

Oplysninger fra CVR

CVR-nummer

29102384

Virksomhedens navn

Aalborg Universitet

Virksomhedens adresse

Fredrik Bajers Vej 7K, 9220 Aalborg Øst

0. Ansøgningens type

Der ansøges om

- ☐ Ansøgningsskema 1 bacheloruddannelse 180 ECTS-point
- ☐ Ansøgningsskema 2 kandidatuddannelse 120 ECTS-point
- ☐ Ansøgningsskema 3 kandidatuddannelse 75 ECTS-point
- ☐ Ansøgningsskema 4 erhvervskandidatuddannelse 75-120 ECTS-point
- ☒ Ansøgningsskema 5 erhvervskandidatuddannelse som kombinationsuddannelse (1+2) 120 ECTS-point
- ☐ Ansøgningsskema 6 erhvervskandidatuddannelse som kombinationsuddannelse 75-120 ECTS-point

Ansøgningsrunde

2026-2

1. Grundoplysninger for uddannelsen

Navn på institution

Aalborg Universitet

Udbudsted

2450 København SV

Bynavn

København SV

Angiv evt. supplerende bynavn

Uddannelsestype

Erhvervskandidat som kombinationsuddannelse

Fagbetegnelse dansk

Cybersikkerhed

Fagbetegnelse engelsk

Cyber Security

Betegnelse dansk (titel)

Civilingeniør, [cand.polyt.](#) i cybersikkerhed

Betegnelse engelsk (titel)

Master of Science (MSc) in Engineering (Cyber Security)

Hvilket hovedområde hører uddannelsen under?

Teknisk videnskab

Vælg undervisningssprog

- ☐ Dansk
- ☒ Engelsk

Forslag til censorkorps. Angiv hvilket censorkorps, som institutionen ønsker at knytte til uddannelsen

Civilingeniøruddannelsernes censorkorps (elektronik, it og energi)

Hvilke adgangskrav gælder til uddannelsen?

Ansøgere med direkte adgang:

AAU:

- Bachelor of Science (BSc) in Engineering (IT, Communication and New Media)
- Bachelor of Science (BSc) in Engineering (Computer Engineering)
- Bachelor of Science (BSc) in Engineering (Electronic Engineering)
- Bachelor of Engineering (BEng) in Electronics
- Bachelor of Science (BSc) in Computer Science
- Bachelor of Science (BSc) in Engineering (Software)
- Bachelor of Science (BSc) in Information Technology

DTU:

- Bachelor of Science (BSc) in Electrical Engineering
- Bachelor of Science (BSc) in Electrical Engineering
- Bachelor of Science (BSc) in Cyber Technology (former Network Technology and IT)
- Bachelor of Science (BSc) in Software Technology
- Bachelor of Science (BSc) in Software Technology

KU:

- Bachelor of Science (BSc) in Computer Science

ITU:

- Bachelor of Science (BSc) in Software Development

AU:

- Bachelor of Science (BSc) in Computer Science
- Bachelor of Science (BSc) in Computer Engineering
- Bachelor of Science (BSc) in Electronics

SDU:

- Bachelor of Science (BSc) in Electronics
- Bachelor of Science (BSc) in Software Engineering
- Bachelor of Science (BSc) in Computer Science

Vurderingen af kvalifikationer fra andre tekniske eller naturvidenskabelige bacheloruddannelser baseres på dokumenterede kompetencer inden for computerteknologi, softwareteknologi, datalogi, elektronik og matematik svarende til i alt 60 ECTS.

Ækvivalente kvalifikationer kan anerkendes, dog gælder der for de fremhævede fagområder specifikke minimumskrav:

- Matematiske kompetencer på bachelorniveau svarende til mindst 10 ECTS, der dækker fag som lineær algebra, diskret matematik, algoritmer og datastrukturer, sandsynlighedsregning og statistik, kryptografi, calculus, vektorregning, dynamiske systemer, optimering samt reguleringsteknik.
- Kompetencer inden for datalogi, computerteknologi eller elektroteknik på bachelorniveau svarende til mindst 20 ECTS, der dækker fag som computerarkitektur, objektorienteret eller funktionel programmering og modellering, software engineering, systemdesign og -udvikling, distribuerede systemer, analog og digital elektronik, signalbehandling, indlejret programmering, softwarearkitekturer, kravspecificering, applikationsudvikling, webprogrammering, brugeroplevelse samt menneske-maskine interaktion.
- Kompetencer på bachelorniveau svarende til mindst 10 ECTS, der dækker et eller flere af følgende områder: distribuerede systemer, indlejrede systemer, IoT, cloud computing, maskinlæring, databaser, kommunikationsteknologier, computernetværk, sikre kommunikationer og cybersikkerhed. Alle ansøgere skal som minimum dokumentere engelskundskaber svarende til "engelsk på B-niveau" (jf. optagelsesbekendtgørelsen).

