PB i Cybersikkerhed

National del

Studieordning 2026

ERHVERVS AKADEMI SYDVEST

STUDIEORDNING

for

Professionsbachelor i cybersikkerhed

Gældende fra 01.08.2025

Indhold

Denne nationale del af studieordningen for Professionsbachelor i Cybersikkerhed er udstedt i henhold til § 21, stk. 1 i bekendtgørelse om tekniske og merkantile erhvervsakademiuddannelser og professionsbacheloruddannelser. Denne studieordning suppleres af institutionsdelen af studieordningen, som er fastsat af den enkelte institution, der udbyder uddannelsen.

Den nationale del er udarbejdet af uddannelsesnetværket for Professionsbachelor i Cybersikkerhed og godkendt af alle de udbydende institutioner.

1. Uddannelsens mål for læringsudbytte

Viden
Den uddannede har:

- udviklingsbaseret viden om erhvervets praksis og anvendt teori og metode inden for forebyggelse, identificering af og reaktion på cybersikkerhedstrusler i en kompleks organisatorisk sammenhæng
- udviklingsbaseret viden om erhvervets praksis og anvendt teori og metode inden for analyse af organisationskulturers påvirkning af cybersikkerhed samt designprincipper for strukturer, der fremmer cybersikkerhed
- forståelse for praksis og anvendt teori og metode inden for nationale og internationale sikkerhedsstandarder og kan reflektere over cybersikkerhedsprincipper

Færdigheder
Den uddannede kan:

- anvende metoder og redskaber inden for forebyggelse, identificering af og reaktion på cybersikkerhedstrusler og mestre analyse af mulige angreb
- anvende metoder og redskaber inden for nationale og internationale standarder til design og udvikling af cybersikkerhedssystemer, herunder mestre implementering af kryptografiske tiltag
- anvende metoder og redskaber inden for udvikling, drift og governance af IT-systemer og strukturer, der fremmer cybersikkerhed i en kompleks organisatorisk sammenhæng, herunder mestre automatisering af cybersikkerhedsopgaver
- vurdere praksisnære og teoretiske problemstillinger inden for cybersikkerhed samt begrunde og vælge relevante løsningsmodeller for cybersikkerhedstiltag i en kompleks organisatorisk sammenhæng
- formidle praksisnære og faglige problemstillinger og løsninger inden for cybersikkerhed til samarbejdspartnere og brugere

Kompetencer
Den uddannede kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til udvikling, drift og governance af IT-systemer, der fremmer cybersikkerhed i en organisation, samt udvikling og implementering af foranstaltninger til at sikre data
- håndtere komplekse og udviklingsorienterede situationer i arbejds- eller studiesammenhænge i forhold til udvikling og implementering af compliance og sikkerhedskultur i en kompleks organisatorisk sammenhæng
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forhold til at rådgive om samt udvikle og drifte cybersikkerhedsforanstaltninger
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til cybersikkerhed, herunder nationale og internationale trusselsbilleder og sikkerhedsstandarder

2. Uddannelsen indeholder 11 nationale fagelementer

2.1. Forretningsforståelse

Indhold
Fagelementet beskæftiger sig med generel virksomhedsforståelse og værdiskabelse i forretningen, herunder forskellige virksomhedstyper og deres værdikæder. Fagelementet arbejder med sammenhængen mellem forretning, informationsteknologi og cybersikkerhed.
Fagelementet introducerer til cybersikkerhedsmodenhed, inkl. governance og risikostyring, samt den cybersikkerhedsansvarliges rolle i organisationen.

Læringsmål for Forretningsforståelse

Viden
Den studerende har:

- udviklingsbaseret viden om organisationstyper og deres værdikæder, og hvordan cybersikkerhed påvirker virksomhedens økonomi og forretningsprocesser
- roller og ansvar i en organisation i relation til cybersikkerhed
- udviklingsbaseret viden om centrale begreber inden for risikostyring knyttet til arbejdet med cybersikkerhed i en organisation
- projektmodeller
- forståelse for praksis og anvendt teori og metode inden for forandringsledelse og kan reflektere over sikkerhedsmæssige problemstillinger i virksomheden.

Færdigheder
Den studerende kan:

- anvende metoder og redskaber til simpel modenhedsvurdering af en organisation og mestre en struktureret og risikobaseret tilgang til cybersikkerhed
- vurdere praksisnære og teoretiske problemstillinger relateret til risici samt begrunde og vælge relevante løsningsmodeller inden for risikohåndtering
- formidle praksisnære og faglige problemstillinger og løsninger vedrørende cybersikkerhed i en organisatorisk kontekst til samarbejdspartnere, brugere og interessenter

Kompetencer
Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at indgå i samspillet mellem IT-sikkerhed, politikker og IT-systemer i en organisation.
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forhold til cybersikkerhedsarbejdet i en organisation
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til den faglige sikkerhedsprofession i virksomheden

ECTS-omfang
Forretningsforståelse har et omfang på 10 ECTS-point

2.2. Programmering

Indhold:
Fagelementet beskæftiger sig med grundlæggende programmering i et programmeringssprog, som lever op til industriens standard indenfor scripting med et særligt henblik på cybersikkerhed. Herunder datatyper, datastrukturer, teori om fx operatorer, betingelser og kontrol-flow. Et yderligere fokus vil være på funktioner, parametre og inputvalidering. I fagelementet vil der desuden blive arbejdet med data fra f.eks. logfiler og databaser samt anvendelse af prædefinerede moduler og tredjepartsbiblioteker til løsning af specifikke problemstillinger. Der vil også være fokus på selvstændig udvikling af værktøjer og programmer til analyse og håndtering af sådanne data. I fagelementet indgår dokumentation, der formidler funktionalitet og overleverer viden.

Læringsmål for Programmering

Viden
Den studerende har:

- udviklingsbaseret viden om grundlæggende datatyper og datastrukturer og forskelle på disse
- udviklingsbaseret viden om teori inden for programmering med fokus på scripting
- udviklingsbaseret viden om IT-udviklingsmiljøer og brug af disse
- forståelse for praksis og anvendt teori og metode inden for programmering, og kan reflektere over teknikker til at finde information til alternative løsninger

Færdigheder
Den studerende kan:

- anvende metoder og redskaber til behandling af I/O fra såvel lokale filer som eksterne databaser og forbindelser og mestre programmering og tilhørende værktøjer til bearbejdelse af data fra forskellige kilder
- anvende metoder og redskaber i programmeringssprog og mestre validering af input og håndtering af fejl
- vurdere praksisnære og teoretiske problemstillinger inden for valg af datatyper og moduler til en given problemstilling og begrunde og vælge relevante løsningsmodeller inden for programmering
- formidle og dokumentere praksisnære og faglige problemstillinger og løsninger vedrørende egne programmer og deres funktionalitet til samarbejdspartnere og brugere

Kompetencer
Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at udvikle og håndtere basale programmer.
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forhold til udvikling af programmer og moduler, som kan anvendes af andre.
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til at fremsøge og anvende relevante moduler i programmeringssprog

ECTS-omfang
Programmering har et omfang på 10 ECTS-point.

2.3. Computerarkitektur

Indhold:
Fagområdet beskæftiger sig med, hvordan de enkelte elementer i en computer, i form af hardware, operativsystem og software, interagerer med hinanden, samt deres funktioner og den betydning, funktionerne har på cybersikkerhed.

Læringsmål for Computerarkitektur

Viden
Den studerende har:

- udviklingsbaseret viden om arkitektur i IT-kontekst
- udviklingsbaseret viden om forskellige hardwaretyper, herunder CPU, hukommelse, lagring, og input output udstyr
- udviklingsbaseret viden om OS arkitektur, herunder kernel, shell, processer og services samt filsystemer
- viden om forskellige talsystemer
- forståelse for praksis og anvendt teori og metode inden for forskellige applikationstyper og deres arkitektur og kan reflektere over, hvilke behov de opfylder, og hvilke sikkerhedsudfordringer, de kan udgøre
- forståelse for praksis og anvendt teori og metode inden for Cloud arkitektur, herunder IaaS, PaaS og SaaS, og kan reflektere over de overvejelser, der gør sig gældende i et sikkerhedsperspektiv

Færdigheder
Den studerende kan:

- anvende metoder og redskaber til opsætning og anvendelse af operativsystemer og udvalgte applikationer i et virtuelt miljø og mestre installation af forskellige operativsystemer
- anvende metoder og redskaber til grundlæggende tiltag til autentificering og brugerstyring
- anvende metoder og redskaber til cloudløsning og mestre implementering af basale sikkerhedsforanstaltninger i forbindelse med løsningen
- vurdere praksisnære og teoretiske problemstillinger inden for arkitektur i relation til cybersikkerhed samt begrunde og vælge relevante løsningsmodeller inden for cloud eller andre typer af arkitektur
- formidle praksisnære og faglige problemstillinger og løsninger til samarbejdspartnere og brugere vedrørende cybersikkerhed i forbindelse med forskellige arkitekturelementer i operativsystemer, application deployment models samt proceskommunikation og -handlinger

Kompetencer
Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at opsætte et labmiljø til undersøgelse af relevante cybersikkerhedsmæssige problemstillinger.
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forbindelse med udvælgelse og opbygning af relevant systemarkitektur
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til computerarkitekturer i et cybersikkerhedsperspektiv

ECTS-omfang
Computerarkitektur har et omfang på 10 ECTS-point.

