språk til instruksjonsnivå. Studieprogrammet BA i Cybersikkerhet gir deg verktøyene og kunnskapen du trenger for dette, herunder en grundig innføring i hvordan hackere kan bryte seg inn i et program eller et system – og hvordan du kan beskytte mot dette gjennom en kombinasjon av sikkerhetsteknologi, overvåkning, offensiv testing og prosesser.

Dette studiet gir deg også en unik innsikt i hvordan cybertrusler i dag påvirker alt fra kaffetraktere til atomkraftverk, fra svindel av enkeltpersoner og til nasjonal infrastruktur – og hvordan alt dette er koblet sammen gjennom internett. Studiet avsluttes med en grundig innføring i Governance, Risk & Compliance (GRC) og hvordan sikkerhet håndteres fra et ledelsesperspektiv.

Studieprogrammet samarbeider aktivt med næringslivet. Bransjen medvirker gjennom gjesteforelesninger og workshops som en integrert del av undervisningen, samt enkelte forelesere med lang bransjeerfaring.

Studenter fra Cybersikkerhet kan eksempelvis få jobber som:

- Utvikler, arkitekt eller IT-konsulent med fokus på sikkerhet og sikkerhetsmoduler
- Analytiker på Security Operations Center (SOC)
- Hendelseshåndterer og etterforsker
- Driftsteknikker med ansvar for sikkerhetsprodukter
- Penetrasjonstester / etisk hacker

Bachelor i Cybersikkerhet gir mange gode muligheter til videre studier. Det finnes relevante program på masternivå innen IT, programvære utvikling, informasjonssystemer og informasjonssikkerhet ved flere universiteter i Norge hvor studentene kan fortsette utdanning sin. Ved fullføring av bachelorgrad fra Kristiania, vil studentene ha mulighet å søke på mastergradprogram i cybersikkerhet ved Kristiania. Studentene er også kvalifisert for å søke på mastergrad i utlandet eller tilsvarende erfarings-basert mastergrad med forbehold om relevant erfaring fra bransjen.

1.1 Formelle krav

Opptakskrav til studiet er generell studiekompetanse, delkompetanse etter 23/5-regelen eller realkompetanse. Søknad på grunnlag av realkompetanse skal gis individuell behandling, og søker må dokumentere at de innehar de kvalifikasjonene som gjør at de har kompetanse til å gjennomføre studiet. Det henvises til *Forskrift om opptak til høyere utdanning*[1] og *Forskrift om opptak, studier, grader og eksamen ved Høyskolen Kristiania*[2] for mer informasjon.

[1] https://lovdata.no/dokument/SF/forskrift/2017-01-06-13

[2] https://lovdata.no/dokument/SF/forskrift/2018-06-01-813?q=H%C3%B8yskolen%20Kristiania

2 Læringsutbytte

Alle studieprogrammer ved Høyskolen Kristiania har fastsatt et overordnet læringsutbytte som enhver student er forventet å oppnå etter å ha fullført studiet. Læringsutbytte beskriver hva studenten er forventet å vite, kunne og være i stand til å gjøre som et resultat av læringsprosessene knyttet til studiet. Læringsutbytte er beskrevet i kategoriene kunnskap, ferdigheter og generell kompetanse.

Kunnskap

Kandidaten...

- har bred kunnskap om cybersikkerhet, sikkerhetsarkitektur, sentrale teorier og problemstillinger, metoder og verktøy
- kjenner til og kan oppdatere sin kunnskap om forsknings- og utviklingsarbeid innenfor cybersikkerhet
- har kunnskap om økosystemet for sikkerhet
- har kunnskap om komponentene som inngår i moderne mykvareutvikling, som front-end & back-end programmering og databaser, samt kjenner til egnede språk og verktøy for dette
- kjenner til en datamaskins komponenter, hvordan digitale verdier prosesseres og hvordan informasjon behandles og lagres i disse systemene, samt trusler og sikring i denne sammenheng
- har kunnskap om forskjellige prosjektformer og -teknikker, særlig relatert smidig prosjektgjennomføring

Ferdigheter

Kandidaten...

