

# Studie- ordning

## Cybersikkerhed (PBA)

August 2026



---

Rasmus Frimodt, rektor

Zealands studieordninger er opdelt i en national del og en lokal (institutionel) del. Nogle studieordninger suppleres desuden af et valgfagskatalog. Alle dele kan findes nedenfor.

Den lokale del af studieordningen er fastsat af den enkelte uddannelsesinstitution. Den nationale del af studieordningen er vedtaget i uddannelsens uddannelsesnetværk.

Ud over studieordningerne har alle uddannelser et tilknyttet uddannelsesbilag, der er en del af hovedbekendtgørelsen om tekniske og merkantile erhvervsakademiuddannelser og professionsbacheloruddannelser, se [www.retsinfo.dk](http://www.retsinfo.dk).

STUDIEORDNING  
for  
Professionsbachelor i cybersikkerhed

National del

Gældende fra 01.08.2026

## Indhold

|      |                                                       |    |
|------|-------------------------------------------------------|----|
| 1.   | Uddannelsens mål for læringsudbytte .....             | 3  |
| 2.   | Uddannelsen indeholder 11 nationale fagelementer..... | 4  |
| 2.1  | Forretningsforståelse.....                            | 4  |
| 2.2  | Programmering .....                                   | 5  |
| 2.3  | Computerarkitektur.....                               | 6  |
| 2.4  | Kommunikation og rapportering.....                    | 7  |
| 2.5  | Automatisering og scripting .....                     | 8  |
| 2.6  | Datasikkerhed .....                                   | 9  |
| 2.7  | Netværksarkitektur .....                              | 10 |
| 2.8  | Cybersikkerhedsgovernance .....                       | 11 |
| 2.9  | Netværks- og kommunikationssikkerhed.....             | 12 |
| 2.10 | Softwaresikkerhed .....                               | 13 |
| 2.11 | Systemsikkerhed .....                                 | 14 |
| 3.   | Praktik.....                                          | 15 |
| 4.   | Krav til den professionsfaglig bacheloreksamen .....  | 16 |
| 5.   | Regler om merit.....                                  | 17 |
| 6.   | Ikrafttrædelse .....                                  | 17 |
| 6.1  | Overgangsordning.....                                 | 17 |

Denne nationale del af studieordningen for professionsbachelor i Cybersikkerhed er udstedt i henhold til § 23 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, og identificering af samt 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 og forståelse for:

- organisationstyper og deres værdikæder, og hvordan cybersikkerhed påvirker virksomhedens økonomi og forretningsprocesser
- roller og ansvar i en organisation i relation til cybersikkerhed
- centrale begreber inden for risikostyring knyttet til arbejdet med cybersikkerhed i en organisation
- projektmodeller
- 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 særligt med henblik på cybersikkerhed. Herunder datatyper, datastrukturer, teori om fx operatorer, betingelser og kontrol-flow. Et yderligere fokus vil være på funktioner, parametre og inputvalidering. Tillige omhandler fagelementet 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 omhandler 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 datalagringsystemer 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 (Confidentiality, Integrity and Availability), som er et gennemgående sikkerhedsparadigme på hele uddannelsen – men også principper såsom Least Privilege og Defense In Depth. Fagelementet omhandler også kryptografi, herunder 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 konfiguration 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 organisation. 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
- anvende 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 netværkssikkerhedstrusler samt implementere løsninger og konfigurere udstyr til netværks- og kommunikationssikkerhed. Fagelementet omhandler forskelligt sikkerhedsudstyr (IDS) til monitorering.

### **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 beskæftiger sig med udvælgelse, anvendelse og implementering af praktiske mekanismer til at forhindre, detektere og reagere over for specifikke cybersikkerhedsmæssige hændelser. Det omfatter emner som generelle governanceprincipper og sikkerhedsprocedurer, væsentlige efterforskningsprocesser, it-trusler samt sikkerhedsprincipper i systemsikkerhed. Faget omhandler 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 konfiguration.

### **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 logging og monitorering 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 konfigurerings 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 den professionsfaglig bacheloreksamen**

Den professionsfaglige bacheloreksamen dokumenterer sammen med uddannelsens øvrige prøver og praktikprøven, at uddannelsens mål for læringsudbyttet er opnået.

I den professionsfaglige bacheloreksamen skal den studerende dokumentere forståelse af og evne til at reflektere over professionens praksis og anvendelse af teori og metode med henblik på at søge løsning på en praksisnær problemstilling.

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 den professionsfaglig bacheloreksamen**

Den professionsfaglige bacheloreksamen afslutter uddannelsen, når alle forudgående prøver er bestået.

### **ECTS-omfang**

Den professionsfaglige bacheloreksamen har et omfang på 10 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**

Beståede 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 01.08.2026. Studieordningen gælder for alle studerende, der optages på uddannelsen fra ikrafttrædelsesdatoen og efterfølgende.

### **6.1 Overgangsordning**

For allerede indskrevne studerende gælder følgende overgangsordning:

Studerende, som er påbegyndt uddannelsen før ikrafttrædelsesdatoen, følger den nationale del af studieordningen af 1. august 2025 indtil 31. maj 2030, hvorefter de overgår til nærværende studieordning.

# Indhold

|                                                                                     |    |
|-------------------------------------------------------------------------------------|----|
| Indhold.....                                                                        | 1  |
| 1. Studieordningens lovmæssige rammer .....                                         | 2  |
| 2. Optagelse på uddannelsen .....                                                   | 2  |
| 3. Uddannelsens forløb .....                                                        | 2  |
| 4. Lokale fagelementer .....                                                        | 3  |
| 4.1. Cybersikkerhedsdrift.....                                                      | 3  |
| 4.2. Cloud og sikkerhed .....                                                       | 4  |
| 5. Praktik og regler for gennemførelse .....                                        | 5  |
| 6. Undervisnings- og arbejdsformer .....                                            | 6  |
| 6.1. Læsning af tekster på fremmedsprog .....                                       | 6  |
| 7. Internationalisering .....                                                       | 6  |
| 7.1 Uddannelse i udlandet .....                                                     | 6  |
| 7.2 Aftaler med udenlandske uddannelsesinstitutioner om parallellforløb .....       | 6  |
| 8. Eksamener på uddannelsen .....                                                   | 6  |
| 8.1. Beskrivelse af eksamenerne .....                                               | 7  |
| 8.1.1. Studiestartsprøven .....                                                     | 7  |
| 8.1.2. Førsteårsprøven .....                                                        | 7  |
| 8.1.3. Eksamen i Forretningsforståelse .....                                        | 8  |
| 8.1.4. Eksamen i Programmering og Computerarkitektur .....                          | 8  |
| 8.1.5. Eksamen i Kommunikation og rapportering og Netværksarkitektur .....          | 9  |
| 8.1.6. Eksamen i Datasikkerhed og Automatisering og scripting .....                 | 10 |
| 8.1.7. Eksamen i Cybersikkerhedsdrift .....                                         | 11 |
| 8.1.8. Eksamen i Cybersikkerhedsgovernance .....                                    | 12 |
| 8.1.9. Eksamen i Netværks- og kommunikationssikkerhed samt Cloud og sikkerhed ..... | 13 |
| 8.1.10. Eksamen i Softwaresikkerhed .....                                           | 14 |
| 8.1.11 Eksamen i Systemsikkerhed .....                                              | 15 |
| 8.1.12 Praktikeksamen .....                                                         | 15 |
| 8.2. Professionsfaglig bacheloreksamen .....                                        | 16 |
| 8.2.1. Krav til professionsfaglig bacheloreksamen .....                             | 16 |
| 8.2.2. Formulerings- og staveevners betydning for bedømmelsen .....                 | 17 |
| 8.3. Det anvendte sprog ved eksamenerne .....                                       | 17 |
| 8.4. Særlige eksamensvilkår .....                                                   | 17 |
| 8.5. Syge- og reeksamen .....                                                       | 17 |
| 8.5.1. Sygeeksamen .....                                                            | 18 |
| 8.5.2. Reeksamen .....                                                              | 18 |
| 8.6. Eksamenssnyd og forstyrrende adfærd .....                                      | 18 |
| 8.6.1. Processen ved afklaring af eksamenssnyd, herunder plagiering .....           | 19 |
| 8.7. Klager .....                                                                   | 19 |
| 8.7.1. Klage over eksamen .....                                                     | 19 |
| 8.7.2. Anke af afgørelse vedr. bedømmelsen .....                                    | 20 |
| 9. Andre regler for uddannelsen .....                                               | 20 |
| 9.1. Merit .....                                                                    | 20 |
| 9.1.1. Meritaftaler for fagelementer omfattet af studieordningens lokale del .....  | 20 |
| 9.2 Ophør af indskrivning på uddannelsen .....                                      | 20 |
| 9.3. Dispensationsregler .....                                                      | 21 |
| 10. Økonomi .....                                                                   | 21 |
| 11. Ikrafttrædelse og overgangsordninger .....                                      | 21 |