2.4. Kommunikation og rapportering

Indhold
Fagelementet beskæftiger sig med, hvordan man kommunikerer effektivt i en virksomhed om cybersikkerhed, både gennem opbygning af en cybersikkerhedskultur og cybersikkerhedstræning og gennem krisekommunikation. Fagelementet indeholder desuden dataindsamling, metrikker, visualisering, formidling og præsentation af cybersikkerhedsrapporter i en organisation, både mundtligt og skriftligt.

Læringsmål for Kommunikation og rapportering

Viden
Den studerende har:

- udviklingsbaseret viden om sikkerhedskommunikation og -rapportering i en virksomhed
- udviklingsbaseret viden om intern og ekstern hændelsesrapportering og krisekommunikation
- forståelse for praksis og anvendt teori og metode inden for indsamling og anvendelse af trusselsvurderinger og kan reflektere over kommunikative virkemidler og kanaler i relation til en virksomheds kultur og værdier

Færdigheder
Den studerende kan:

- anvende metoder og redskaber til data-drevet cybersikkerhed baseret på risici og trusler og mestre opbygning af hændelsesrapportering og krisekommunikation
- vurdere praksisnære og teoretiske problemstillinger relateret til at udarbejde og orientere om trusselsanalyse samt begrunde og vælge relevante løsningsmodeller inden for sikkerhedstiltag
- formidle praksisnære og faglige problemstillinger og løsninger vedrørende cybersikkerhed til relevante interne og eksterne målgrupper i mundtlige præsentationer og skriftlige rapporter

Kompetencer
Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at planlægge og gennemføre awareness aktiviteter, herunder udbrede en risikomodel i en organisation
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forhold til at fremme en cybersikkerhedskultur i en organisation
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til kommunikation og rapportering af cybersikkerhed

ECTS-omfang
Kommunikation og rapportering har et omfang på 10 ECTS-point.

2.5. Automatisering og scripting

Indhold:
Fagelementet har et fokus på indlæring og forståelse af programmeringsdelen af automatisering i et cybersikkerhedsperspektiv. Herunder indgår opbygning af services i forskellige operativsystemer, til f.eks. monitorering eller gentagne operationer, som man gerne vil sikre kører uden brugerinput. I dette fagelement vil der ydermere være et fokus på brug af terminalværktøjer, såsom shell, PowerShell og lignende, for at skabe fortrolighed i denne interaktion mellem terminal og operativsystem. Der vil også være et område af fagelementet, der beskæftiger sig med dokumentationen af disse automatiseringsløsninger.

Læringsmål for Automatisering og scripting

Viden
Den studerende har:

- udviklingsbaseret viden om terminalværktøjer i forskellige operativsystemer
- udviklingsbaseret viden om indbyggede værktøjer til automatisering i operativsystemer
- udviklingsbaseret viden om serialisering
- forståelse for praksis og anvendt teori og metode inden for opbygning af services i et operativsystem og kan reflektere over manuelle løsningers egnethed til automatisering i et sikkerhedsperspektiv

Færdigheder
Den studerende kan:

- anvende metoder, redskaber og relevante moduler til automatisering af sikkerhedstiltag og mestre løsning af problemstillinger inden for domænet ved anvendelsen af en terminal
- vurdere praksisnære og teoretiske problemstillinger vedrørende tredjepartsmoduler samt begrunde og vælge relevante løsningsmodeller inden for scripting og automatisering
- formidle og dokumentere praksisnære og faglige problemstillinger og løsninger vedrørende automatiseringstiltag til samarbejdspartnere og brugere

Kompetencer
Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at benytte terminalværktøjer i gængse operativsystemer
- håndtere komplekse og udviklingsorienterede situationer i forhold til udvikling og konfiguration af nye automatiseringsforslag til gængse operativsystemer
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik ved udvikling af automatiseringsforslag, som kan anvendes af andre
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til at fremsøge og anvende relevante automatiseringsløsninger

ECTS-omfang
Automatisering og scripting har et omfang på 5 ECTS-point.

2.6. Datasikkerhed

Indhold:
Fagelementet beskæftiger sig med lokale og eksterne datalagringssystemer såsom cloud. Der vil i dette fagelement være et fokus på forskellige tiltag og værktøjer man kommer i berøring med i forbindelse med sikring af data samt vurdering af konsekvensen ved brug af disse. Dette indebærer blandt andet et fokus på sikkerhedsparadigmer og sikkerhedsprincipper - herunder CIA-triaden, som er et gennemgående sikkerhedsparadigme på hele uddannelsen – men også principper såsom Least Privilege og Defense In Depth. Der vil i fagelementet ydermere indgå teori om kryptografi, såsom forskellen på hashing og kryptering, og best practices indenfor krypteringsstandarder, samt relevante sårbarheder i forbindelse med backup og databaseløsninger som fx injection.

Læringsmål for Datasikkerhed

Viden
Den studerende har:

- udviklingsbaseret viden om grundlæggende sikkerhedsparadigmer
- udviklingsbaseret viden om forskelle mellem lokal og ekstern lagring
- udviklingsbaseret viden om sikkerhedsdesign-principper
- udviklingsbaseret viden om sårbarheder i forbindelse med lagring og sikring af data
- forståelse for praksis og anvendt teori og metode inden for datasikkerhed og kan reflektere over best practices indenfor sikring af data som kryptering og hashing

Færdigheder
Den studerende kan:

- anvende metoder og redskaber til ekstern lagring af data og mestre tiltag til adgangskontrol, både lokalt og i cloud
- vurdere praksisnære og teoretiske problemstillinger i relation til CIA eller lignende samt begrunde og vælge relevante løsningsmodeller inden for krypteringstiltag til sikring af data

- formidle praksisnære og faglige problemstillinger og løsninger vedrørende datasikkerhed og tilhørende valg af tiltag til samarbejdspartnere og brugere

Kompetencer
Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at vurdere og udvælge metoder til sikring af data i et givent system, herunder værktøjer til adgangskontrol både lokalt og i cloud
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forbindelse med sikring af data
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til best practice inden for datasikkerhed.

ECTS-omfang
Datasikkerhed har et omfang på 5 ECTS-point.

2.7. Netværksarkitektur

Indhold:

Fagelementet beskæftiger sig med netværksudstyr og komponenter og de forskellige udfordringer i netværk knyttet til cybersikkerhed, herunder specificering af relevante sikkerhedskrav til en netværksløsning i cloud- og hybridmiljø. Fagelementet beskæftiger sig med praktisk opsætning, drift og sikring af mindre netværk.

Læringsmål for Netværksarkitektur

Viden

Den studerende har:

- udviklingsbaseret viden om OSI modellen eller tilsvarende reference model
- udviklingsbaseret viden om adressering i de forskellige lag
- udviklingsbaseret viden om relevante netværksprotokoller
- udviklingsbaseret viden om subnetting og routing/segmentering
- udviklingsbaseret viden om netværksudstyr og komponenter
- forståelse for praksis og anvendt teori og metode inden for netværksanalyse og kan reflektere over forskellige sikkerhedsudfordringer i netværk

Færdigheder

Den studerende kan:

- anvende metoder og redskaber til netværksanalyse og mestre opsætning, fejlfinding og tiltag til sikring af mindre netværk
- vurdere praksisnære og teoretiske problemstillinger i forhold til sikkerhedskrav til netværk samt begrunde og vælge relevante løsningsmodeller inden for specificering og deployment af netværksløsninger, herunder i cloud- og hybridmiljø

- formidle praksisnære og faglige problemstillinger og løsninger vedrørende specifikation og dokumentation af sikkerhedskrav til samarbejdspartnere og brugere

Kompetencer

Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at designe, herunder opdele, simple netværk i segmenter ved brug af netværksudstyr
- håndtere komplekse og udviklingsorienterede situationer i forbindelse med analyse af netværkstrafik med henblik på at forebygge eller afbøde angreb
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forhold til design, opsætning og konfigurering af simple netværk
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til protokoller og netværksarkitekturer

ECTS-omfang
Netværksarkitektur har et omfang på 10 ECTS-point.