- behersker bransjeverktøy (f.eks. for sikkerhetesting, overvåkning, hendelseshåndtering, risikoanalyser) og teknikker
- kan reflektere over egen faglig utøvelse og justere denne under veiledning og treffe begrunnede valg av IDS, endepunkt beskyttelse, nettverkstrafikk analyse og andre relevant annen relevant programvare
- behersker faglige teknikker og verktøy (IDE, testrammeverk, versjonskontrollverktøy) for informasjonsteknologi

Generell kompetanse

Kandidaten...

- har innsikt i relevante problemstillinger i grunnleggende beskyttelse og responsmekanismer for cybersikkerhet
- kan formidle sentralt fagstoff fra områdene knyttet til cybersikkerhet igjennom både skriftlige og muntlige fremstillingsformer
- kan utveksle synspunkter og erfaringer med andre som har bakgrunn innenfor cybersikkerhet og gjennom dette bidra til etablering og utvikling av rutiner i organisasjon for informasjon og infrastruktur beskyttelse
- kjenner til nytenkning, cybersikkerhet standarter og innovasjonsprosesser

3 Studiets struktur

Bachelor i Cybersikkerhet er et treårig studium som totalt teller 180 studiepoeng, hvorav 150 studiepoeng dekkes av obligatoriske emner, og 30 studiepoeng av valgfrie (valgemner).

Studiet gjennomføres over seks semestre, og strukturen er bygget opp på følgende måte:

Bachelor i Cybersikkerhet				
1. semester	**Introduksjon til programmering 7,5 sp**	**Databaser 7,5 sp**	**Digital teknologi 7,5 sp**	**Kreativt webprosjekt 7,5 sp**
2. semester	**Objektorientert programmering 15 sp**		**Informasjonssikkerhet 7,5 sp**	**Etikk, samfunnsansvar og bærekraft 7,5 sp**
3. semester	**Etisk hacking 15 sp**		**Skysikkerhet 7,5 sp**	**Cyberforsvar 7,5 sp**
4. semester	**Valgemne, utveksling eller praksis 30 sp til sammen**			
5. semester	**Governance, Risk and Compliance 15 sp**		**IoT/OT sikkerhet 7,5 sp**	**Smidig prosjekt 7,5 sp**
6. semester	**Undersøkelsesmetoder 7,5 sp**	**Bachelorprosjekt 22,5 sp**		

Tabell 1 Emnematrise

Obligatoriske emner	Valgemner/utveksling/praksis

3.1 Faglig progresjon

Studie er treårig Bachelor grad og gir til slutten tittelen Bachelor i Cybersikkerhet. En del av første året er felles med Bachelor i Informasjonsteknologi spesialiseringene egne linjer, og gir en solid grunnkompetanse i programmering, prosjektarbeid, systemutvikling, sikkerhet, datateknikk og databaser.

På det andre året er kjernen generell forståelse av cybersikkerhet og de mest relevante verktøy for dette. År to gir spesifikt en innføring i etisk hacking, skysikkerhet og cyberforsvar. Semester fire inneholder valgemner, evt. benytter studenten dette semesteret til utveksling.

I tredje år er fokuset rettet mot Governance, risk & compliance (GRC) og IoT / OT sikkerhet. I tillegg gjennomføres emnet «Smidig prosjekt» i semester fem som samler kunnskapen man har tilegnet seg og lar dette bli anvendt i et større tverrfaglig gruppebasert prosjektarbeid. Det tredje året inneholder også fellesfag fra bachelor IT utdanningen med et innføringsemne i forskningsmetoder med vekt på kvantitative og kvalitative metoder, samt bachelorprosjekt.