Der er tale om en betinget optagelse på EKA 1+2, hvor de studerende har det første år som studerende på heltid til at finde ansættelse til deltidsforløbet. Lykkes det ikke, har de studerende tilbagefaldsret til den ordinære 120 ECTS-kandidatuddannelse.

Beskriv uddannelsens formål og erhvervssigte

Formålet med uddannelsen i cybersikkerhed er at sikre, at de studerende udvikler både teoretisk viden og praktiske færdigheder inden for de komplekse sikkerhedsudfordringer, som virksomheder, offentlige institutioner, sundhedsorganisationer og den finansielle sektor står over for, herunder problemstillinger relateret til netværkssikkerhed, privatlivsbeskyttelse, trusselanalyse, adgangsstyring, cloud security, databeskyttelse og cybersikkerhedsregulering.

I uddannelsen vil der være specifikt fokus på risiko- og trusselanalyser, compliance og sikkerhedsstrategier og kommunikation i krisesituationer. Herudover er målet, at de studerende bliver i stand til at omsætte denne viden i professionel praksis.

De studerende opnår kompetencer til selvstændigt at varetage:

- Kritisk infrastruktur
- Udvikle sikre systemer, netværk og software
- Udarbejde risikoanalyser og designe og implementere strategiske løsninger

Disse kompetencer er relevante i såvel private virksomheder – som [f.eks.](#) PWC, Dubex A/S og Terma – og offentlige institutioner, herunder Statens IT, Digitaliseringsstyrelsen, sundhedsvæsenet samt politi, efterretningstjenester og cybersikkerhedsmyndigheder.

Angiv hvilken struktur og konstituerende faglige elementer uddannelsen består af.

Uddannelsens struktur, moduler, deres placering og ECTS-point er skitseret i vedlagte kassogram, der viser et typisk studieforløb (se bilag).

De konstituerende faglige elementer i studie-ordningen svarer til 95 ECTS-point og valgfag til 25 ECTS-point, herunder 15 ECTS-point valgfri projektmoduler, hvor de enkelte valgmuligheder har særskilte læringsmål.

I det følgende er de konstituerende faglige elementer kort beskrevet for uddannelsens seks semestre.

1. semester:

Grundlæggende sikkerhed og kryptografi (5 ECTS kursusmodul):

Kurset giver et fælles fundament i net-værks og applikationssikkerhed samt grundlæggende kryptografi, så studerende kan forstå centrale sikkerhedsprincipper, algoritmer og angrebstyper.

Netværkssikkerhed (5 ECTS kursusmodul):

Kurset giver en introduktion til netværksovervågning og netværkssikkerhed, herunder centrale trusler, botnets og sikkerhedsprotokoller.

Dilemmaer i cybersikkerhed (5 ECTS kursusmodul):

Kurset fokuserer på etiske, juridiske og praktiske dilemmaer i cybersikkerhed, hvor studerende lærer at forstå værdier, konflikter og konsekvenser i sikkerhedsoperationer.

Sikkerhed i IoT-og cloud-arkitekturer (5 ECTS kursusmodul):

Kurset giver en introduktion til IoT, edge og cloud systemer med fokus på sikkerhed, privatliv og moderne virtualiserings og arkitek-turprincipper.

Sikkerhed i distribuerede systemer (10 ECTS projektmodul):

Projektet fokuserer på udvikling af sikre distribuerede systemer og introducerer samtidig centrale videnskabelige metoder De studeren-de arbejder med sikkerhed, privacy, IoT integration, kildekritik, akademisk praksis og metodisk dataindsamling som grundlag for strukturerede og velformidlede ingeniørfaglige projekter.