2.8. Cybersikkerhedsgovernance

Indhold
Fagelementet beskæftiger sig med grundlæggende principper og antagelser i cybersikkerhedsarbejde i en virksomhed. Der vil være fokus på cybersikkerhedsgovernance og virksomhedens politikker, standarder og procedurer, ligesom relevant lovgivning og standarder inden for cybersikkerhed indgår i fagelementet.
Faget beskæftiger sig med ledelsesværktøj til informationssikkerhed, og kommunikation af anbefalinger og analyser på alle niveauer og i alle ledelseslag i en organisation. Fagelementet beskæftiger sig også med praktiske og etiske overvejelser i forhold til rollen som sikkerhedsansvarlig i en organisation.

Læringsmål for Cybersikkerhedsgovernance

Viden

Den studerende har:

- udviklingsbaseret viden om cybersikkerhedsgovernance, herunder virksomhedspolitikker, -standarder og –procedurer
- udviklingsbaseret viden om lovgivning og standarder indenfor it-sikkerhed
- udviklingsbaseret viden om business continuity og disaster recovery
- forståelse for praksis og anvendt teori og metode inden for risikoanalyse og kan reflektere over trusler og trusselsbilleder

Færdigheder

Den studerende kan:

- anvende metoder og redskaber til at vurdere sikkerhedsprincipper i en given kontekst og mestre risikovurdering af mindre systemer og virksomheder
- vurdere praksisnære og teoretiske problemstillinger vedrørende cybersikkerhed ud fra en risikostyringsmodel samt begrunde og vælge relevante løsningsmodeller for mitigerende handlinger ud fra et aktuelt risikobillede
- følge et ledelsesværktøj til informationssikkerhed og formidle praksisnære og faglige problemstillinger og løsninger vedrørende anbefalinger og analyser til samarbejdspartnere, brugere og ledere på alle niveauer i en organisation

Kompetencer

Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at drive udvikling af specifikke cybersikkerhedsstandarder for en given organisation
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i relation til vedligehold og udvikling af en governance model i en organisation
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til at varetage rollen som sikkerhedsansvarlig i en organisation

ECTS-omfang
Cybersikkerhedsgovernance har et omfang på 10 ECTS-point.

2.9. Netværks- og kommunikationssikkerhed

Indhold:
Fagelementet beskæftiger sig med at forstå og håndtere netværkssikkerhedstrusler samt implementere løsninger og konfigurere udstyr til netværks- og kommunikationssikkerhed. Fagelementet omhandler forskelligt sikkerhedsudstyr (IDS) til monitorering. Derudover vurdering af sikkerheden i et netværk, udarbejdelse af plan til at lukke eventuelle sårbarheder i netværket samt gennemgang af forskellige VPN-teknologier.

Læringsmål for Netværks- og kommunikationssikkerhed

Viden
Den studerende har:

- udviklingsbaseret viden om sikkerhed i de mest anvendte protokoller, herunder trådløs sikkerhed
- udviklingsbaseret viden om netværkstrusler
- udviklingsbaseret viden om forskellige sniffingstrategier og -teknikker
- forståelse for praksis og anvendt teori og metode inden for netværksmanagement i et sikkerhedsperspektiv og kan reflektere over forskellige VPN setups samt anvendelsen af gængse netværksenheder

Færdigheder
Den studerende kan:

- anvende metoder og redskaber til overvågning af netværkstrafik og netværkskomponenter og mestre identifikation af sårbarheder, test for angreb rettet mod de mest anvendte protokoller samt reaktion på trusler
- vurdere praksisnære og teoretiske problemstillinger vedrørende virtualisering af netværk samt begrunde og vælge relevante løsningsmodeller til automatisering i forbindelse med netværksadministration
- formidle praksisnære og faglige problemstillinger og løsninger mundtligt og skriftligt til samarbejdspartnere og brugere vedrørende netværksdesign, konfiguration og eventuelle sårbarheder i netværk

Kompetencer
Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at opsætte, konfigurere, monitorere og administrere netværkssikkerhedskomponenter
- håndtere komplekse og udviklingsorienterede situationer i forhold til at anvende krypteringstiltag til sikring af netværkskommunikation
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forhold til at designe, konstruere, implementere samt teste et sikkert netværk
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til netværks- og kommunikationssikkerhed

ECTS-omfang
Netværks- og kommunikationssikkerhed har et omfang på 10 ECTS-point.

2.10. Softwaresikkerhed

Indhold:
Elementet fokuserer på sikkerhedsperspektivet i software, blandt andet programkvalitet og betydningen af fejlhåndtering og datahåndtering for sårbarheder i softwarearkitektur. Elementet introducerer også til forskellige designprincipper, herunder ”security by design”.

Læringsmål for Softwaresikkerhed

Viden
Den studerende har:

- udviklingsbaseret viden om kriterier for programkvalitet og konsekvenserne for cybersikkerhed
- udviklingsbaseret viden om trusler mod software
- udviklingsbaseret viden om fejlhåndtering i programmer
- forståelse for praksis og anvendt teori og metode inden for sikkerhedsdesignprincipper og kan reflektere over "security by design" og "privacy by design"

Færdigheder
Den studerende kan:

- anvende metoder og redskaber til at opdage og forhindre sårbarheder i programkode og mestre håndtering af forventede og uventede fejl samt udvalgte krypteringstiltag
- vurdere praksisnære og teoretiske problemstillinger vedrørende sikkerhedsaspekter samt begrunde og vælge relevante løsningsmodeller inden for anvendelsen af API og/eller standardbiblioteker
- formidle praksisnære og faglige problemstillinger og løsninger til samarbejdspartnere og brugere vedrørende lovlige og ikke-lovlige input data, bl.a. til test

Kompetencer
Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at risikovurdere programkode for sårbarheder
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forhold til i relation til at sikkerhedsvurdere softwarearkitektur
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til sikkerhedsdesign af software

ECTS-omfang
Softwaresikkerhed har et omfang på 10 ECTS-point.

2.11. Systemsikkerhed

Indhold
Fagelementet beskræftiger sig med udvælgelse, anvendelse og implementering af praktiske mekanismer til at forhindre, detektere og reagere over for specifikke cybersikkerhedsmæssige hændelser. Der indgår emner som generelle governanceprincipper og sikkerhedsprocedurer, væsentlige efterforskningsprocesser, it-trusler samt sikkerhedsprincipper i systemsikkerhed. Der vil blive arbejdet med den praktiske del af systemsikkerhed ift. at udnytte modforanstaltninger til sikring af systemer, implementering og analyse af logs for hændelser samt dokumentation af systemer og konfigurering.

Læringsmål for Systemsikkerhed

Viden
Den studerende har:

- udviklingsbaseret viden om sikkerhedsprincipper til systemsikkerhed, herunder overvejelser om adgangskontrol
- udviklingsbaseret viden om sikkerheds-administration i DBMS.
- udviklingsbaseret viden om relevante it-trusler
- udviklingsbaseret viden om væsentlige efterforskningsprocesser

- forståelse for praksis og anvendt teori og metode inden for sikkerhedsprincipper til systemsikkerhed og kan reflektere over genoprettelse af systemer efter en hændelse

Færdigheder
Den studerende kan:

- anvende metoder og redskaber til at implementere systematisk logning og monitering af enheder og mestre at følge et benchmark til at sikre opsætning af enhederne, analysere logs for hændelser samt udnytte modforanstaltninger til sikring af systemer
- anvende metoder og redskaber til at identificere forskellige typer af endpoint-trusler og mestre at fjerne eller afbøde trusler mod systemer
- vurdere praksisnære og teoretiske problemstillinger samt begrunde og vælge relevante løsningsmodeller for krypteringstiltag i forbindelse med systemsikkerhed
- formidle og dokumentere praksisnære og faglige problemstillinger og løsninger vedrørende systemer og konfigurering til samarbejdspartnere og brugere

Kompetencer
Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at håndtere enheder på command line-niveau
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forhold til udvælgelse, anvendelse og implementering af praktiske mekanismer til at forhindre, detektere og reagere over for specifikke it-sikkerhedsmæssige hændelser
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til systemsikkerhed

ECTS-omfang
Systemsikkerhed har et omfang på 10 ECTS-point.