# 1. Studieordningens lovmæssige rammer

For uddannelsen gælder seneste version af følgende love og bekendtgørelser:

- Bekendtgørelse af lov om erhvervsakademier for videregående uddannelser.
- Bekendtgørelse af lov om erhvervsakademiuddannelser og professionsbacheloruddannelser (LEP-loven).
- Bekendtgørelse om tekniske og merkantile erhvervsakademiuddannelser og professionsbacheloruddannelser
- Bekendtgørelse om adgang til erhvervsakademiuddannelser og professionsbacheloruddannelser (adgangsbekendtgørelsen).
- Bekendtgørelse om prøver i erhvervsrettede videregående uddannelser (eksamensbekendtgørelsen).
- Bekendtgørelse om karakterskala og anden bedømmelse ved uddannelser på Uddannelses- og Forskningsministeriets område (karakterbekendtgørelsen).
- Bekendtgørelse om censorkorps og censorvirksomhed på de videregående uddannelser (Censorbekendtgørelsen).

Link til gældende bekendtgørelser: <http://zealand.dk/docs/Studielovgivning.pdf>

De gældende love og bekendtgørelser er også tilgængelige på [www.retsinfo.dk](http://www.retsinfo.dk)

## 2. Optagelse på uddannelsen

Optagelse på uddannelsen sker i henhold til reglerne i bekendtgørelse om adgang til erhvervsakademiuddannelser og professionsbacheloruddannelser.

## 3. Uddannelsens forløb

Uddannelsen, der er en fuldtidsuddannelse, er normeret til 3 ¼ studenterårsværk. Et studenterårsværk er en fuldtidsstuderendes arbejde i 1 år. Et studenterårsværk svarer til 60 point i European Credit Transfer System (ECTS). Uddannelsen er således normeret til i alt 195 ECTS-point.

| Semester | Nationale fagelementer*                 | Lokale fagelementer            | Eksamener**                                |
|----------|-----------------------------------------|--------------------------------|--------------------------------------------|
| 1        |                                         |                                | Studiestartsprøve                          |
|          | Forretningsforståelse (10 ECTS)         |                                | Eksamen i Forretningsforståelse            |
|          | Programmering (10 ECTS)                 |                                | Eksamen i Programmering og                 |
|          | Computerarkitektur (10 ECTS)            |                                | Computerarkitektur                         |
| 2        | Kommunikation og rapportering (10 ECTS) |                                | Eksamen i Kommunikation og rapportering og |
|          | Netværksarkitektur (10 ECTS)            |                                | Netværksarkitektur                         |
|          | Datasikkerhed (5 ECTS)                  |                                | Eksamen i Datasikkerhed og                 |
|          | Automatisering og scripting (5 ECTS)    |                                | Automatisering og Scripting                |
| 3        |                                         | Cybersikkerhedsdrift (10 ECTS) | Eksamen i Cybersikkerhedsdrift             |

|   |                                                |                              |                                                                        |
|---|------------------------------------------------|------------------------------|------------------------------------------------------------------------|
|   |                                                | Valgfag (10 ECTS)            | Valgfagseksamen                                                        |
|   |                                                | Valgfag (10 ECTS)            | Valgfagseksamen                                                        |
| 4 | Cybersikkerhedsgovernance (10 ECTS)            |                              | Eksamen i Cybersikkerhedsgovernance                                    |
|   | Netværks- og kommunikationssikkerhed (10 ECTS) |                              | Eksamen i Netværks- og kommunikationssikkerhed samt Cloud og sikkerhed |
|   |                                                | Cloud og sikkerhed (10 ECTS) |                                                                        |
| 5 | Softwaresikkerhed (10 ECTS)                    |                              | Eksamen i Softwaresikkerhed                                            |
|   | Systemsikkerhed (10 ECTS)                      |                              | Eksamen i Systemsikkerhed                                              |
|   |                                                | Valgfag (10 ECTS)            | Valgfagseksamen                                                        |
| 6 | Praktik (30 ECTS)                              |                              | Praktikeksamen                                                         |
| 7 |                                                | Valgfag (5 ECTS)             | Valgfagseksamen                                                        |
|   | Professionsfaglig bacheloreksamen (10 ECTS)    |                              | Professionsfaglig bacheloreksamen                                      |

\*Beskrivelse af de nationale fagelementer findes i den nationale del af studieordningen. De lokale fagelementer, herunder valgfag, findes i den lokale del af studieordningen (og for nogle uddannelser i et separat valgfagskatalog).

Alle studerende vil blive understøttet i en bevidstgørelse om bæredygtighed og grøn omstilling i relation til uddannelsens faglighed. Tolkningen af specifikke læringsmål vil så vidt muligt ske i denne kontekst, og dermed bidrage til dannelse inden for bæredygtighed og grøn omstilling.

## 4. Lokale fagelementer

De lokale fagelementer er beskrevet nedenfor. For nogle uddannelser er beskrivelsen af valgfag dog samlet i et separat valgfagskatalog. For beskrivelse af praktik, se afsnittet om Praktik og regler for gennemførelse.

### 4.1. Cybersikkerhedsdrift

Indhold:

Fagelementet beskæftiger sig med tekniske og organisatoriske systemer til forebyggelse og håndtering af cybersikkerhedshændelser. Fokus er på det driftsmæssige. I faget indgår emner som backup-strategier, risikoanalyse, analyse af hændelsesdata og logs samt dokumentation af disse. Der vil endvidere indgå disaster recovery planer og risikovurderinger i forhold til aktuelle trusselsbilleder samt håndtering af mindre hændelser i en organisation.

Læringsmål:

*Viden*

Den studerende har:

- viden om systemer til sikkerhedsovervågning og drift, inklusiv best practice indenfor backup strategier
- viden om sikringsprocesser som plan-do-check-act inklusiv risikoanalyse-og håndtering
- viden om patch management
- viden om organisering af roller og systemer
- forståelse for praksis og anvendt teori og metode inden for cybersikkerhedsstandards og kan reflektere over tilknyttede roller.

### *Færdigheder*

Den studerende kan:

- anvende metoder og redskaber til indsamling af data til risikoanalyse
- anvende metoder og redskaber til behandling af logs og events
- vurdere praksisnære og teoretiske problemstillinger samt begrunde og vælge relevante løsningsmodeller inden for analyse og dokumentation af hændelsesdata og logs
- udarbejde og formidle praksisnære og faglige problemstillinger og løsninger vedrørende disaster recovery planer til samarbejdspartnere og brugere

### *Kompetencer*

Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til mindre sikkerhedshændelser ved brug af relevant informationer og værktøjer i en sikringscyklus.
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik ved udvikling af disaster recovery planer og risikovurderinger.
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til nye sikkerhedsstandarder samt udviklingen i trusselsbilledet.

ECTS-omfang:

10 ECTS

## **4.2. Cloud og sikkerhed**

Indhold:

Faget skal give den studerende kompetencer til selvstændigt at opbygge, konfigurere, migrere og drive cloud-løsninger i forskellige koncepter som open source-baserede stacks og kommercielle hyperscale-platformer. Endvidere skal den studerende kunne rådgive om strategiske valg, der balancerer værdiskabelse, afhængighed, sikkerhed og bæredygtighed mod hinanden.