2. semester:

Hacker Space (5 ECTS kursusmodul):

Kurset giver praktisk og teoretisk indsigt i netværksbaserede cyberangreb, malware og forsvarsstrategier. De studerende arbejder hands on i sikre testmiljøer med trusselsidentifikation, angrebs- og forsvarsværktøjer, intrusion detection/prevention og analyse af ondsindet netværksaktivitet som DoS, DDoS og misbrug af DNS infrastruktur.

Softwaresikkerhed (5 ECTS kursusmodul):

Kurset giver et solidt fundament i sikker soft-wareudvikling med fokus på sikkerhedsmål, typiske sårbarheder og moderne metoder r til at udvikle sikre programmer. De studerende opnår færdigheder i trusselsvurdering, valg af modforanstaltninger, sikkerhedsanalyse af arkitektur og kode.

Identitets-og adgangshåndtering (5 ECTS kursusmodul):

Kurset giver en dyb forståelse af digitale og fysiske identiteter, privacy principper og moderne teknologier til identitets og adgangsstyring, herunder autentifikation, autorisation, identity and access management og policy arkitekturer. Studerende lærer at designe sikre services, beskytte persondata og analysere informationsflows.

Sikre systemer: Angreb og forsvar (15 ECTS projektmodul):

Kurset giver praktisk og teoretisk erfaring med både beskyttelse og sikkerhedstest af software, embedded og distribuerede systemer, herunder analyse af angrebsvektorer, etablering af modforanstaltninger og håndtering af fundne sårbarheder.

3. semester:

Avancerede emner i cybersikkerhed (5 ECTS kursusmodul):

Kurset bygger videre på de studerendes opnåede kompetencer inden for programmering, softwareudvikling og cybersikkerhed og introducerer avancerede, forskningsbaserede emner inden for netværks- og applikationssikkerhed.

4. semester:

De studerende vælger ét af tre projektmoduler med selvstændige læringsmål:

Projektmodul A: Udvikling af sikre systemer

Kombinerer viden fra tidligere kurser og projekter for at udvikle avancerede cybersikkerhedsløsninger med fokus på sikker softwareudvikling, netværkssikkerhed, kryptografi og adgangskontrol.

Projektmodul B: Governance af it-sikkerhed

Fokuserer på cybersikkerhed i et strategisk og organisatorisk perspektiv, hvor tekniske, juridiske, økonomiske og kulturelle faktorer kombineres for at forstå og håndtere komplekse sikkerhedstrusler.

Projektmodul C: Cybersikkerhedstræning

Fokuserer på at identificere organisationers cybersikkerhedsbehov og udvikle målrettede undervisnings- og træningsforløb, der styrker medarbejderes sikkerhedskompetencer.

5. – 6. semester:

Speciale (30 ECTS projektmodul):

Specialet fokuserer på at gennemføre et forskningsbaseret cybersikkerhedsprojekt, hvor relevante teorier, metoder og eksperimentelle data anvendes til at analysere, afgrænse og løse komplekse sikkerhedsrelaterede problemstillinger.

Derudover udvikles kompetencer inden for videnskabelig formidling, teknologisikkerhed, selvstændigt projektarbejde og faglig specialisering inden for cybersikkerhed.

Angiv antal ECTS-point for hele uddannelsen

120

Angiv normeret studietid i mdr.

34

Her angives beskæftigelseskravet i timer pr. uge (årsnorm)

25

Angiv antal ECTS-point på heltidsforløb (med SU)

60

Heltidskandidatuddannelse som erhvervskandidatuddannelsen giver ret til
indskrivning på

Kandidatuddannelsen i cybersikkerhed

Angiv den firecifrede UDD-kode fra Danmarks Statistik, som er tilknyttet den
heltidskandidatuddannelse som erhvervskandidatuddannelsen giver ret til
indskrivning på

3168

2. Øvrige krav til ansøgningen

Kort beskrivelse af hvordan aftagere og øvrige relevante interessenter er inddraget i processen omkring udvikling af uddannelsen.

AAU har i efteråret 2025 afholdt to åbne dialogmøder i hhv. Aalborg og Esbjerg med en række virksomheder for herigennem at præsentere rammerne for og mulighederne i kandidatreformen.