3. Praktik

Læringsmål for praktikken på uddannelsen

Viden
Den studerende har:

- udviklingsbaseret viden om den daglige drift i praktikvirksomheden samt i opgavefunktionen inden for cybersikkerhed
- forståelse for praktikvirksomhedens praksis og anvendelse af teori og metode

Færdigheder
Den studerende kan:

- anvende alsidige tekniske og analytiske arbejdsmetoder samt mestre de færdigheder, der knytter sig til beskæftigelse inden for professionen i praktikvirksomheden
- vurdere praksisnære og teoretiske problemstillinger samt begrunde og vælge relevante løsningsmodeller i relation til praktikopholdet

- formidle praksisnære problemstillinger til praktikvirksomhedens samarbejdspartnere, interessenter og brugere

Kompetencer
Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i relation til praktikopholdet
- selvstændigt og professionelt anvende viden, færdigheder og kompetencer opnået i løbet af uddannelsen til at indgå i fagligt og tværfagligt samarbejde samt påtage sig ansvar for relevante arbejdsopgavers udførelse
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til professionen under praktikopholdet

ECTS-omfang
Praktikken har et omfang på 30 ECTS-point.

Antal prøver
Praktikken afsluttes med 1 prøve.

4. Krav til bachelorprojektet

Bachelorprojektet dokumenterer sammen med uddannelsens øvrige prøver og praktikprøven, at uddannelsens mål for læringsudbytte er opnået.

Bachelorprojektet skal endvidere dokumentere den studerendes forståelse af praksis og central anvendt teori og metode i relation til en praksisnær problemstilling. Problemstillingen skal tage udgangspunkt i en konkret opgave inden for uddannelsens område. Problemstillingen, der skal være central for uddannelsen og erhvervet, formuleres af den studerende, eventuelt i samarbejde med en privat eller offentlig virksomhed. Institutionen skal godkende problemstillingen.

Prøven i bachelorprojektet
Bachelorprojektet afslutter uddannelsen, når alle forudgående prøver er bestået.

ECTS-omfang
Bachelorprojektet har et omfang på 20 ECTS-point.

Prøveform
Prøven består af et projekt og en mundtlig del. Prøven er med ekstern censur, og der gives en samlet individuel karakter efter 7-trin skalaen for projektet og den mundtlige del.

5. Regler om merit

Bestående uddannelseselementer ækvivalerer de tilsvarende uddannelseselementer ved andre uddannelsesinstitutioner, der udbyder uddannelsen.

Den studerende har pligt til at oplyse om gennemførte uddannelseselementer fra en anden dansk eller udenlandsk videregående uddannelse og om beskæftigelse, der må antages at kunne give merit.

Uddannelsesinstitutionen godkender i hvert enkelt tilfælde merit på baggrund af gennemførte uddannelseselementer og beskæftigelse, der står mål med fag, uddannelsesdele og praktikdele.

Afgørelsen træffes på grundlag af en faglig vurdering.

Den studerende har ved forhåndsgodkendelse af studieophold i Danmark eller udlandet pligt til efter endt studieophold at dokumentere det godkendte studieopholds gennemførte uddannelseselementer.

Den studerende skal i forbindelse med forhåndsgodkendelsen give samtykke til, at institutionen efter endt studieophold kan indhente de nødvendige oplysninger.

Ved godkendelse efter ovenstående anses uddannelseselementet for gennemført, hvis det er bestået efter reglerne om den pågældende uddannelse.

6. Ikrafttrædelse

Denne nationale del af studieordningen træder i kraft den 01.08.2025.

Studieordningen gælder for alle studerende på uddannelsen fra ikrafttrædelsesdatoen.

PB i Cybersikkerhed

Institutionsdel

Studieordning 2026

ERHVERVS AKADEMI SYDVEST

Indhold

1. Studieordningens rammer

Bekendtgørelse af lov om erhvervsakademier for videregående uddannelser

Bekendtgørelse af lov om erhvervsakademiuddannelser og professionsbacheloruddannelser (LEP-loven)

Bekendtgørelse om eksamener og prøver ved professions- og erhvervsrettede videregående uddannelser (eksamensbekendtgørelsen)

Bekendtgørelse om adgang til erhvervsakademiuddannelser og professionsbacheloruddannelser (adgangsbekendtgørelsen)

Bekendtgørelse om karakterskala ved uddannelser på Uddannelses- og Forskningsministeriets område (karakterbekendtgørelsen)

Bekendtgørelse om tekniske og merkantile erhvervsakademiuddannelser og professionsbacheloruddannelser

1.1 Ikrafttrædelse og overgangsregler

Denne institutionelle del af studieordningen træder i kraft den 01.01.2026 og har virkning for alle studerende, som påbegynder uddannelsen fra 01.01.2026 og senere.

Studerende indskrevet på uddannelsen før 01.01.2026 færdiggør deres uddannelse ved den studieordning, der var gældende på starttidspunktet, medmindre andet er beskrevet på EASV Moodle. Efter endt orlov eller barsel genoptages studiet undtagelsesvis på den daværende gældende studieordning.

1.2 Den uddannedes titel på dansk og engelsk

Uddannelsen giver den uddannede ret til at anvende betegnelsen Professionsbachelor i cybersikkerhed. Den engelske titel er Bachelor of Cyber Security.

1.3 Uddannelsens formål, omfang og niveau

Formålet med professionsbachelor i cybersikkerhed er at kvalificere den uddannede til at kunne fungere selvstændigt som cybersikkerhedsspecialist med fokus på at arbejde med fortrolighed, integritet og tilgængelighed i forbindelse med udvikling, drift og sikkerhedsledelse af it-systemer i såvel private som offentlige virksomheder og organisationer.
Uddannelsen er indplaceret på niveau 6 i kvalifikationsrammen for videregående uddannelser.

Uddannelsen er nomineret til 210 ECTS-point, der omfatter:

- ✓ Uddannelseselementer med et samlet omfang på 160 ECTS-point, der tilrettelægges inden for uddannelsens faglige områder
- ✓ Praktik med et samlet omfang på 30 ECTS-point
- ✓ Afsluttende bachelorprojekt på 20 ECTS-point

2. Uddannelsens fagområder

Uddannelseselementerne tilrettelægges inden for følgende fagområder, der samlet set omfatter 160 ECTS-point, og som er indbyrdes vægtet i forholdet 1:1:1.

Cybersikkerhedsledelse, -governance og -processer: Fagområdet indeholder viden om governance, ledelsesværktøj og processer til at forhindre, overvåge, detektere og reagere over for trusler mod fortrolighed, integritet og tilgængelighed af systemer og applikationer. Fagområdet omhandler selvstændig organisering og ledelse af sikkerhedsarbejdet i organisationer og virksomheder samt principper, standarder og best practices i cybersikkerhed, herunder etiske, juridiske, politiske og ledelsesmæssige aspekter af cybersikkerhedsarbejde.

Netværkssikkerhed, detektering og arkitektur: Fagområdet indeholder netværksarkitekturer, medier og protokoller samt redskaber til at forhindre, overvåge, detektere og reagere over for trusler mod fortrolighed, integritet og tilgængelighed af netværkskommunikation. Fagområdet indeholder de tekniske komponenter, som udgør de forskellige IT-systemer.

Software- og datasikkerhed og automation: Fagområdet indeholder sikkerhedsperspektivet i software, blandt andet programkvalitet og betydning af fejl- og datahåndtering for en software-arkitekturs sårbarheder. Fagområdet indeholder sikkerhedsdesignprincipper. Desuden indeholder fagområdet tiltag til kryptering og lagring samt automatisering, basal scripting og programmering.