Læringsmål:

### *Viden*

Den studerende har:

- viden om cloud-arkitektur og modeller
- viden om digital suverænitæt, datalokalitet, dataportabilitet, indlåsnings effekter (vendor lock-in) og europæiske strategier som EUCS, EU Cloud Code of Conduct
- viden om drift af cloud-infrastruktur, herunder anskaffelse, konfiguration, monitorering og automatisering
- viden om bæredygtigheden og sikkerheden af cloudløsninger
- viden om migreringsstrategier mellem platforme, herunder migrering mellem cloud platforme, samt exit- og portabilitetshensyn.

### *Færdigheder*

Den studerende kan:

- anvende metoder og værktøjer til hands-on at opsætte, konfigurere og drifte cloud-løsninger
- planlægge og gennemføre en migrering mellem platforme
- monitorere, fejlfinde og sikre en cloud-løsning i drift
- sammenligne bæredygtigheden af forskellige cloudløsninger

### *Kompetencer*

Den studerende kan:

- selvstændigt indgå i fagligt og tværfagligt samarbejde om udvikling, migrering og drift af suveræne og sikre cloud-løsninger

- identificere egne læringsbehov og strukturere egen læring i et teknologi- og reguleringsfelt i hurtig udvikling

ECTS-omfang:  
10 ECTS

## 5. Praktik og regler for gennemførelse

Indhold, overordnede læringsmål og ECTS-omfang for praktikken er beskrevet i den nationale del af studieordningen.

I praktikken arbejder den studerende med fagligt relevante problemstillinger og opnår kendskab til relevante erhvervsfunktioner. Sammenhæng mellem den teoretiske undervisning og praktikken er udgangspunktet for den studerendes mål for praktikken.

Praktikperioden er sidestillet med et fuldtidsjob med de krav til arbejdstid, indsats, engagement og fleksibilitet, som den færdiguddannede må forventes at møde i sit første job.

Praktikforløbet kan tilrettelægges fleksibelt og differentieret og kan danne grundlag for den studerendes professionsfaglige bacheloreksamen

### *Praktikaftale*

Den studerende, Zealand og virksomheden aftaler det konkrete indhold for den studerendes praktikperiode med udgangspunkt i de overordnede læringsmål for praktikken

Praktikaftalen skal indeholde de individuelle mål for praktikken, samt en beskrivelse af den eller de opgaver den studerende skal løse for virksomheden. Dette er efterfølgende retningsgivende for tilrettelæggelse af den studerendes arbejde i praktikperioden.

Praktikaftalen kan desuden indeholde aftale om arbejdstid og rapportering.

### *Virksomheden*

Virksomheden udpeger en kontaktperson i virksomheden.

Virksomheden bidrager med en konkret og realistisk problemstilling/arbejdsopgaver, som ønskes bearbejdet af den studerende.

Virksomheden stiller informationer, der er relevante for løsning af opgaverne, til rådighed for den studerende.

Virksomheden skal løbende vurdere den studerendes aktivitet i praktikperioden, og ved problemer meddele dette til den studerende og vejleder eller praktikkoordinatoren på Zealand.

### *Den studerende*

Den studerende skal selv være opsøgende mht. til at finde virksomheder, der er relevante inden for det aktuelle fagområde.

Den studerende har pligt til at overholde praktikaftalen, da praktikken er en obligatorisk del af uddannelsen.

Hvis den studerende ikke har fundet en praktikplads, bliver den studerende indkaldt til søgedage og andre aktiviteter, der skal bidrage til at finde en praktikplads. Den studerende skal deltage aktivt i disse tilbud. Ved den studerendes manglende deltagelse, uden der foreligger usædvanlige forhold, har Zealand ret til at udskrive den studerende fra uddannelsen.

### *Zealand*

Zealand stiller en vejleder til rådighed, der i begrænset omfang er til rådighed for virksomheden og den studerende.

Zealand gennemfører et besøg i virksomheden under praktikperioden. Foregår praktikken i udlandet kan besøget arrangeres virtuelt. Dette gælder også hvis antallet af praktikforløb eller andre væsentlige årsager gør besøg på alle involverede virksomheder vanskeligt.



For yderligere information om praktikken henvises til studiets praktikkoordinator.

## 6. Undervisnings- og arbejdsformer

Undervisningen gennemføres ved anvendelse af forelæsninger, holdundervisning, dialogundervisning, øvelsesrækker, præsentationer, cases, seminarer, gæstelærere, projekter samt virksomhedsophold.

I undervisningen inddrages den nyeste viden og resultater fra nationale og internationale forsknings-, forsøgs- og udviklingsarbejder fra de discipliner, som knytter sig til erhvervet.

I undervisningen inddrages endvidere erfaringer fra praksis og viden fra centrale tendenser i erhvervet og metoder til at udvikle erhvervet samt udføre kvalitets- og udviklingsarbejde.

Undervisningen på Cybersikkerhedsuddannelsen foregår som en dynamisk, interaktiv proces, hvor hovedvægten lægges på de studerendes aktive deltagelse. Undervisningen tager udgangspunkt i relevant erhvervspraksis og kobler praksis og teori.

### 6.1. Læsning af tekster på fremmedsprog

Dele af uddannelsens undervisningsmateriale kan være på engelsk.

Der kræves ikke yderligere kendskab til fremmedsprog, udover hvad adgangsbekendtgørelsen angiver.

## 7. Internationalisering

### 7.1 Uddannelse i udlandet

Den studerende kan efter uddannelsens godkendelse af en ansøgt forhåndsmerit gennemføre udvalgte uddannelseselementer i udlandet. Studieophold i udlandet kan fortrinsvis finde sted på 3., 5. og 6. semester.

Ved forhåndsgodkendelse af studieophold i udlandet har den studerende pligt til efter endt studieophold at dokumentere det godkendte studieopholds gennemførte uddannelseselementer. Den studerende skal i forbindelse med forhåndsgodkendelsen give samtykke til, at Zealand efter endt studieophold kan indhente de nødvendige oplysninger.

Ved godkendelse af forhåndsmerit anses uddannelseselementet for gennemført, hvis det er bestået efter reglerne om uddannelsen.

### 7.2 Aftaler med udenlandske uddannelsesinstitutioner om parallellforløb

Oplysninger om partnerinstitutioner, internationale praktikophold, meritoverførsel og procedurer offentliggøres løbende af Zealand.

## 8. Eksamener på uddannelsen

Formålet med eksamener i uddannelsens fagelementer er at dokumentere, i hvilken grad den studerende opfylder de faglige mål, der er fastsat af uddannelsen og dens elementer. Alle eksamener skal bestås med mindst karakteren 02. Den studerende har ret til 3 forsøg pr. eksamen, studiestartsprøven undtaget.

Beståede eksamener kan ikke tages om. Det er den studerendes ansvar at sætte sig ind i og overholde Zealands regler for afholdelse af eksamener, se også link til gældende regler:

<https://www.zealand.dk/docs/Eksamensregler.pdf>. Begyndelse på et uddannelseselement, semester mv. er samtidig tilmelding til de tilhørende eksamener. Det er ikke muligt at afmelde eksamenerne. Såfremt den studerende ikke opfylder forudsætningerne for deltagelse i en given eksamen, har den studerende brugt et eksamensforsøg.

For krav til den professionsfaglige bacheloreksamen henvises til afsnit 8.2

### **8.1. Beskrivelse af eksamenerne**

Uddannelsen indeholder en variation af eksamensformer, der afspejler undervisningens indhold og arbejdsformer. På nogle uddannelser kan eksamensformen for et eventuelt 2. eller 3. forsøg variere fra den ordinære eksamen.

#### **8.1.1. Studiestartsprøven**

Studiestartsprøven har til formål at klarlægge, om den studerende reelt er begyndt på uddannelsen. Ifølge bekendtgørelsen om prøver i erhvervsrettede videregående uddannelser skal studiestartsprøven afholdes senest to måneder efter uddannelsens start, og resultatet skal være meddelt den studerende senest 2 uger efter prøvens afholdelse. Er prøven ikke bestået, har den studerende mulighed for at deltage i en omprøve, der afholdes senest tre måneder efter uddannelsens start. Den studerende har to forsøg til at bestå studiestartsprøven. Prøven bedømmes bestået/ikke bestået (intern bedømmelse), og er ikke ECTS-udløsende. Bestås studiestartsprøven ikke, udskrives den studerende (se også afsnit 9.2). Ved efteroptag efter afholdelse af studiestartsprøven, kan den studerende dispenseres fra prøven.