3.2 Emner første studieår

Emne	Sp	Beskrivelse
Databaser	7,5	Etter å ha fullført emnet Databaser skal man kunne forklare hva en relasjonsdatabase er, hva den kan brukes til og hvordan den skiller seg fra andre former for persistent lagring. Man skal kunne modellere og strukturere data for et domene. Man skal kunne opprette tabeller, legge inn ulike typer data i disse, kople tabellene sammen og hente ut data og gjøre endringer ved hjelp av SQL spørringer. Man skal kunne forklare og anvende prinsippene for god design (normalisering, nøkkelbruk).
Introduksjon til programmering	7,5	Emnets fokus er å gi studenten en første innføring i grunnleggende programmering. Studenten lærer blant annet om variabler, datatyper, løkker, betingelsessetninger, funksjoner, og bruk av DOM-funksjoner for å endre på HTML og CSS. Det fokuseres på å lage små applikasjoner for nettsider, på klientside, som tar i bruk av funksjoner. Emnet anvender kun ren JavaScript, det vil si gjør ikke bruk av biblioteker eller rammeverk.
Digital teknologi	7,5	For å kunne benytte en datamaskin på en effektiv måte må man vite hvordan informasjon kodes digitalt, samt hvordan den lagres, prosesseres og overføres av og mellom maskinvare og programvare. Ved å arbeide med emnet skal studenten lære seg å analysere datasystemer i ulike abstraksjonslag fra bit-nivå, via digitale kretser og maskinvarekomponenter (CPU, minne, busser og ulikt I/O-utstyr), data vs. instruksjoner, operativsystem, applikasjoner og nettverkskommunikasjon. De skal kunne forklare hvordan man med binærtall kan representere ulike former for informasjon. De skal erverve seg begrepsapparatet som trengs for å vurdere ulik maskin- og programvare opp mot hverandre. De skal kunne benytte modeller for funksjonell lagdeling i systemer, samt prosedyrer og verktøy til å forklare virkemåte og derigjennom kunne utføre effektiv feilsøking av enkeltmaskiner og nettverkskommunikasjon.

Kreativt webprosjekt	7,5	Studenten skal gjennom et prosjekt kunne benytte HTML- og CSS-teknikker for å kunne lage en interaktiv og kreativ løsning med animasjoner (CSS3-animasjon). Etter å ha fullført emnet skal studenten gjennom teamarbeid kunne utføre en kreativ prosess.
Objektorientert programmering	15	Emnet gir en innføring i objektorientert programmering. Studenten kan definere og anvende spesialiseringer av klasser gjennom arv/interface/polymorfi. Studenten blir også introdusert til noen sentrale begreper innen analyse og design ifm utvikling av objektorientert kode.
Informasjonssikkerhet	7,5	Trusselbildet for en datamaskinbruker er i dag preget av angrep fra datakriminelle som er ute etter direkte økonomisk gevinst, eller å overta enkeltmaskiner for å benytte disse videre til kriminell virksomhet. Bevissthet om de ulike truslene som finnes i Internett er forutsetningen for å treffe riktige tiltak. Etter å ha fullført emnet skal en student være i stand til å analysere trusselbildet og foreta egnede sikringstiltak på egen maskin, i eget hjemmenettverk og gi begrunnede råd i forhold til oppsett og teknologivalg for websteder. Man skal også ha oversikt over hvilke lover og forskrifter som gjelder for bruk av datamaskiner til lagring, prosessering og formidling av data, her under personvern og opphavsrett.
Etikk, samfunnsansvar og bærekraft	7,5	Kunnskap om etikk, samfunnsansvar og bærekraft er viktig både for å ta etisk funderte beslutninger og fordi organisasjoners omdømme og lønnsomhet er knyttet til deres sosiale og miljømessige resultater. Dette emnet gir en grunnleggende innføring i problemstillinger, teori og verktøy innen etikk, samfunnsansvar og bærekraft. Sentrale temaer i emnet er etisk teori, etiske dilemmaer, interessentteori, miljø og bærekraft, og bedrifters samfunnsansvar.