3. Oversigt over uddannelsen

<table>
<tr><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th></tr>
<tr><td>Forretnings-forståelse

10 ECTS</td><td>Kommunika-tion og rapportering

10 ECTS</td><td rowspan="3">Valgfag og specialisering

30 ECTS</td><td>Cyber-sikkerheds-governance

10 ECTS</td><td>Software-sikkerhed

10 ECTS</td><td rowspan="3">Praktik

30 ECTS</td><td>Valgfag og specialisering

10 ECTS</td></tr>
<tr><td>Programme-ring

10 ECTS</td><td>Automatisering og scripting
5 ECTS

Datasikker-hed
5 ECTS</td><td>Netværks- og kommunika-tionssikker-hed

10 ECTS</td><td>System-sikkerhed

10 ECTS</td><td>Bachelor-projekt

20 ECTS</td></tr>
<tr><td>Computer-arkitektur

10 ECTS</td><td>Netværks-arkitektur

10 ECTS</td><td>Valgfag og specialisering

10 ECTS</td><td>Valgfag og specialisering

10 ECTS</td></tr>
</table>

3.1 Nationale fagelementer
Fremgår af den nationale del af studieordningen.

3.2 Lokale fagelementer
På uddannelsen er der udover de nationale fagelementer også 60 ECTS lokale fagelementer, tilrettelagt som valgfag og specialiseringer. I det følgende beskrives de lokale fagelementer og valgfag på uddannelsen, herunder læringsmål, indhold og omfang. Prøver/eksamener i fagelementer samt eksamensforudsætninger fremgår af afsnit 5.

3.3 Valgfag og specialisering
De valgfrie uddannelseselementer og specialiseringer giver den studerende mulighed for at opnå yderligere kompetencer gennem specialisering inden for emner, der i bred forstand relaterer sig til cybersikkerheds-området. Der udbydes løbende en række valgfag. Valgfagene fremgår af valgfagskatalog på EASV Moodle, og udarbejdes i tæt samarbejde med det lokale erhvervsliv og med bidrag fra både undervisere og studerende.

Valgfag og specialisering udgør 60 ECTS på uddannelsen.

De valgfrie elementer udbydes på uddannelsens 3, 4, 5 og 7 semester.

4. Undervisnings- og arbejdsformer
Undervisningen på uddannelsen tilrettelægges som en dynamisk og interaktiv proces med vægt på de studerendes aktive deltagelse, hvor både studerende og undervisere bidrager konstruktivt til læringsprocessen. Det forventes, at den enkelte studerende tager ansvar for egen læring.

Undervisningen tilrettelægges med henblik på at styrke den studerendes evne til at:
- arbejde selvstændigt
- samarbejde med andre
- tænke innovativt

Derfor tilrettelægges undervisningen med udgangspunkt i anvendt teori og relevant erhvervspraksis, herunder generelle problemstillinger og udfordringer inden for cybersikkerheds området.
Der udvælges emner, tværfaglige cases og tematiserede opgaver, der er relevante for forskellige typer af virksomheder, med fokus på de udfordringer, der følger af et omskifteligt cyber trusselniveau, løbende teknologisk udvikling, digitalisering og globalisering.

For at sikre et optimalt og professionelt læringsudbytte samt understøtte den studerendes personlige udvikling anvendes forskellige undervisningsformer.

Centrale undervisningsformer omfatter klasseundervisning, hvor der lægges vægt på dialog og diskussion, projektorienterede cases, individuelle opgaver samt gruppearbejde.
Der kan endvidere indgå gæsteforelæsninger og virksomhedsbesøg.

5. Prøver og eksamener på uddannelsen

Semester	Eksamen/prøve	ECTS-omfang	Intern/ ekstern	Bedømmelse
1. semester	Studiestartsprøve	-	Intern	Godkendt/Ikke godkendt
1. semester	Computerarkitektur	10	Intern	7-trinsskala
2. semester	Førsteårsprøve – prøve i de obligatoriske uddannelseselementer Forretningsforståelse, Kommunikation og Rapportering, Programmering, Automatisering og Scripting, Datasikkerhed og Netværksarkitektur	50	Ekstern	7-trinsskala
3. semester	Valgfag og specialisering	30	Intern	7-trinsskala
4. semester	Cybersikkerhedsgovernance	10	Intern	7-trinsskala
4. semester	Valgfag og specialisering	10	Intern	7-trinsskala
5. semester	Netværks- og Systemsikkerhed – prøve i de obligatoriske uddannelseselementer Netværks- og Kommunikationssikkerhed og Systemsikkerhed	20	Intern	7-trinsskala
5. semester	Softwaresikkerhed	10	Intern	7-trinsskala
5. semester	Valgfag og specialisering	10	Intern	7-trinsskala
6. semester	Praktik	30	Intern	7-trinsskala
7. semester	Valgfag og specialisering	10	Intern	7-trinsskala
7. semester	Hovedopgave	20	Ekstern	7-trinsskala

Oplysninger om tid og sted for de enkelte prøver/eksamener findes på EASV Moodle.

Begyndelsen på semesteret, fagelementer mv. er samtidig en tilmelding til de tilhørende prøver og eksamener. Den studerende har tre prøveforsøg til hver eksamen/prøve, bortset fra studiestartsprøven, hvor der er to prøveforsøg.
Hvis den studerende er afskåret fra at gennemføre uddannelsen, fordi den studerende har opbrugt sine eksamensforsøg, udskrives den studerende fra uddannelsen i henhold til reglerne i Adgangsbekendtgørelsen.

Alle eksamener/prøver afholdes på dansk for PB i cybersikkerhed. Studerende med andet modersmål end dansk kan søge om dispensation fra kravet om, at stave- og formuleringsevne indgår i bedømmelsen af det afsluttede bachelorprojekt, samt de prøver, hvor det af denne studieordning fremgår, at de nævnte evner indgår i bedømmelsen. Ansøgningen sendes til uddannelseschefen senest 4 uger før prøvens afvikling.

Eksamensforudsætninger
For at kunne deltage i en prøve/eksamen kan der være en eller flere eksamensforudsætninger, der skal være opfyldt. Eksamensforudsætninger er beskrevet under de enkelte prøver/eksamener.

En eksamensforudsætning kan være flere forskellige elementer, ex. aflevering af et skriftligt produkt, deltagelse i undervisningen, en præsentation mm.

Manglende opfyldelse af én eller flere eksamensforudsætninger betyder, at den studerende ikke kan deltage i prøven/eksamen, og der er brugt et prøveforsøg.

5.1 Rammer og kriterier for uddannelsens prøver og eksamener
I det følgende beskrives hver enkelt prøve/eksamen i uddannelsens prøver og eksamener, herunder:

- Eksamensforudsætninger
- Prøveform og tilrettelæggelse
- Bedømmelseskriterier
- Formkrav, hvis der indgår et skriftligt produkt, herunder hvis der er krav til individualisering ifm. gruppeprojekter

5.1.1 Studiestartsprøven
I henhold til Eksamensbekendtgørelsen, skal den studerende deltage i og bestå en studiestartprøve for at kunne fortsætte på uddannelsen. Studiestartprøven har til formål at klarlægge, om den studerende reelt er begyndt på uddannelsen. Studiestartprøven afholdes senest to måneder efter uddannelsens start.

Prøveform og tilrettelæggelse
Den studerende skal deltage i en individuel, skriftlig test.
Studiestartsprøven er en opgave, der har til formål af afdække de studerendes forhåndskundskaber og motivation for uddannelsen.

Bedømmelseskriterier
Studiestartprøven har intern bedømmelse, og bedømmes med "Godkendt" eller "Ikke godkendt".

Er prøven ikke godkendt, har den studerende mulighed for at deltage i endnu en studiestartprøve, der skal afholdes senest tre måneder efter uddannelsens start. Den studerende har to forsøg til at få godkendt studiestartprøven.
Prøveformen ved 2. forsøg er den samme som 1. forsøg.
Hvis den studerende ikke får godkendt prøven i 2 forsøg, udskrives den studerende fra uddannelsen i henhold til reglerne i Adgangsbekendtgørelsen.

5.1.2 Computerarkitektur
Eksamensforudsætninger
Aflevering og godkendelse af 2 obligatoriske opgaver, jf. studieplanen på EASV Moodle

Prøveform og tilrettelæggelse
Prøven er en mundtlig individuel prøve, der varer 20 minutter inkl. votering.

Bedømmelseskriterier
Bedømmelsen sker med udgangspunkt i læringsmålene for det obligatoriske uddannelseselement Computerarkitektur, beskrevet i den nationale del af studieordningen.

5.1.3 Førsteårsprøven
Førsteårsprøven skal være bestået inden udgangen af første studieår.
Såfremt den studerende ikke har deltaget i eller består førsteårsprøven inden udgangen af første studieår, udskrives den studerende fra uddannelsen i henhold til reglerne i Adgangsbekendtgørelsen.