Efterfølgende har AAU (Prorektor, samt repræsentanter fra enheden AAU-Karriere) deltaget i individuelle dialogmøder med de virksomheder, der har ønsket det. Formålet med de individuelle møder er nærmere præsentation af det nye kandidatlandskab samt yderligere dialog om potentialer for samarbejde om udvikling af de nye uddannelser og virksomhedsinvolvering i de kommende studerendes uddannelsesforløb.

AAU fortsætter også fremadrettet med at afholde møder med de relevante virksomheder med henblik på deling af (nye) informationer, samt understøttelse af samarbejde og netværksskabelse.

Aftagerpanelet for Studienavn for Elektronik og IT samt øvrige relevante interessenter er løbende inddraget i udviklingen af uddannelsen gennem flere komplementære aktiviteter.

De overordnede rammer og perspektiver for erhvervskandidatuddannelser har været drøftet med instituttets aftagerpanel på møde den 27. oktober 2025. Her deltog repræsentanter fra centrale virksomheder inden for elektronik- og IT-området (se bilag).

Den 21. maj 2026 blev der afholdt et industriforum på Campus København med deltagelse af 10 virksomhedsrepræsentanter fra Volvo, Norlys, Radiometer Medical Aps, SenArch, SimCorp, Danish Cloud Community og andre. Deltagerne gav værdifulde input til, hvordan uddannelsen kan implementeres i praksis på tværs af forskellige virksomhedstyper.

Behovet for og indholdet i den konkrete kandidatuddannelse i cybersikkerhed er afdækket gennem løbende dialog med relevante virksomheder og organisationer via uddannelsens faglige netværk. Dette netværk omfatter virksomheder, som de studerende samarbejder med i forbindelse med projektarbejde og projektrelaterede ophold, herunder Terma, Radiometer, SimCorp, Norlys og Tivoli.

3. Baggrundsuplysninger til brug for sagsbehandling

Henvielse til evt. tidligere godkendt heltidsuddannelse og dennes takstindplacering

Kandidatuddannelsen i cybersikkerhed

Forslag til takstindplacering

Heltidstakst 3

Begrundelse for takstindplacering

Samme takstindplacering som heltidskandidatuddannelsen ([cand.polyt.](#)) i cybersikkerhed

Beskriv ligheder og forskelle til beslægtede uddannelser, herunder beskæftigelse og eventuel dimensionering

Uddannelsesforslaget er en del af AAU's institutionsplan og er desuden behandlet som en del af den halvårslige nationale koordinering af nye uddannelser/omlægninger med ophæng i universitetsreformen. Koordineringsprocessen er forankret i Danske Universiteters Uddannelsespolitiske Udvalg (RUP). Der har ikke været indsigelser fra andre uddannelsesinstitutioner ift. uddannelsesforslaget.

Erhvervskandidatuddannelsen i cybersikkerhed er faglig identisk med den eksisterende kandidatuddannelse i cybersikkerhed ved AAU Campus

København. Uddannelsesforslaget har derfor de samme ligheder og forskelle til beslægtede uddannelser som heltidsuddannelsen.

Andre danske universiteter tilbyder for nærværende ikke nogen kandidatuddannelse, der har cybersikkerhed som det centrale omdrejningspunkt. Uddannelsen har et delvist fagligt overlap med kandidatuddannelserne i datalogi, som findes på AAU, AU og SDU, særligt inden for software security, systemdesign og kryptografi.

DTU udbyder en kandidatuddannelse i Computer Science and Engineering, hvor cybersikkerhed indgår som en specialisering, mens AU udbyder en kandidatuddannelse i datalogi med en specialisering i cybersikkerhed. AU's uddannelse er dog mere teoretisk og forskningsorienteret, mens DTU's uddannelse er tilrettelagt som en specialisering inden for en bredere teknisk kandidatuddannelse og har mindre fokus på governance, compliance, trusselhåndtering og organisatorisk implementering. Til forskel herfra har den ansøgte uddannelse cybersikkerhed som sit centrale omdrejningspunkt og er mere direkte orienteret mod anvendt cybersikkerhed.

Behovet for kandidatuddannelsen i cybersikkerhed understøttes af den gennemsnitlige ledighed i 4.-7. kvartal efter dimission, idet denne er meget lav og lå ved seneste opgørelse på hhv. 0,3% og 1,6% (2022 og 2023).