Forudsætninger for deltagelse i prøven:

Ingen forudsætninger. Det er en god ide at tage studiestartskurset på Moodle inden studiestartsprøven.

Prøvens tilrettelæggelse og indhold:

Skriftlig prøve med spørgsmål inden for en række overordnede studierelevante emner. Alle hjælpemidler tilladt. Prøven bliver afholdt som stedprøve, og bliver lagt i den studerendes skema. For de studerende, som er tilmeldt blended learning uddannelser, afholdes prøven virtuelt.

Tidsmæssig placering og evt. omprøve:

Studiestartsprøven afholdes i forbindelse med studiestarten eller i forlængelse af studiestarten.

Bedømmelse og meddelelse af resultat:

Studiestartsprøven bedømmes som bestået/ikke bestået. Bestås prøven ikke i første forsøg er den studerende automatisk tilmeldt omprøve.

Omprøve:

Samme som ordinære prøve.

Klager over studiestartsprøven kan indgives til uddannelsesinstitutionen, der træffer afgørelse. Klagen skal indgives senest 2 uger efter at bedømmelsen er blevet meddelt. Faglige spørgsmål ved institutionens afgørelse kan ikke indbringes for en anden administrativ myndighed. Retlige spørgsmål ved institutionens afgørelse (f.eks. ift. tidsfrist for prøvens afholdelse eller antallet af prøveforsøg) kan indbringes for Uddannelses- og Forskningsstyrelsen. Zealand kan give dispensation hvis der foreligger usædvanlige forhold.

#### **8.1.2. Førsteårsprøven**

Førsteårsprøven udgøres af den eller de eksamener, som den studerende ifølge denne studieordning skal deltage i inden udgangen af det første studieår, se også afsnit 3 om Uddannelsens forløb. Førsteårsprøven skal være bestået inden udgangen af den studerendes 1. studieår efter studiestart, for at den studerende kan fortsætte uddannelsen. Se henvisning til den gældende bekendtgørelse i afsnit 1.

Førsteårsprøven består af følgende eksamener på 1. og 2. semester: Eksamen i Forretningsforståelse, Eksamen i Programmering og Computerarkitektur, Eksamen i Kommunikation og rapportering og Netværksarkitektur og Eksamen i Datasikkerhed og Automatisering og Scripting.

### **8.1.3. Eksamen i Forretningsforståelse**

Forudsætninger for deltagelse i eksamen:

Som del af et fagelement kan der være en eller flere obligatoriske studieaktiviteter, der defineres og beskrives af underviseren. De obligatoriske studieaktiviteter varierer fra fagelement til fagelement og kan bestå i eksempelvis afleveringer, deltagelsespligt, præsentationer eller pointsystem.

De obligatoriske studieaktiviteter skal være opfyldt senest 10 dage før eksamens start, for at den studerende kan indstilles til eksamen. Hvis en studerende ikke opfylder forudsætningerne, kan den studerende ikke gå til eksamen og har brugt et eksamensforsøg.

Eksamens tilrettelæggelse og indhold:

Kombineret skriftlig og mundtlig eksamen med afsæt i en virksomhedscase. Individuel eller gruppeprøve på 2-4 studerende.

Den studerende udarbejder en rapport, hvor de skal identificere og analysere forretningsmæssige problemstillinger og udviklingsmuligheder samt udarbejde begrundede anbefalinger, der understøtter virksomhedens strategiske og operationelle mål.

Den mundtlige eksamen er individuel og har en varighed på 30 minutter inklusive votering.

Formkrav:

Rapporten må maksimalt udgøre 8 normalsider + 3 normalsider pr. ekstra studerende i gruppen.

En normalside er 2.400 tegn inkl. mellemrum og fodnoter. Forside, indholdsfortegnelse, litteraturliste og bilag tæller ikke med i sideomfanget. Bilag er uden for bedømmelse.

Hvis en skriftlig opgavebesvarelse ikke opfylder de fastsatte formkrav i studieordningen, kan bedømmerne afvise opgavebesvarelsen. Hvis opgavebesvarelsen afvises, anvendes et eksamensforsøg.

Bedømmelseskriterier:

Bedømmelseskriterierne for eksamen er læringsmålene for fagelementet Forretningsforståelse.

Der gives individuel karakter efter 7-trinsskalaen, med ekstern bedømmelse og er en helhedsvurdering af det skriftlige og mundtlige del.

Tidsmæssig placering:

Eksamen afvikles ved afslutningen af semesteret.

ECTS-omfang:

10 ECTS

Syge- og reeksamen:

Syge- og reeksamen gennemføres på samme grundlag som den ordinære eksamen. Den studerende kan genanvende den allerede afleverede rapport eller aflevere en revideret rapport efter institutionens nærmere bestemmelser.

### **8.1.4. Eksamen i Programmering og Computerarkitektur**

Forudsætninger for deltagelse i eksamen:

Som del af et fagelement kan der være en eller flere obligatoriske studieaktiviteter, der defineres og beskrives af underviseren. De obligatoriske studieaktiviteter varierer fra fagelement til fagelement og kan bestå i eksempelvis afleveringer, deltagelsespligt, præsentationer eller pointsystem.

De obligatoriske studieaktiviteter skal være opfyldt senest 10 dage før eksamens start, for at den studerende kan indstilles til eksamen. Hvis en studerende ikke opfylder forudsætningerne, kan den studerende ikke gå til eksamen og har brugt et eksamensforsøg.

Eksamens tilrettelæggelse og indhold:

Kombineret skriftlig og mundtlig eksamen. Eksamen gennemføres som en individuel portfolioeksamen bestående af et antal obligatoriske portfolioelementer, som er udarbejdet i løbet af undervisningsforløbet.

Portfolioen skal dokumentere den studerendes arbejde med fagene Programmering og Computerarkitektur. Den samlede portfolio afleveres forud for eksamen og danner grundlag for et individuelt mundtligt forsvar.

Den mundtlige eksamen har en varighed på 30 minutter inklusive votering. Den studerende indleder eksamen med 5 minutter præsentation.

Formkrav:

Formkravene til portfolioelementerne vil blive præsenteret i løbet af undervisningsforløbet.

Bedømmelseskriterier:

Bedømmelseskriterierne for eksamen er læringsmålene for fagelementet Programmering og Computerarkitektur.

Der gives individuel karakter efter 7-trinsskalaen, med intern bedømmelse og er en helhedsvurdering af det skriftlige og mundtlige del.

Tidsmæssig placering:

Eksamen afvikles ved afslutningen af semesteret.

ECTS-omfang:

20 ECTS der udgøres af:

Programmering 10 ECTS

Computerarkitektur 10 ECTS

Syge- og reeksamen:

Syge- og reeksamen gennemføres på samme grundlag som den ordinære eksamen. Den studerende kan genanvende den allerede afleverede portfolio eller aflevere en revideret portfolio efter institutionens nærmere bestemmelser.

### **8.1.5. Eksamen i Kommunikation og rapportering og Netværksarkitektur**

Forudsætninger for deltagelse i eksamen:

Som del af et fagelement kan der være en eller flere obligatoriske studieaktiviteter, der defineres og beskrives af underviseren. De obligatoriske studieaktiviteter varierer fra fagelement til fagelement og kan bestå i eksempelvis afleveringer, deltagelsespligt, præsentationer eller pointsystem.

De obligatoriske studieaktiviteter skal være opfyldt senest 10 dage før eksamens start, for at den studerende kan indstilles til eksamen. Hvis en studerende ikke opfylder forudsætningerne, kan den studerende ikke gå til eksamen og har brugt et eksamensforsøg.