Eksamensforudsætninger
- Aflevering og godkendelse af 2 obligatoriske opgaver, jf. studieplanen på EASV Moodle i hvert af de fire obligatoriske uddannelseselementer Forretningsforståelse, Kommunikation og Rapportering, Programmering og Netværksarkitektur
- Aflevering og godkendelse af 1 obligatorisk opgave, jf. studieplanen på EASV Moodle i hvert af de to obligatoriske uddannelseselementer Automatisering og Scripting og Datasikkerhed
- Den skriftlige rapport, som prøven og bedømmelsen baseres på, skal:
    - Opfylde alle formkrav, jf. nedenfor, og
    - Være afleveret rettidigt, jf. eksamensplanen på EASV Moodle

Prøveform og tilrettelæggelse
Prøven er en ekstern, mundtlig gruppeprøve, som tager udgangspunkt i et skriftligt projekt.
Bedømmelsen sker efter 7-trinsskalaen.
Grupperne skal bestå af 2–4 studerende. Eventuelle undtagelser skal godkendes af underviseren.
Prøven dækker 50 ECTS. Der gives én samlet karakter for den skriftlige rapport og den mundtlige præstation.

Projektet præsenteres af gruppen ved den mundtlige prøve, der har en varighed på maksimalt 10 minutter. Herefter gennemføres en individuel eksamination af hvert gruppemedlem på 30 minutter inkl. votering.

Bedømmelseskriterier
Bedømmelsen sker med udgangspunkt i læringsmålene for de obligatoriske uddannelseselementer Forretningsforståelse, Kommunikation og Rapportering, Programmering, Automatisering og Scriptning, Datasikkerhed og Netværksarkitektur, beskrevet i den nationale del af studieordningen.

Formkrav til den skriftlige projektrapport
Projektet skal indeholde følgende:
- Forside med rapporttitel
- Indholdsfortegnelse
- Indledning med hovedtemaer, problemformulering og metodevalg
- Konklusion (der skal være sammenhæng mellem indledning og konklusion; det skal i princippet
- være muligt at forstå konklusionen alene på baggrund af indledningen)
- Litteraturliste (med alle anvendte kilder)
- Bilag (kun dokumenter, der er centrale for rapporten)

Projektet skal have et omfang på minimum 20 normalsider og maksimum 40 normalsider.
En normalside defineres som 2.400 anslag inkl. mellemrum og fodnoter, men ekskl. forside, indholdsfortegnelse, litteraturliste og bilag. Bilag indgår ikke i bedømmelsen.

5.1.4 Cybersikkerhedsgovernance

Eksamensforudsætninger
Aflevering og godkendelse af 2 obligatoriske opgaver, jf. studieplanen på EASV Moodle

Prøveform og tilrettelæggelse
Prøven er en mundtlig individuel prøve, der varer 20 minutter inkl. votering.

Bedømmelseskriterier
Bedømmelsen sker med udgangspunkt i læringsmålene for det obligatoriske uddannelseselement Cybersikkerhedsgovernance, beskrevet i den nationale del af studieordningen.

5.1.5 Netværks- og Systemsikkerhed

Eksamensforudsætninger
Aflevering og godkendelse af 2 obligatoriske opgaver, jf. studieplanen på EASV Moodle i hvert af de to obligatoriske uddannelseselementer Netværks- og Kommunikationssikkerhed og Systemsikkerhed

Prøveform og tilrettelæggelse
Prøven er en mundtlig individuel prøve, der varer 30 minutter inkl. votering.

Bedømmelseskriterier
Bedømmelsen sker med udgangspunkt i læringsmålene for de obligatoriske uddannelseselementer Netværks- og Kommunikationssikkerhed og Systemsikkerhed, beskrevet i den nationale del af studieordningen.

5.1.6 Softwaresikkerhed

Eksamensforudsætninger
Aflevering og godkendelse af 2 obligatoriske opgaver, jf. studieplanen på EASV Moodle

Prøveform og tilrettelæggelse
Prøven er en mundtlig individuel prøve, der varer 20 minutter inkl. votering.

Bedømmelseskriterier
Bedømmelsen sker med udgangspunkt i læringsmålene for det obligatoriske uddannelseselement Softwaresikkerhed, beskrevet i den nationale del af studieordningen.

5.1.7 Valgfag og Specialisering

Eksamener i Valgfag og Specialisering udgør i alt 60 ECTS fordelt på 3., 4., 5. og 7. semester af uddannelsen.
Information om eksamener, herunder forudsætninger og prøveform samt bedømmelseskriterier fremgår af valgfagskataloget på EASV Moodle.

6. Praktik

Læringsmål for praktikken fremgår af den nationale del af studieordningen. Praktikken udgør 30 ECTS.

Krav og forventninger til praktikkens gennemførelse

I praktikken arbejder den studerende med fagligt relevante problemstillinger inden for uddannelsens kerneområder og opnår kendskab til relevante erhvervsfunktioner. Den studerende er under praktikken knyttet til en eller flere virksomheder. Praktikforløbet kan tilrettelægges fleksibelt og differentieret og kan danne grundlag for det afsluttede bachelorprojekt.

Med udgangspunkt i læringsmål for praktikken, jf. den nationale del af studieordningen, fastlægger den studerende og praktikvejlederen i fællesskab konkrete mål for praktikperioden.

Dette er efterfølgende retningsgivende for tilrettelæggelse af den studerendes arbejde i praktikperioden.

Praktikperioden er at sidestille med et fuldtidsjob med de krav til arbejdstid, indsats, engagement og fleksibilitet, som en færdiguddannet må forventes at møde i sit første job. Kan den studerende af dokumenterede helbredsmæssige årsager ikke være i praktik i 37 timer, kan der søges om dispensation til at få tilrettelagt praktikperioden hensigtsmæssigt.

Eksamensforudsætninger

- Den studerende skal have deltaget aktivt i praktikforløbet,
- praktikrapporten, der udgør såvel bedømmelses- som eksaminationsgrundlag, skal opfylde formkravene jf. nedenstående,
- praktikrapporten skal være afleveret rettidigt jf. eksamensplanen, der findes på EASV Moodle, og
- den studerende skal have gennemført evaluering af praktikforløbet via udsendt spørgeskema.

Praktikprøvens tilrettelæggelse og bedømmelse

Praktikprøven er en intern individuel mundtlig prøve på baggrund af praktikrapporten.
Bedømmelseskriterierne vil være læringsmålene for praktik.

Der gives én samlet karakter efter 7-trinsskalaen ud fra en helhedsvurdering af den skriftlige praktikrapport og den mundtlige præstation.

Eksaminanden præsenterer centrale emner fra praktikopholdet i ca. 15 minutter, herefter gennemføres en eksaminationsdialog, hvor alle emner fra praktikforløbet kan inddrages. Der afsættes 30 minutter pr. eksaminand inkl. votering.

Praktikprøven kan afholdes som videokonference, såfremt det godkendes af uddannelseschefen.

Prøven placeres på uddannelsens 6. semester efter endt praktikophold. Nærmere oplysning om tid og sted samt om aflevering af praktikrapport findes på EASV Moodle.

Formkrav til det skriftlige projekt

Praktikrapporten, som udgør den skriftlige del af prøven, skal minimum indeholde:

- Forside med navn, praktikvirksomhed, skole, praktikperiode
- Forord
- Indledning
- Beskrivelse af virksomheden. (Hvad beskæftiger virksomheden sig med, hvor mange ansatte, hvad er deres profession osv.)
- Refleksioner over opnåelse af konkrete læringsmål
- Beskrivelse af konkrete arbejdsopgaver
- Konklusion
- Bilag: Virksomhedsudtalelse og logbog/dagbog
- Evt. litteraturliste (inkl. alle kilder, der er lavet henvisninger til i projektet)
- Evt. yderligere bilag (inkluder kun bilag, som er centrale for rapporten)

Praktikrapporten skal maksimum være 20 normalsider foruden bilag. En normalside er 2.400 tegn inkl. mellemrum og fodnoter. Forside, indholdsfortegnelse, litteraturliste samt bilag tæller ikke med heri. Bilag er uden for bedømmelse.

Praktikrapporten afleveres på dansk for PB i cybersikkerhed.

7. Det afsluttende bachelorprojekt

Det afsluttende projekt skal sammen med prøven efter praktikken og uddannelsens øvrige prøver dokumentere, at uddannelsens mål for læringsudbytte er opnået.