Tabell 2 Emner første studieår

3.3 Emner andre studieår

Emne	Sp	Beskrivelse
Etisk hacking	15	Etisk hacking er metoden som brukes av autorisert personell for å omgå systemets sikkerhet for å identifisere potensielle datainnbrudd og trusler i et nettverk. Dette emnet handler om hvordan du tenker som en angriper for å finne svake punkter i infrastrukturen. Etter å fullført emnet Etisk Hacking skal man forstå hvordan simulerte angrep og offensive tester brukes for å styrke sikkerheten i et system eller program. Studentene skal kunne gjennomføre penetrasjonstester av web-applikasjoner for å avdekke sårbarheter, og man skal kunne vurdere og teste et nettverk eller et helt selskap for svakheter som kan utnyttes av en ondsinnet hacker. Man skal kunne forklare og anvende prinsippene for sikker design og arkitektur, og se dette fra en angripers synspunkt.

Skysikkerhet	7,5	Skytjenester har blitt kjernen i den moderne digitaliserte infrastrukturen. Med det økende antallet av nettangrep, må man orkestrere og etablere skytjenester på en sikker måte. Etter å ha fullført emnet Skysikkerhet skal studenten kunne forstå hvordan skytjenester sikres. Man skal kunne planlegge, installere og konfigurere en skybasert løsning, med sikkerhet som en grunnsten gjennom hele prosessen. Man skal kunne forklare og anvende prinsippene for sikker design og arkitektur, og se dette fra et skyperspektiv.
Cyberforsvar	7,5	Cyber Defense inkluderer mekanismer og ferdigheter for å forhindre at datasystemer og ulike enheter blir angrepet og utnyttet av hackere og lignende aktører. Etter å ha fullført emnet skal studenten kunne forstå hvordan IT systemer sikres gjennom sikkerhetsverktøy og metoder, overvåkning og hendelseshåndtering. Studentene skal lære hvordan man jobber med sikring av systemer, hendelseshåndtering og etterforskning knyttet til kompromitterte systemer. Man skal kunne forklare og anvende prinsippene for sikker design og arkitektur, og se dette fra en forsvarers synspunkt.

Tabell 3 Emner andre studieår

3.4 Emner tredje studieår

Emne	Sp	Beskrivelse
Smidig prosjekt	7,5	Hensikten med emnet er å gi studenten en dypere erfaring i å mestre helheten i et større prosjekt, med vekt på bruk av en smidig metode: Scrum. Scrum er et smidig prosessrammeverk for å utvikle innovative produkter og tjenester, spesielt egnet for programvareutvikling. Gjennom en prosess for utvikling av en teknisk løsning skal studenten planlegge og gjennomføre en omfattende prosjektcase for en bedrift i en tverrfaglig gruppe, og vil få trening i å bruke moderne agile teknikker og verktøy underveis. Den første uken vil studenten også bli introdusert til og gjennomføre en sprint-uke med Google Design Sprint.
Governance, Risk & Compliance	15	Etter å fullført emnet Governance, risk & compliance (GRC) skal man kunne forstå sentrale konsepter og prosesser som bidrar til god eier- og virksomhetsstyring (Governance). Man vil lære hvordan risikostyring og compliance krav bidrar til god governance og hvordan GRC styrker måloppnåelse og samtidig kontrollerer og styrer sikkerhetsarbeidet i organisasjonen/selskapet. Man skal kunne forklare og anvende prinsippene innen GRC i en cybersecurity sammenheng, samt forstå hvordan cybersecurity spiller inn i den store sammenhengen og samspillet mellom IT, ansatte, ledelse og eiere av organisasjonen/selskapet.