Eksamens tilrettelæggelse og indhold:

Mundtlig eksamen med udgangspunkt i skriftligt produkt. Projekteksamen er baseret på udvikling, dokumentation og demonstration af et Proof of Concept. Eksamen gennemføres på baggrund af projektet, hvor de studerende udvikler et Proof of Concept, der adresserer en relevant problemstilling inden for netværksarkitektur og cybersikkerhed.

Projektet kan udarbejdes individuelt eller i grupper op til 4 studerende.

Eksamen indledes med en fælles præsentation og demonstration på 10 minutter + 5, minutter pr ekstra studerende. Herefter eksamineres de studerende individuelt. Den individuelle eksamination har en varighed på 20 minutter inkl. votering.

#### Formkrav:

Projektet afleveres som en samlet projektrapport med tilhørende dokumentation. Der skal som minimum indgå relevant teknisk dokumentation, netværksdiagrammer, designbeskrivelser, testresultater samt dokumentation af det udviklede Proof of Concept.

Rapporten må maksimalt udgøre 15 normalsider + 5 normalsider pr. ekstra studerende.

En normalside er 2.400 tegn inkl. mellemrum og fodnoter.

Forside, indholdsfortegnelse, litteraturliste og bilag tæller ikke med i sideomfanget. Bilag er uden for bedømmelse.

Hvis en skriftlig opgavebesvarelse ikke opfylder de fastsatte formkrav i studieordningen, kan bedømmerne afvise opgavebesvarelsen. Hvis opgavebesvarelsen afvises, anvendes et eksamensforsøg.

#### Bedømmelseskriterier:

Bedømmelseskriterierne for eksamen er læringsmålene for fagelementerne Netværksarkitektur samt Kommunikation og rapportering. Der foretages en samlet vurdering af det afleverede projekt, demonstrationen og den individuelle mundtlige præstation.

Der gives individuel karakter efter 7-trinsskalaen og med ekstern bedømmelse.

#### Tidsmæssig placering:

Eksamen afvikles ved afslutningen af semesteret.

#### ECTS-omfang:

20 ECTS der udgøres af,

10 ECTS Netværksarkitektur

10 ECTS Kommunikation og rapportering

#### Syge- og reeksamen:

Syge- og reeksamen gennemføres på samme grundlag som den ordinære eksamen. Den studerende kan genanvende den allerede afleverede projekt eller aflevere et revideret projekt efter institutionens nærmere bestemmelser.

### 8.1.6. Eksamen i Datasikkerhed og Automatisering og scripting

#### Forudsætninger for deltagelse i eksamen:

Som del af et fagelement kan der være en eller flere obligatoriske studieaktiviteter, der defineres og beskrives af underviseren. De obligatoriske studieaktiviteter varierer fra fagelement til fagelement og kan bestå i eksempelvis afleveringer, deltagelsespligt, præsentationer eller pointsystem.

De obligatoriske studieaktiviteter skal være opfyldt senest 10 dage før eksamens start, for at den studerende kan indstilles til eksamen. Hvis en studerende ikke opfylder forudsætningerne, kan den studerende ikke gå til eksamen og har brugt et eksamensforsøg.

#### Eksamens tilrettelæggelse og indhold:

Eksamen er en individuel praktisk stedprøve, hvor den studerende med udgangspunkt i en udleveret case skal analysere, udvikle, konfigurere, teste og dokumentere en eller flere automatiseringsløsninger.

Eksamen gennemføres i et kontrolleret eksamensmiljø, hvor den studerende arbejder direkte i relevante operativsystemer og terminalmiljøer.

Eksamen har en varighed på 4 timer.

Alle hjælpemidler er tilladt med undtagelse af generative AI-værktøjer. Anvendelse af generative AI-værktøjer, herunder sprogmodeller og kodegeneratorer, er ikke tilladt under prøven.

Formkrav:

Ved prøvens afslutning afleverer den studerende:

- udviklet kode og eventuelle konfigurationsfiler,
- dokumentation af løsningen,
- en kort redegørelse for designvalg, test og anvendte metoder.

Den samlede besvarelse afleveres elektronisk.

Hvis en skriftlig opgavebesvarelse ikke opfylder de fastsatte formkrav i studieordningen, kan bedømmerne afvise opgavebesvarelsen. Hvis opgavebesvarelsen afvises, anvendes et eksamensforsøg.

Bedømmelseskriterier:

Bedømmelseskriterierne for eksamen er læringsmålene for fagelementerne Datasikkerhed og Automatisering og Scripting. Der foretages en samlet vurdering af den afleverede løsning og dokumentation.

Der gives individuel karakter efter 7-trinsskalaen og med intern bedømmelse.

Tidsmæssig placering:

Eksamen afvikles ved afslutningen af semesteret.

ECTS-omfang:

10 ECTS der udgøres af,

5 ECTS Datasikkerhed

5 ECTS Automatisering og scripting

Syge- og reeksamen:

Syge- og reeksamen gennemføres på samme grundlag som den ordinære eksamen.

### **8.1.7. Eksamen i Cybersikkerhedsdrift**

Forudsætninger for deltagelse i eksamen:

Som del af et fagelement kan der være en eller flere obligatoriske studieaktiviteter, der defineres og beskrives af underviseren. De obligatoriske studieaktiviteter varierer fra fagelement til fagelement og kan bestå i eksempelvis afleveringer, deltagelsespligt, præsentationer eller pointsystem.

De obligatoriske studieaktiviteter skal være opfyldt senest 10 dage før eksamens start, for at den studerende kan indstilles til eksamen. Hvis en studerende ikke opfylder forudsætningerne, kan den studerende ikke gå til eksamen og har brugt et eksamensforsøg.

Eksamens tilrettelæggelse og indhold:

Mundtlig eksamen baseret på skriftligt produkt. Den skriftlige aflevering udarbejdes individuelt eller i grupper på op til 4 studerende. Eksamens mundtlige del er individuel og varer i alt 30 min. inkl. votering.

Formkrav:

Det skriftlige produkt må max være 5 normalsider + 3 normalsider pr ekstra studerende i gruppen.

Forside, indholdsfortegnelse, litteraturliste og bilag tæller ikke med i sideomfanget. Bilag er uden for bedømmelse.

Hvis en skriftlig opgavebesvarelse ikke opfylder de fastsatte formkrav i studieordningen, kan bedømmerne afvise opgavebesvarelsen. Hvis opgavebesvarelsen afvises, anvendes et eksamensforsøg.

Bedømmelseskriterier:

Eksamen bedømmes internt. Der gives individuel karakter efter 7-trinsskalaen og bedømmelsen er en helhedsvurdering af den skriftlige og mundtlige del.

Alle hjælpemidler er tilladt

Tidsmæssig placering:

Eksamen afvikles på 3.semester

ECTS-omfang:

10 ECTS

Syge- og reeksamen:

Syge- og reeksamen gennemføres på samme grundlag som den ordinære eksamen. Den studerende kan genanvende det allerede afleverede skriftlige produkt eller aflevere et revideret skriftligt produkt efter institutionens nærmere bestemmelser.

### **8.1.8. Eksamen i Cybersikkerhedsgovernance**

Forudsætninger for deltagelse i eksamen:

Som del af et fagelement kan der være en eller flere obligatoriske studieaktiviteter, der defineres og beskrives af underviseren. De obligatoriske studieaktiviteter varierer fra fagelement til fagelement og kan bestå i eksempelvis afleveringer, deltagelsespligt, præsentationer eller pointsystem.

De obligatoriske studieaktiviteter skal være opfyldt senest 10 dage før eksamens start, for at den studerende kan indstilles til eksamen. Hvis en studerende ikke opfylder forudsætningerne, kan den studerende ikke gå til eksamen og har brugt et eksamensforsøg.

Eksamens tilrettelæggelse og indhold:

Eksamen er en mundtlig eksamen på baggrund af et skriftligt projekt. Projektet tager udgangspunkt i en virksomhed eller organisation og skal behandle en eller flere problemstillinger inden for cybersikkerhedsgovernance.

Der skal være 2-5 studerende i en gruppe. Studieleder kan i særlige tilfælde dispensere fra dette.

Eksamen indledes med en fælles præsentation. Der afsættes op til 5 minutter pr. studerende, dog maksimalt 20 minutter.