For krav til det afsluttende bachelorprojekt samt læringsmål henvises til den nationale del af denne studieordning.

Prøven placeres ved udgangen af uddannelsens sidste semester. Nærmere oplysning om tid og sted findes på EASV Moodle.

Eksamensforudsætninger

Ikke korrekt aflevering af det skriftlige projekt, som udgør den skriftlige del af prøven, betyder at den studerende ikke kan deltage i prøven, og der er brugt et prøveforsøg.

Prøven kan først finde sted efter at den afsluttende prøve i praktikken og uddannelsens øvrige prøver er bestået.

Prøveform og tilrettelæggelse

Prøven er en ekstern individuel prøve, der bedømmes efter 7-trinsskalaen.
Grupper skal bestå af 2–4 studerende. Eventuelle undtagelser skal godkendes af uddannelseschefen.
Der gives én samlet karakter for den skriftlige rapport og den mundtlige præstation.
Projektet præsenteres af den studerende i 15 minutter, efterfulgt af en eksaminationsdialog. Der afsættes

30 minutter pr. eksaminand inkl. votering.

Det afsluttende eksamensprojekt udgør 20 ECTS.

Prøvens sprog er dansk for PB i cybersikkerhed.

Bedømmelseskriterier

Bedømmelseskriterierne er læringsmålene for uddannelsen jf. den nationale del af studieordningen. Stave- og formuleringsevne indgår i bedømmelsen.

Formkrav til det skriftlige projekt

Projektrapporten skal have et omfang på mindst 20 normalsider. Projektrapport udarbejdet af én studerende må maksimalt udgøre 40 normalsider; projektrapport udarbejdet af flere studerende kan udvides med yderligere 10 normalsider pr. studerende.

8. Fagelementer som kan gennemføres i udlandet

Den studerende kan efter uddannelsens godkendelse af en ansøgt forhåndsmerit gennemføre hvert enkelt fagelement i udlandet. Ved forhåndsgodkendelse af studieophold i udlandet har den studerende pligt til efter endt studieophold at dokumentere det godkendte studieopholds gennemførte fagelementer. Den studerende skal i forbindelse med forhåndsgodkendelsen give samtykke til, at institutionen efter endt studieophold kan indhente de nødvendige oplysninger. Ved godkendelse af forhåndsmerit anses fagelementet for gennemført, hvis det er bestået efter reglerne om uddannelsen.

9. Merit for lokale fagelementer herunder valgfag

Bestående lokale fagelementer erstatter de tilsvarende fagelementer ved andre uddannelsesinstitutioner, som udbyder denne uddannelse såvel som ved andre uddannelser. Der søges om forhåndsmerit, hvis der ønskes merit for fagelementer, som ikke udbydes af uddannelsen.

10. Deltagelsespligt

For at undervisningen kan fungere optimalt og uddannelsens læringsmål og -udbytte kan opnås, har den studerende deltagelsespligt i form af aflevering/fremlæggelse af opgaver/projekter mv.

Aflevering/fremlæggelse af opgaver/projekter mv. kan være udtrykt som eksamensforudsætninger, der skal opfyldes, førend den studerende kan deltage i den pågældende eksamen. Eksamensforudsætninger er beskrevet under de enkelte eksamener i afsnit 5.

Uddannelsen griber ind med hjælp og vejledning så tidligt som muligt, hvis en studerende ikke overholder sin deltagelsespligt.

11. Studieaktivitet

På Erhvervsakademi SydVest skal den studerende være studieaktiv for fortsat at være indskrevet på uddannelsen. På Erhvervsakademi SydVest er manglende studieaktivitet defineret således, at *den studerende ikke har bestået nogen af uddannelsens prøver og eksamener i en sammenhængende periode på 1 år.*

Manglende opfyldelse af studieaktivitetskravet medfører udskrivning fra uddannelsen i henhold til reglerne i Adgangsbekendtgørelsen.

12. Prøvevilkår

Begyndelsen på semesteret, fagelementer mv. er samtidig en tilmelding til de tilhørende eksamener/prøver.

Den studerende kan kun framelde sig eksamen med begrundelse i sygdom (ved lægeerklæring), dødsfald i familien eller usædvanlige forhold som har indflydelse på den studerendes almene tilstand. Derudover kan der dispenseres for reglerne, hvis den studerende er eliteidrætsudøver, og på den baggrund er nødsaget til at framelde sig eksamen. Afmeldingen skal ske til uddannelseschefen senest ved eksamensstart eller snarest muligt derefter. Der skal forelægge skriftlig dokumentation for afmeldingen, før der evt. gives dispensation for det brugte eksamensforsøg.

12.1 Hjælpemidler

Eventuelle regler for indskrænkning af brug af hjælpemidler, vil fremgå af beskrivelsen af den enkelte prøve.

12.2 Særlige prøvevilkår

Den studerende kan, hvor det er begrundet i fysisk eller psykisk funktionsnedsættelse, søge om særlige prøvevilkår. Ansøgningen skal indgives til uddannelseschefen senest 4 uger før prøven afvikles. Der kan dispenseres fra ansøgningsfristen ved pludselig opståede helbredsmæssige problemer. Ansøgningen skal ledsages af en lægeattest, udtalelse fra fx tale-, høre-, ordblinde- eller blindeinstitut eller anden dokumentation for helbredsmæssige forhold eller relevant specifik funktionsnedsættelse.

12.3 Syge- og omprøve

12.3.1 Sygeprøve

Hvis den studerende har været forhindret i at gennemføre en prøve på grund af dokumenteret sygdom eller af anden uforudseelig grund, får den studerende mulighed for at aflægge (syge)prøven snarest muligt. Er det en prøve, der er placeret i uddannelsens sidste eksamenstermin, får den studerende mulighed for at aflægge prøven i samme eksamenstermin eller i umiddelbar forlængelse heraf.

Sygeprøven kan være identisk med næste ordinære prøve. Den studerende skal selv orientere sig om, hvornår (syge)prøven afvikles. Orientering om tid og sted for sygeprøver findes på Moodle.

Sygdom skal dokumenteres ved lægeerklæring. Institutionen skal senest have modtaget lægeerklæring tre

hverdage efter prøvens afholdelse. Studerende, der bliver akut syge under en prøves afvikling, skal dokumentere, at vedkommende har været syg på den pågældende dag. Dokumenteres sygdom ikke efter ovenstående regler, er der brugt et prøveforsøg. Den studerende skal selv afholde udgiften til lægeerklæring.

12.3.2 Omprøve

Ved ikke bestået prøve eller ikke fremmøde ved prøve er den studerende automatisk tilmeldt omprøve, så længe der resterer prøveforsøg. Den studerende kan være tilmeldt 3 gange til den samme prøve. Omprøven kan være identisk med næste ordinære prøve. Den studerende skal selv orientere sig om, hvornår omprøven afholdes. Orientering om tid og sted for omprøver findes på Moodle.

13. Fejl eller mangler i forbindelse med eksamen/prøve

Hvis der bliver gjort opmærksom på fejl og mangler i forbindelse med en eksamen/prøve, træffer uddannelseschefen afgørelse om, hvordan fejlen eller manglen kan afhjælpes.

Ved fejl eller mangler af særlig alvorlig karakter, eller hvor det må anses at være den mest korrekte måde at afhjælpe fejlen på, kan uddannelseschefen annullere den pågældende eksamen/prøve og foranstalte en omprøve. Ved en annulleret prøve/eksamen bortfalder bedømmelsen.

Ved andre væsentlige fejl eller mangler kan der gives tilbud om en ekstraordinær eksamen. Tilbuddet gives til alle berørte studerende. Den studerende kan vælge at beholde sin oprindelige bedømmelse, selvom vedkommende har deltaget i den ekstraordinære eksamen.

14. Eksamenssnyd og forstyrrende adfærd

Under eksamen/prøve skal den studerende optræde hensynsfuldt, herunder efterleve de anvisninger, som gives af eksamenstilsynet, eksaminator og censor.

Snyd til prøver og eksamen behandles efter reglerne i Bekendtgørelse om eksamener og prøver i professions- og erhvervsrettede videregående uddannelser (eksamensbekendtgørelsen).