IoT/OT sikkerhet	7,5	Etter å fullført emnet IoT / OT sikkerhet skal studenten kunne forstå hvordan IoT (Internet of Things) og OT (Operasjonell Teknologi) virker inn på informasjonssikkerhet, både på individ og samfunnsnivå. Fremveksten av Internet of Things medfører at mange flere enheter kobles til og blir tilgjengelig fra Internett, dette gjelder alt fra kjøkkenutstyr i hjemmet og til livskritisk medisinsk utstyr i helsesektoren. Tidligere var dette isolerte komponenter – men som nå er koblet til store skyløsninger og kan styres av brukerne via Internett. Samtidig har Operasjonell Teknologi som styrer strømnett, fabrikker og annen infrastruktur i økende grad blitt koblet direkte eller indirekte til Internett. Kombinasjonen av disse to samfunnsendringene vil ha stor påvirkning for oss alle de neste tiårene, og studenten vil gjennom dette faget forstå både sikkerhetsproblematikk knyttet til dette og hvordan vi kan sikre dette på best mulig måte. Man skal kunne forklare og anvende prinsippene for sikker design og arkitektur, og se dette fra et IoT og OT synspunkt.
Undersøkelsesmetoder	7,5	The aim of this course is to provide students with a fundamental understanding of research as a conceptual, empirical, and practical approach to gathering new insight and knowledge within information technology. Teaching centres on applied research from the fields of information systems and computer science and presents students with relevant methods from this domain, along with their possibilities and limitations. For example: How to develop a research strategy for investigating a problem, how to choose a research method for collecting data and how to critically evaluate the ethical implication of research strategies and methods.

Tabell 4 Emner tredje studieår

3.5 Valgemner/praksis/utveksling fjerde semester

For studieprogrammet *Bachelor i cybersikkerhet* er det lagt opp til at studenter tar et utvekslingsopphold, eller tar valgemner i 4. semester, som til sammen utgjør 30 studiepoeng. Oppdatert informasjon om valgmuligheter gis på Høyskolen Kristianias nettsider og gjennom læringsplattformen.

Det tas forbehold om endringer i hvilke valgemner som tilbys.

3.6 Bachelorprosjekt

Emne	Sp	Beskrivelse
Bachelorprosjekt	22,5	I denne avsluttende oppgaven skal studentene vise at de kan fordype seg i og anvende kunnskapen innenfor sentrale områder i valgt bachelorstudium, og ligge innenfor studieløpets fagområde. Studenten skal få yrkeserfaring ved å gjennomføre et prosjekt i en bedrift, etablere eget selskap eller delta i forskningsprosjekt. Studenten skal demonstrere bred kunnskap om sentrale emner og teorier, og vise ferdigheter i metoder, verktøy og teknologi innenfor fagområdet.

Tabell 5 Bachelorprosjekt

3.7 Industribachelor

Industribachelor er et program der du tar en bachelor (180 studiepoeng) over fire studieår (åtte semestre) og får samtidig 1,5 års arbeidserfaring i en bedrift.
Hvilke studieprogrammer som kan søke vil kunne variere fra år til år avhengig av hvilke bedrifter som det gjøres samarbeid med og de behovene som bedriftene har. Det er begrenset antall plasser per bedrift og antallet plasser avhenger av behovet til bedriftene. Om du får plass eller ikke kommer blant annet an på dine prestasjoner i de fire første semestrene, ditt interessenivå for fagfeltet og hvor godt du er i stand til å jobbe sammen med andre mennesker.
Studiet gjennomføres over 8 semestre og strukturen er bygget opp på følgende måte:

Bachelor i Cybersikkerhet				
1 semester	Introduksjon til programmering	Databaser	Digital Teknologi	Kreativt webprosjekt
2 semester	Objektorientert programmering		Informasjonssikkerhet	Etikk, samfunnsansvar og bærekraft
3 semester	Etisk hacking		Skysikkerhet	Cyberforsvar
4 semester				
5 semester	Governance, Risk and Compliance		Bedrift	
6 semester	100 % i bedrift			
7 semester	Bedrift		IoT/OT sikkerhet	Smidig prosjekt
8 semester	Bachelorprosjekt			Undersøkelsesmetoder

Tabell 6 Emnematrise for industribachelor

4 Undervisnings- og vurderingsformer

4.1 Pedagogisk plattform og gjennomføring av undervisning

Bachelor i Cybersikkerhet er designet slik at summen av emnene og studiearbeidet med disse skal lede studentene frem mot det intenderte læringsutbyttet beskrevet i kapittel 2 i denne programbeskrivelsen.

De enkelte emnene er satt sammen for å vise en bredde innen kunnskap, ferdigheter og generell kompetanse som speiler praksisfeltet. Noen av emnene er mer orienterte mot kunnskapsutbytte, andre mer orienterte mot å bygge spesifikke ferdigheter, mens andre igjen inkluderer flere ferdigheter i koblinger mellom teori og praksis. Dette gjenspeiles i undervisningen.