Vælg forventet opstartsår

2028

Angiv forventet optag på uddannelsen det første år

10

Angiv forventet optag på uddannelsen det andet år

10

Angiv det forventede optag på uddannelsen det tredje år

10

Øvrige bemærkninger til ansøgningen?

☒ ★Det bekræftes hermed at ansøgningen er godkendt af rektor

Navn på kontaktperson

Sisse Byskov

Kontaktpersons e-mail

siby@adm.aau.dk

Kontaktpersonens telefonnummer

99403226

Vedhæft samlet PDF-fil

Bilag EKA Cybersikkerhed.pdf

121.1 KB

Bilag til ansøgning om erhvervskandidatuddannelse som kombinationsuddannelse (1+2) 120 ECTS-point

Cybersikkerhed

Indholdsfortegnelse

Kassogram	1
Aftagerpanel 2019	2
Aftagerpanel 2025.....	2

Kassogram

Semester	Semesterstruktur				
	Uddannelse			Uddannelse / Beskæftigelse	
1.	Grundlæggende sikkerhed og kryptografi, 5 ECTS	Netværkssikkerhed, 5 ECTS	Dilemmaer i cybersikkerhed, 5 ECTS	Sikkerhed i IoT- og cloud-arkitekturer, 5 ECTS	Sikkerhed i distribuerede systemer (projekt), 10 ECTS
2.	Hacker Space, 5 ECTS	Softwaresikkerhed, 5 ECTS	Identitets-og adgangshåndtering, 5 ECTS	Sikre systmer: Angreb og forsvar (projekt), 15 ECTS	
3.	Avancerede emner i cybersikkerhed, 5 ECTS	Valgfag, 5 ECTS*	Valgfag, 5 ECTS*	Beskæftigelse	
4.	Valgfrit projekt, 15 ECTS *			Beskæftigelse	
5.	Speciale 30 ECTS			Beskæftigelse	
6.				Beskæftigelse	

Farvekoder:
Obligatorisk
Valgfag/projekt
Projekt
Beskæftigelse

* Valgfag:	3. semester
5 ECTS	Privacy Engineering
5 ECTS	Avanceret software-sikkerhed
5 ECTS	Regulering af IT-sikkerhed
5 ECTS	Sikkerhed og compliance i virksomheder

* Valgfag:	3. semester
5 ECTS	Privacy Engineering
5 ECTS	Avanceret software-sikkerhed
5 ECTS	Regulering af IT-sikkerhed
5 ECTS	Sikkerhed og compliance i virksomheder

Aftagerpanel 2019

Eksterne medlemmer af aftagerpanelet:

- Jan Aagaard, DEIF A/S
- Jens Christian Lindof, RTX
- Claus Siggaard Andersen, Telenor
- Rune Domsten, Indesmatech ApS
- Michael Pedersen, Nilfisk

Interne deltagere:

- Thomas Bak, Instituttleder, Institut for Elektroniske Systemer
- Ove Andersen, Studieleder, Viceinstituttleder, Institut for Elektroniske Systemer
- Tatiana K. Madsen, Studienævnsformand, Studienævn for Elektronik og IT
- Jens Myrup Pedersen, Lektor, Institut for Elektroniske Systemer
- Jan H. Mikkelsen, Lektor, Institut for Elektroniske Systemer
- Henning Olesen, Lektor, Institut for Elektroniske Systemer

Aftagerpanel 2025

Eksterne medlemmer af aftagerpanelet:

- Claus Siggaard Andersen, Vice President 5G Engineering, Gatehouse Satcom A/S
- Jakob Birk Filsø, Principal Engineer, Robotto Co ApS
- Jan Harding Gliemann, CTO - Senior Vice President, DEIF A/S

- Jens Christian Lindof, CTO & Vice President, RTX A/S
- Lars Finn Sloth Larsen, Head of Application and System Software, Danfoss A/S
- Rune Domsten, CO-founder, Indesmatech ApS
- Tobias Piechowiak, Lead Research Scientist, Jabra GN

Interne deltagere:

- Mads Græsbøll Christensen, Instituttleder, Institut for Elektroniske Systemer
- Ove Andersen, Studieleder, Viceinstituttleder, Institut for Elektroniske Systemer
- Lene Sørensen, Studienævnnsforperson, Studienævn for Elektronik og IT