Det betegnes eksempelvis som eksamenssnyd, når den studerende:

- plagierer jf. afsnit 14.1,
- forfalsker,
- fortier eller vildleder om egen indsats eller resultater,
- indgår i ikke-tilladt samarbejde,
- modtager eller forsøger at modtage hjælp under eksamen eller prøve, eller hjælper andre, når der ikke er tale om gruppeprøve,
- benytter ikke-tilladte hjælpemidler,
- uretmæssigt har opnået forudgående kendskab til eksamensopgaven,
- afgiver uretmæssige fremmødeoplysninger, eller
- forsøger at omgå, deaktivere eller på anden måde hindre hensigten med EASV's anvendelse af overvågningsprogrammer.

Den studerende skal ved aflevering af en skriftlig besvarelse med underskrift bekræfte, at opgaven er udfærdiget uden uretmæssig hjælp.

14.1 Brug af eget og andres arbejde – plagiat

Eksamenssnyd ved plagiering omfatter tilfælde, hvor en skriftlig opgave helt eller delvist fremtræder som produceret af eksaminanden eller eksaminanderne selv, selv om opgaven:

1) omfatter identisk eller næsten identisk gengivelse af andres formuleringer eller værker, uden at det gengivne er markeret med anførselstegn, kursivering, indrykning eller anden tydelig markering med angivelse af kilden, jf. institutionens krav til skriftlige arbejder på Moodle
2) omfatter større passager med et ordvalg, der ligger så tæt på et andet værk eller lignendes formuleringer m.v., at man ved sammenligning kan se, at passagerne ikke kunne være skrevet uden anvendelse af det andet værk
3) omfatter brug af andres ord eller idéer, uden at disse andre er krediteret på behørig vis
4) genbruger tekst og/eller centrale idéer fra egne tidligere bedømte arbejder uden iagttagelse af bestemmelserne i punkt. 1 og 3.

14.2 Sanktioner ved eksamenssnyd og forstyrrende adfærd under prøven

Eksamenssnyd eller forstyrrende adfærd under eksamen/prøve medfører, at den studerende ikke får bedømt sin besvarelse og bliver noteret for et prøveforsøg.
Den studerende kan desuden få en skriftlig advarsel. Under skærpende omstændigheder eller i gentagelsestilfælde kan institutionen endvidere beslutte, at den studerende bliver midlertidigt eller permanent bortvist fra institutionen.

15. Klage over prøver og anke af afgørelser

Klager over prøver behandles efter kapitel 11 i Bekendtgørelse om eksamener og prøver i professions- og erhvervsrettede videregående uddannelser (eksamensbekendtgørelsen).

15.1 Klage over prøver

Klage over studiestartsprøven

Klager over studiestartsprøven kan indgives til uddannelsesinstitutionen, der træffer afgørelse. Klagen skal sendes til uddannelseschefen senest 2 uger (14 kalenderdage) efter, at bedømmelsen er blevet meddelt. Faglige spørgsmål ved institutionens afgørelse kan ikke indbringes for en anden administrativ myndighed. Retlige spørgsmål ved institutionens afgørelse kan indbringes for Uddannelses- og Forskningsstyrelsen jf. afsnit 15.2.

Klage over eksamen i uddannelseselement og delprøve

Den studerende kan indgive en skriftlig klage over retlige og faglige spørgsmål, herunder prøveforløbet, ved en eksamen i et uddannelseselement eller en delprøve.

Klagen skal sendes til uddannelseschefen senest 2 uger (14 kalenderdage) efter, bedømmelsen ved den pågældende prøve er meddelt. Hvis udløbet af fristen falder på en helligdag, er det den første hverdag derefter, som er fristudløbsdagen.

Vedrører klagen faglige spørgsmål anmoder uddannelsesinstitutionen straks bedømmerne, dvs. eksaminator og censor ved den pågældende prøve, om en udtalelse. Udtalelsen fra bedømmerne skal kunne danne grundlag for institutionens afgørelse vedrørende faglige spørgsmål. Institutionen fastsætter normalt en frist på 2 uger for afgivelse af udtalelserne, juli måned indgår dog ikke. Umiddelbart efter at bedømmernes udtalelse foreligger, får klageren lejlighed til at kommentere udtalelserne inden for en frist af normalt en uge.

Afgørelsen træffes af institutionen på grundlag af klagen, bedømmernes faglige udtalelser og klagerens eventuelle kommentarer til udtalelsen.
Afgørelsen skal være skriftlig og begrundet, og kan gå ud på:

1. tilbud om en ny bedømmelse af en skriftlig opgave (ombedømmelse)
2. tilbud om en ny eksamen (omprøve)
3. at den studerende ikke får ikke medhold i klagen
4. en kombination af 1-3, hvis eksamen omfatter en skriftlig opgavebesvarelse med mundtligt forsvar

15.2 Anke af afgørelse

Faglige spørgsmål ved uddannelsesinstitutionens afgørelse jf. afsnit 15.1 kan indbringes for et ankenævn. Den studerende indgiver sin skriftlige klage til institutionen, senest to uger efter den studerende har modtaget institutionens afgørelse.

Ankenævnet består af to beskikkede censorer, der udpeges af censorformanden, en eksaminationsberettiget underviser og en studerende inden for fagområdet, der begge udpeges af uddannelseschefen. Ankenævnet træffer afgørelse på grundlag af det materiale, som lå til grund for institutionens afgørelse og den studerendes klage. Ankenævnet skal have truffet afgørelse senest 2 måneder ved vintereksamen – ved sommereksamen 3 måneder – efter at anken er indgivet.

Ankenævnets afgørelse kan gå ud på:

1. tilbud om ny bedømmelse af en skriftlig opgave (ombedømmelse) ved nye bedømmere,
2. tilbud om ny eksamen (omprøve) ved nye bedømmere,
3. at den studerende ikke får medhold i anken, eller
4. en kombination af 1-3, hvis eksamen omfatter en skriftlig opgavebesvarelse med mundtligt forsvar.

Faglige spørgsmål ved ankenævnets afgørelse kan ikke indbringes for en anden administrativ myndighed.

Retlige spørgsmål ved ankenævnets afgørelse kan indbringes for institutionen, som træffer afgørelse. Klagen skal indgives til institutionen, senest 2 uger efter den studerende har modtaget afgørelsen fra institutionen. Institutionens afgørelse vedr. retlige spørgsmål kan indbringes for Uddannelses- og Forskningsstyrelsen jf. afsnit 15.3.

15.3 Klage over retlige spørgsmål

Uddannelsesinstitutionens endelige afgørelser kan indbringes for Uddannelses- og Forskningsstyrelsen, når klagen vedrører retlige spørgsmål. Klagefristen er to uger fra den dag, afgørelsen er meddelt klageren. Klagen indgives til institutionen, der udarbejder en udtalelse, som klageren skal have lejlighed til at kommentere på inden for en frist af mindst 1 uge. Institutionen sender herefter den samlede sag til behandling i styrelsen.

15.4 Ombedømmelse og omprøve

Går afgørelsen ud på tilbud om ombedømmelse eller omprøve, skal den studerende informeres om, at ombedømmelse eller omprøve kan resultere i lavere karakter.

Den studerende skal, inden for en frist af 2 uger efter at afgørelsen er afgivet, acceptere tilbuddet om ombedømmelse eller omprøve Hvis den studerende ikke accepterer inden for fristen, gennemføres ombedømmelse eller omprøve ikke.

Ombedømmelse eller omprøve skal finde sted snarest muligt. Hvis beviset for uddannelsens færdiggørelse er udstedt, skal det inddrages indtil bedømmelsen foreligger endeligt, hvorefter et nyt bevis udstedes.

Besluttes det, at der skal gives tilbud om en ombedømmelse eller omprøve, udpeger uddannelseschefen nye bedømmere. Censorformanden udpeger evt. censor. De nye bedømmere skal bedømme besvarelsen på baggrund af opgaveteksten og opgaven. De nye bedømmere meddeler institutionen resultatet af ombedømmelsen vedlagt en skriftlig begrundelse.

Faglige spørgsmål ved ombedømmelse eller omprøve kan ikke indbringes for uddannelsesinstitutionen igen eller en anden administrativ myndighed. Retlige spørgsmål kan indbringes for institutionen, der træffer afgørelse.

16. Dispensation

Institutionen kan dispensere fra reglerne i denne institutionsdel af studieordningen, når det findes begrundet i usædvanlige forhold. Institutionerne, der udbyder denne uddannelse, samarbejder om en ensartet dispensationspraksis.

ERHVERVS
AKADEMI
SYDVEST