Arbeids- og undervisning- og vurderingsformer i de enkelte emnene er valgt for å gi et godt og meningsbærende samsvar mellom det læringsutbyttet som ønskes oppnådd, de undervisningsformer som benyttes og den eksamen som avslutter emnet.

De metodiske valgene speiler også emnets bidrag inn i studieprogrammet som et hele. Studentene møter derfor et variert sett med læringsaktiviteter gjennom studietiden, en variasjon som i sum skal speile det praksisfelt studenten utdanner seg til.

Bachelor i Cybersikkerhet legger vekt på å bygge en bred kompetanse innen fagfeltet og på å oppøve studentens evne til selvstendig arbeid. Undervisningen har som mål å kommentere, illustrere og utdype stoff fra læremateriell, samt å gi tilleggsstoff som ikke foreligger i trykt form.

Som ved all høyere utdanning stiller også Høyskolen Kristiania krav til studentenes eget selvstendige læringsarbeid. Høyskolen ser det som sin oppgave å tilrettelegge for og fasilitere studentenes arbeid gjennom gode læringsdesign. Samtidig presiserer vi at en underviser kun kan formidle og legge til rette. Selve læringen skjer hos den enkelte student som en følge av studentens eget arbeid. I tilknytning til undervisningen må studenten derfor regne med en betydelig egeninnsats.

De viktigste arbeids-, undervisnings- og vurderingsformer studenten møter ved *Bachelor i* Cybersikkerhet er beskrevet i det følgende.

- Forelesning/formidling, instruksjon, ikke-spesifisert veiledning og annen lærerledet aktivitet

- Veiledning og formativ vurdering
- Digitalt for- og etterarbeid
- Case-, gruppe- og/eller prosjektarbeid
- Workshops og seminararbeid
- Selvstendig øving / lab-arbeid / praktisk arbeid individuelt eller i grupper
- Annen studentaktivitet, herunder presentasjoner, plenumsdiskusjoner, formidling med videre
- Kollokvie- og oppgavearbeid
- Selvstendig akademisk arbeid med pensum og annet

For studenter som har behov for veiledning utover timeplanlagt undervisning, har høyskolen tilgjengelige fagressurser, herunder administrativt ansatte, bibliotekarer, digitale læringsressurser (f. eks filmer på nett) og studentveiledere. Disse kan kontaktes av den enkelte student ved behov.

I tillegg til litteratur og hjelp til litteratursøk tilbyr biblioteket også variert opplæring i akademisk skriving.

4.2 Eksamens- og vurderingsformer

Vurdering er en situasjon der et innlevert eller presentert arbeid vurderes opp mot et sett kriterier. Kriterier gitt av læringsutbyttet som er definert for det enkelte emne. Vurderingen kan gjøres av medstudenter, undervisere eller sensorer. Disse vil også gjerne gi en tilbakemelding, enten som en veiledende tilbakemelding eller som en karakter (eksamen).

Ved Høyskolen Kristiania skiller vi mellom vurdering *som* læring, vurdering *for* læring og vurdering *av* læring. Formen på de arbeidene som vurderes (vurderingsformen) kan være den samme ved alle disse tre vurderingssituasjonene mens *formålet* varierer.

Ved vurdering som læring (medstudentvurdering) og for læring (tilbakemelding fra underviser) er formålet å forme en læringsprosess, å hjelpe studenten til å oppnå et best mulig læringsresultat. Denne type vurdering oppfatter vi som en del av undervisningsformene, og disse finnes igjen i kapittel 4.1 ovenfor.