Herefter eksamineres gruppens medlemmer individuelt. Den individuelle eksamination har en varighed på 20 minutter inklusive votering.

Formkrav:

Det skriftlige projekt må maksimalt udgøre 10 normalsider + 5 normalsider pr. ekstra studerende. En normalside er 2.400 tegn inklusive mellemrum og fodnoter. Forside, indholdsfortegnelse, litteraturliste og bilag tæller ikke med i sideomfanget. Bilag er uden for bedømmelse.

Hvis en skriftlig opgavebesvarelse ikke opfylder de fastsatte formkrav i studieordningen, kan bedømmerne afvise opgavebesvarelsen. Hvis opgavebesvarelsen afvises, anvendes et eksamensforsøg.

Bedømmelseskriterier:

Bedømmelseskriterierne for eksamen er læringsmålene for fagelementet Cybersikkerhedsgovernance.

Der foretages en samlet vurdering af det skriftlige produkt og den individuelle mundtlige præstation. Eksamen bedømmes efter 7-trinsskalaen og med ekstern bedømmelse.

Tidsmæssig placering:

Eksamen afvikles ved afslutningen af semesteret.

ECTS-omfang:

10 ECTS.

Syge- og reeksamen:

Syge- og reeksamen gennemføres på samme grundlag som den ordinære eksamen. Den studerende kan genanvende det allerede afleverede projekt eller aflevere et revideret projekt efter institutionens nærmere bestemmelser.

### **8.1.9. Eksamen i Netværks- og kommunikationssikkerhed samt Cloud og sikkerhed**

Forudsætninger for deltagelse i eksamen:

Som del af et fagelement kan der være en eller flere obligatoriske studieaktiviteter, der defineres og beskrives af underviseren. De obligatoriske studieaktiviteter varierer fra fagelement til fagelement og kan bestå i eksempelvis afleveringer, deltagelsespligt, præsentationer eller pointsystem.

De obligatoriske studieaktiviteter skal være opfyldt senest 10 dage før eksamens start, for at den studerende kan indstilles til eksamen. Hvis en studerende ikke opfylder forudsætningerne, kan den studerende ikke gå til eksamen og har brugt et eksamensforsøg.

Eksamens tilrettelæggelse og indhold:

Portfolioeksamen med mundtligt forsvar. Eksamen gennemføres som en individuel portfolioeksamen bestående af et antal obligatoriske portfolioelementer udarbejdet i løbet af undervisningsforløbet.

Den samlede portfolio afleveres forud for eksamen og danner grundlag for et individuelt mundtligt forsvar. Den mundtlige eksamen har en varighed på 30 minutter inklusive votering.

Formkrav:

Portfolioen afleveres elektronisk og skal bestå af dokumentation for de obligatoriske portfolioelementer. Portfolioen skal dokumentere den studerendes arbejde med fagets læringsmål inden for netværks- og kommunikationssikkerhed, samt Cloud og sikkerhed. Portfolioen skal indeholde dokumentation for relevante aktiviteter, analyser, konfigurationer, test, monitoreringer, sikkerhedsvurderinger og øvrige produkter udarbejdet i forbindelse med fagenes aktiviteter.

Hvis en skriftlig opgavebesvarelse ikke opfylder de fastsatte formkrav i studieordningen, kan bedømmerne afvise opgavebesvarelsen. Hvis opgavebesvarelsen afvises, anvendes et eksamensforsøg.

Bedømmelseskriterier:

Bedømmelseskriterierne for eksamen er læringsmålene for fagelementerne Netværks- og kommunikationssikkerhed samt Cloud og sikkerhed.

Der foretages en samlet vurdering af portfolioen og den mundtlige præstation.

Eksamen bedømmes efter 7-trinsskalaen og med ekstern bedømmelse.

Tidsmæssig placering:

Eksamen afvikles ved afslutningen af semesteret.



ECTS-omfang:

20 ECTS der udgøres af:

10 ECTS Netværks- og kommunikationssikkerhed

10 ECTS Cloud og sikkerhed

Syge- og reeksamen:

Syge- og reeksamen gennemføres på samme grundlag som den ordinære eksamen. Den studerende kan genanvende den allerede afleverede portfolio eller aflevere en revideret portfolio efter institutionens nærmere bestemmelser.

### **8.1.10. Eksamen i Softwaresikkerhed**

Forudsætninger for deltagelse i eksamen:

Som del af et fagelement kan der være en eller flere obligatoriske studieaktiviteter, der defineres og beskrives af underviseren. De obligatoriske studieaktiviteter varierer fra fagelement til fagelement og kan bestå i eksempelvis afleveringer, deltagelsespligt, præsentationer eller pointsystem.

De obligatoriske studieaktiviteter skal være opfyldt senest 10 dage før eksamens start, for at den studerende kan indstilles til eksamen. Hvis en studerende ikke opfylder forudsætningerne, kan den studerende ikke gå til eksamen og har brugt et eksamensforsøg.

Eksamens tilrettelæggelse og indhold:

Portfolioeksamen med mundtligt forsvar.

Den samlede portfolio afleveres forud for eksamen og danner grundlag for et individuelt mundtligt forsvar.

Den mundtlige eksamen har en varighed på 30 minutter inklusive votering.

Formkrav:

Portfolioen består af et antal obligatoriske portfolioelementer udarbejdet i løbet af undervisningsforløbet.

Portfolioen skal dokumentere den studerendes arbejde med fagets læringsmål inden for softwaresikkerhed, herunder sikker programmering, programkvalitet, sikkerhedsdesign og vurdering af sårbarheder i software.

Hvis en skriftlig opgavebesvarelse ikke opfylder de fastsatte formkrav i studieordningen, kan bedømmerne afvise opgavebesvarelsen. Hvis opgavebesvarelsen afvises, anvendes et eksamensforsøg.

Bedømmelseskriterier:

Bedømmelseskriterierne for eksamen er læringsmålene for fagelementet Softwaresikkerhed.

Der foretages en samlet vurdering af portfolioen og den mundtlige præstation.

Eksamen bedømmes efter 7-trinsskalaen og med intern bedømmelse.

Tidsmæssig placering:

Eksamen afvikles ved afslutningen af semesteret.

ECTS-omfang:

10 ECTS.

Syge- og reeksamen:

Syge- og reeksamen gennemføres på samme grundlag som den ordinære eksamen. Den studerende kan genanvende den allerede afleverede portfolio eller aflevere en revideret portfolio efter institutionens nærmere bestemmelser.

### **8.1.11 Eksamen i Systemsikkerhed**

Forudsætninger for deltagelse i eksamen:

Som del af fagelementet kan der være en eller flere obligatoriske studieaktiviteter, der defineres og beskrives af faglæreren. De obligatoriske studieaktiviteter skal være opfyldt senest 10 dage før eksamens start, for at den studerende kan indstilles til eksamen. Hvis en studerende ikke opfylder forudsætningerne, kan den studerende ikke gå til eksamen og har brugt et eksamensforsøg.

Eksamens tilrettelæggelse og indhold:

Kombineret skriftlig og mundtlig prøve.

Projektet kan udarbejdes individuelt eller i grupper med max 5 personer pr gruppe.

Eksamen indledes med en demonstration af den udviklede løsning. Ved gruppeprojekter afsættes op til 10 minutter pr. studerende, dog maksimalt 25 minutter. Efter demonstrationen gennemføres individuel eksamination. Til den individuelle eksamination afsættes 20 minutter pr. eksaminand inklusiv votering.

Formkrav:

Der afleveres et oplæg på maksimalt én side i punktform. Oplægget skal indeholde de emner og problemstillinger, som den studerende forventer at præsentere og inddrage ved den mundtlige eksamen. Det er muligt at justere eller supplere emnerne ved den mundtlige eksamen.

De nærmere krav til oplæggets indhold og udformning præsenteres af underviseren.

Hvis en skriftlig opgavebesvarelse ikke opfylder de fastsatte formkrav i studieordningen, kan bedømmerne afvise opgavebesvarelsen. Hvis opgavebesvarelsen afvises, anvendes et eksamensforsøg.