Vurdering av læring er en avsluttende vurdering der de faktisk oppnådde læringsresultatene vurderes, eksamen. Eksamen er ved høyskolen Kristiania definert som «En eksamen er en avsluttende oppgave innen et emne eller et avgrenset delemne». Det innleverte eller

presenterte arbeidet vurderes gjennom en sensur, og resultatet av vurderingen skal fremkomme på vitnemålet.
Ved *Bachelor* i *Cybersikkerhet* vil studentene kunne møte på følgende eksamensformer:

- Muntlig eksamen
- Utøvende / praktisk eksamen
- Eksamen under tilsyn
- Hjemmeeksamen
- Mappeeksamen
- Semesteroppgave
- Bacheloroppgave

I enkelte emner er det definert obligatoriske aktiviteter. En obligatorisk aktivitet er krav som må være godkjent for å gå opp til eksamen. Aktiviteten kan enten være et krav om at et eller flere arbeider skal leveres inn (arbeidskrav) og/eller krav om deltakelse ved definerte aktiviteter og/eller forelesninger og/eller obligatorisk praksis.

En obligatorisk aktivitet vurderes som Godkjent/Ikke godkjent, og retten til å gå opp til eksamen i et emne med obligatorisk aktivitet krever at denne aktiviteten er vurdert til Godkjent. I motsatt fall mister studenten eksamensrett i emnet inntil aktiviteten(e) er blitt vurdert til Godkjent.

For utfyllende informasjon om eksamen og obligatorisk aktivitet, se Høyskolen Kristianias hjemmesider.

5 Internasjonalisering og internasjonal studentutveksling

Med henvisning til Studietilsynsforskriften av februar 2017 (§ 2-2, pkt 7 og 8) har studiet ordninger for internasjonalisering og internasjonal studentutveksling.

Ordningene for internasjonalisering er tilpasset studietilbudets nivå, omfang og egenart. Innholdet i ordninger for internasjonal studentutveksling er faglig relevant.

5.1 Ordninger for internasjonalisering

Med internasjonalisering menes her at studietilbudet settes i en internasjonal kontekst og at studentene eksponeres for et mangfold av perspektiver.
Ordninger for internasjonalisering kan omfatte en rekke aktiviteter, slik som bruk av internasjonal litteratur, internasjonale gjesteforelesere, utenlandske studenter på innveksling eller studenters deltagelse på internasjonale konferanser eller workshops i utlandet (listen er ikke uttømmende).
For spesifikke ordninger for internasjonalisering, vises det til studiets emnebeskrivelser.

5.2 Ordninger for internasjonal studentutveksling

Høyskolen Kristiania har avtaler med flere utenlandske læresteder som gir studentene mulighet til å ta et semester i utlandet.

Høyskolen har følgende mobilitetsprogram:

- Nordplus i Norden eller Baltikum
- ERASMUS+ i Europa
- «Exchange» eller «Study Abroad» program, for studenter i og utenfor Europa

For Bachelor Cybersikkerhet tilrettelegges det for utveksling i 4. semester.

Høyskolen Kristiania har avtaler om utvekslingsopphold for studentene og studieoppholdets relevans sikres av studieprogramleder. Utvekslingsemner fra partnere godkjennes av studieprogramleder, for innpass i aktuelle bachelorgrader, her med omfang tilsvarende *30 studiepoeng.*

Ordninger om utveksling gjelder for studenter som har avtale om gradsgivende studier og som har oppnådd minimum 60 studiepoeng ved Høyskolen Kristiania på utreisetidspunktet. For både steds- og nettbaserte studier er utvekslingen stedsbasert.

For nominering til studentutveksling stilles det som regel krav til normert studieprogresjon, karakterer og motivasjonsbrev. Det kan også stilles krav til dokumentasjon av kreativt arbeid/porteføljer og Høyskolen Kristiania kan gjennomføre intervjuer av søkere til utveksling. Høyskolen Kristiania har som målsetting å sende godt kvalifiserte og motiverte studenter til anerkjente utenlandske institusjoner. Vær oppmerksom på at det er et begrenset antall utvekslingsplasser ved studiestedene.

Det tas forbehold om endringer av aktuelle studiesteder, og oppdatert informasjon publiseres på høyskolens nettside. Se utfyllende informasjon om utveksling her: https://www.kristiania.no/for-studenter/studier-i-utlandet/utveksling/