Bedømmelseskriterier:

Bedømmelseskriterierne for eksamen er læringsmålene for fagelementet Systemsikkerhed.

Der foretages en samlet vurdering af projektrapporten, demonstrationen og den individuelle mundtlige præstation.

Eksamen bedømmes efter 7-trinsskalaen og med intern bedømmelse.

Tidsmæssig placering:

Eksamen afvikles ved afslutningen af semesteret.

ECTS-omfang:

10 ECTS.

Syge- og reeksamen:

Syge- og reeksamen gennemføres på samme grundlag som den ordinære eksamen. Den studerende kan genanvende den allerede afleverede skriftlige produkt eller aflevere en revideret skriftligt produkt efter institutionens nærmere bestemmelser.

### **8.1.12 Praktikeksamen**

Forudsætninger for deltagelse i eksamen:

For at kunne indstilles til praktikprøven skal den studerende have deltaget i sit praktikforløb i overensstemmelse med de rammer og opgaver, som angives i den studerende praktikpladsaftale, som er en aftale mellem praktikvirksomheden, den studerende og Zealand.

Manglende opfyldelse af forudsætninger betyder, at den studerende ikke kan deltage i eksamen, og der er brugt et eksamensforsøg.

Eksamens tilrettelæggelse og indhold:

Skriftlig eksamen. Alle hjælpemidler er tilladt.

Skriftlig individuel praktikrapport. Krav til indhold beskrives i manual, som fremgår af institutionens kommunikationsplatform.

Formkrav:

Fremgår af manualen for praktik.

Hvis en skriftlig opgavebesvarelse ikke opfylder formalia (fastsat i Studieordningen eller manualen), kan bedømmerne afvise opgavebesvarelsen. Hvis opgavebesvarelsen afvises, skal der ikke gives en bedømmelse, og den studerende har brugt et eksamensforsøg.

Bedømmelseskriterier:

Læringsmålene for praktikken danner grundlag for bedømmelsen. Eksamen bedømmes internt efter 7-trinsskalen.

Tidsmæssig placering:

Afslutningen af 6. semester

ECTS-omfang:

30 ECTS

## **8.2. Professionsfaglig bacheloreksamen**

Overordnede krav til den professionsfaglige bacheloreksamen er beskrevet i den nationale del af studieordningen. Yderligere krav er præciseret nedenfor.

Den studerende har ret til at udarbejde en afsluttende skriftlig opgavebesvarelse individuelt og aflægge individuelt mundtligt forsvar.

### **8.2.1. Krav til professionsfaglig bacheloreksamen**

Forudsætninger for deltagelse i eksamen:

Den professionsfaglige bacheloreksamen afslutter uddannelsen. Deltagelse forudsætter, at alle øvrige eksamener på uddannelsen er bestået.

Eksamens tilrettelæggelse og indhold:

Mundtlig eksamen med udgangspunkt i et skriftligt produkt.

For at dokumentere den professionsfaglige bacheloreksamen skal den studerende udarbejde en skriftlig projektrapport. Den skriftlige del af den professionsfaglige bacheloreksamen skal udarbejdes individuelt eller i grupper af op til 3 studerende.

Projektet skal omhandle en central problemstilling indenfor cybersikkerhed, og det skal fortrinsvist gennemføres i samarbejde med en virksomhed eller organisation.

Den studerende vil få tildelt en eller flere vejledere for bachelorprojektet. En vejleder skal godkende bachelorprojektets emne og/eller problemformulering på forhånd for at sikre, at den studerende ikke arbejder forgæves.

Den professionsfaglige bacheloreksamen forsvares ved en individuel mundtlig eksamination, som har en varighed af 40 minutter for hver studerende, inkl. votering og præsentation. Eksamen indledes med en præsentation på 10 minutter.

Formkrav:

Projektrapportens maksimale omfang er: maks. 30 normalsider + 10 normalsider pr studerende.

En normalside er 2.400 tegn inkl. mellemrum og fodnoter. Forside, indholdsfortegnelse, litteraturliste samt bilag tæller ikke med heri. Bilag er uden for bedømmelse.

Ved gruppearbejde skal det skal være tydeligt, hvem har skrevet hvad i projektrapporten.

Hvis en skriftlig opgavebesvarelse ikke opfylder formalia (fastsat i Studieordningen), kan bedømmerne afvise opgavebesvarelsen. Hvis opgavebesvarelsen afvises, skal der ikke gives en bedømmelse, og den studerende har brugt et eksamensforsøg.

Bedømmelseskriterier:

Bedømmelseskriterierne tager udgangspunkt i læringsmålene for den afsluttende professionsfaglige bacheloreksamen. Eksamen er med ekstern censur og der gives en samlet karakter, baseret på en helhedsvurdering af det skriftlige projekt og det mundtlige forsvar.

Tidsmæssig placering:

7. semester

ECTS-omfang:

10 ECTS

Syge- og reeksamen:

Reeksamen svarer til ordinær eksamensform. Den studerende har mulighed for at redigere det skriftlige projekt, hvis reeksamen skyldes at tidligere forsøg ikke er bestået.

### **8.2.2. Formulerings- og staveevners betydning for bedømmelsen**

Stave- og formuleringssevne indgår i den professionsfaglige bacheloreksamen. Bedømmelsen er udtryk for en helhedsvurdering af det faglige indhold samt stave- og formuleringssevnen, dog vægtes det faglige indhold tungest.

Studerende, der kan dokumentere en relevant specifik funktionsnedsættelse, kan søge om dispensation fra kravet om, at stave- og formuleringssevne indgår i bedømmelsen. Ansøgningen indsendes til studievejledningen på mail: [studievejledning@zealand.dk](mailto:studievejledning@zealand.dk) senest seks uger før eksamens afvikling.

### **8.3. Det anvendte sprog ved eksamenerne**

Eksamenerne aflægges på dansk medmindre andet er nævnt i beskrivelsen af de enkelte eksamener.

Eksamenerne kan aflægges på svensk eller norsk i stedet for dansk. I uddannelser eller enkeltfag, der udbydes på engelsk eller et andet fremmedsprog, kan eksamenerne aflægges på dette sprog.

Studerende med andet modersmål end dansk kan søge om dispensation fra kravet om, at stave- og formuleringssevne indgår i bedømmelsen af den afsluttende professionsfaglige bacheloreksamen, samt de eksamener, hvor det af denne studieordning fremgår, at de nævnte evner indgår i den professionsfaglige bacheloreksamen. Ansøgningen indsendes via [www.zealand.dk/for-studerende/blanketter/](http://www.zealand.dk/for-studerende/blanketter/) senest seks uger før eksamens afvikling.

### **8.4. Særlige eksamensvilkår**

Studerende kan, hvor det er begrundet i fysisk eller psykisk funktionsnedsættelse, søge om særlige eksamensvilkår og tilladelse til at medbringe andre hjælpemidler. Ansøgningen indsendes til studievejledningen på mail: [studievejledning@zealand.dk](mailto:studievejledning@zealand.dk) senest seks uger før eksamens afvikling. 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.

### **8.5. Syge- og reeksamen**

Der gælder særlige regler om syge- og reeksamen for studiestartsprøven, se afsnit 8.1.1.

### 8.5.1. Sygeeksamen

En studerende, der har været forhindret i at gennemføre en eksamen på grund af dokumenteret sygdom (eller anden dokumentation af usædvanlige forhold), kan få mulighed for at aflægge (syge)eksamen snarest muligt. Er det en eksamen, der er placeret i uddannelsens sidste eksamenstermin, får den studerende mulighed for at aflægge (syge)eksamen i samme eksamenstermin eller i umiddelbar forlængelse heraf. Godkendes den studerendes dokumenterede fravær til den pågældende eksamen, vil den studerende automatisk blive tilmeldt (syge)eksamen.

Orientering om tid og sted for (syge)eksamen findes på Wiseflow. Sygdom skal dokumenteres ved lægeerklæring (evt. omkostninger til fremskaffelse af dokumentation dækkes af den studerende). I Zealands eksamensregler er det muligt at læse mere om krav for dokumentation ved sygdom, se <https://www.zealand.dk/docs/Eksamensregler.pdf>. Zealand skal senest have modtaget lægeerklæring 8 dage efter eksamens afholdelse. Studerende, der bliver akut syge under en eksamens afvikling, skal dokumentere at vedkommende har været syg på den pågældende dag. Dokumenteres sygdom ikke efter ovenstående regler, har den studerende brugt et eksamensforsøg. Lægeerklæring skal sende via blanket på hjemmesiden: [www.zealand.dk/for-studerende/blanketter/](http://www.zealand.dk/for-studerende/blanketter/).

### 8.5.2. Reeksamen

Ved ikke bestået eksamen, vil den studerende automatisk blive tilmeldt reeksamen, så længe der resterer eksamensforsøg. Reeksamen afholdes snarest muligt og så vidt muligt senest når den pågældende eksamen igen afholdes. Den studerende skal selv orientere sig om, hvornår reeksamen afholdes. Orientering om tid og sted for reeksamen findes på Wiseflow. Zealand kan dispensere fra den fortsatte tilmelding, når det er begrundet i usædvanlige forhold, herunder dokumenteret handicap.

### 8.6. Eksamenssnyd og forstyrrende adfærd

Eksamensafholdelse på Zealand behandles efter reglerne i bekendtgørelse om eksamener og prøver ved professions- og erhvervsrettede videregående uddannelser ([Eksamensbekendtgørelsen](#)).

Under eksamen skal den studerende optræde hensynsfuldt, herunder efterleve de anvisninger, som gives af eksamenstilsynet, eksaminator og censor. Eksamenssnyd foreligger bl.a. når den studerende

- Plagierer, herunder genbruger egen tekst (selvplagiering uden kildehenvisning og citationstegn)
- Forfalsker
- Fortier eller vildleder om egen indsats eller resultater
- Indgår i ikke-tilladt samarbejde
- Modtager eller forsøger at modtage hjælp under eksamen, eller hjælper andre, når der ikke er tale om en gruppeeksamen
- Benytter ikke-tilladte hjælpemidler
- Uretmæssigt har opnået forudgående kendskab til eksamensopgaven
- Afgiver urigtige fremmødeoplysninger
- Forsøger at omgå, de-aktivere eller på anden måde hindre hensigten med uddannelsesinstitutionens anvendelse af elektroniske overvågningsprogrammer

Eksamenssnyd, herunder plagiering, medfører, at den studerende ikke får bedømt sin besvarelse og bliver noteret for et brugt eksamensforsøg.

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.

Læs mere om eksamensregler på [Moodle](#).

### 8.6.1. Processen ved afklaring af eksamenssnyd, herunder plagiering

Det indberettes til studieadministration og studieleder hvis der under eller efter en eksamen opstår formodning om, at en eksaminand:

- uretmæssigt har skaffet sig eller ydet hjælp,
- har udgivet en andens arbejde for sit eget (plagiat), eller
- har anvendt eget tidligere bedømt arbejde eller dele heraf uden henvisning (plagiat).

#### *Udsættelse af eksamen*

Vedrører indberetningen eksamenssnyd som plagiering i en skriftlig opgave, som er bedømmelsesgrundlag ved en senere mundtlig eksamen udsætter studielederen eksamen, hvis det ikke er muligt at afklare forholdet inden den fastsatte eksamensdato.

#### *Indberetningens form og indhold*

Indberetningen skal ske uden unødigt forsinkelse. Med indberetningen skal følge en skriftlig fremstilling af sagen, der omfatter oplysninger, der kan identificere de indberettede personer, samt en kort redegørelse og den foreliggende dokumentation for forholdet. Er der tale om gentagelsestilfælde for én eller flere af de indberettede personer, skal dette oplyses.

Ved indberetning af plagiering skal de plagierede dele markeres med tydelig henvisning til de kilder, der er plagieret fra. Den plagierede tekst skal ligeledes markeres i kildeteksten.

#### *Inddragelse af eksaminanden - partshøring*

Partshøringen er altid skriftlig, og indebærer fremsendelse af dokumentationen for formodningen af eksamenssnyd med henblik på at anmode om den studerendes skriftlige opfattelse.

### 8.7. Klager

Klager over eksamener på Zealand samt evt. anke behandles efter reglerne i bekendtgørelse om eksamener og prøver ved professions- og erhvervsrettede videregående uddannelser ([Eksamensbekendtgørelsen](#)).

Læs mere om klager på [Moodle](#).

#### 8.7.1. Klage over eksamen

Den studerende har mulighed for at klage over forhold vedrørende en eksamen. Klagen kan vedrøre både retlige og faglige spørgsmål herunder:

1. Eksaminationsgrundlaget, herunder eksamensspørgsmål, opgaver og lignende, samt dets forhold til uddannelsens mål og krav
2. Eksamensforløbet
3. Bedømmelsen

Zealand skal have modtaget den studerendes klage senest to uger efter at karakteren er offentliggjort. Zealand kan ved usædvanlige forhold dispensere fra fristen.

Klagen skal være skriftlig og begrundet og skal indgives til Zealand via [klager@zealand.dk](mailto:klager@zealand.dk).

Hvis den studerende får medhold i klagen, vil der blive tilbudt en ny bedømmelse (ved skriftlige eksamener) eller en reeksamen (ved mundtlige eksamener). Tilbuddet om ny bedømmelse eller reeksamen kan resultere i en lavere karakter.

Klage over retlige spørgsmål (fx inhabilitet, høring, klagevejledning, om eksamensbekendtgørelsen er fortolket korrekt m.v.) kan indbringes for Uddannelses- og Forskningsstyrelsen. Klagen indgives til Zealand via [klager@zealand.dk](mailto:klager@zealand.dk). Zealand afgiver en udtalelse, som den studerende skal have lejlighed til at

kommentere inden for en frist på normalt en uge. Zealand sender klagen, udtalelsen og den studerendes eventuelle kommentarer til Uddannelses- og Forskningsstyrelsen. Klagefristen til Zealand er 2 uger fra den dag, afgørelsen er meddelt klageren, jf. eksamensbekendtgørelsen kap. 11.

#### **8.7.2. Anke af afgørelse vedr. bedømmelsen**

Hvis den studerende modtager afslag på en klage, kan afgørelsen ankes. Afgørelsen bringes for et ankenævn. Ankenævnets virksomhed er omfattet af forvaltningsloven, herunder om inhabilitet og tavshedspligt.

Anken indsendes til Zealand via [klager@zealand.dk](mailto:klager@zealand.dk). Fristen for at anke er to uger efter den studerende er gjort bekendt med afgørelsen. De samme krav som nævnt under klage (skriftlighed, begrundelse osv.) gælder også ved anke. Ankenævnet består af to beskikkede censorer, der udpeges af censorformanden, en eksamensberettiget underviser og en studerende inden for fagområdet (uddannelsen), som begge udpeges af Zealand.

## **9. Andre regler for uddannelsen**

### **9.1. Merit**

Meritaftaler for de nationale fagelementer er angivet i den nationale del af studieordningen.

#### **9.1.1. Meritaftaler for fagelementer omfattet af studieordningens lokale del**

Beståede uddannelseselementer ækvivalerer de tilsvarende uddannelseselementer ved andre uddannelsesinstitutioner, som udbyder denne uddannelse såvel som ved andre uddannelser.

Der søges om merit, hvis den studerende mener at have meritgivende uddannelseselementer.

### **9.2 Ophør af indskrivning på uddannelsen**

I eksamensbekendtgørelsen (se afsnit 1) beskrives, hvornår en studerende kan udskrives fra uddannelsen, herunder ved ikke-bestået studiestartsprøve/førsteårsprøve og opbrugte eksamensforsøg. Supplerende regler gældende ved Zealand er præciseret nedenfor.

Indskrivningen kan bringes til ophør for studerende, der ikke har bestået nogen eksamener i en sammenhængende periode på 1 år. Dette gælder dog ikke for studerende i lønnet praktik. Perioder, hvor den studerende ikke har deltaget i eksamener på grund af orlov, barsel, adoption eller værnepligt, medtælles ikke. Den studerende skal på forlangende fremskaffe dokumentation for disse forhold. Uddannelsen kan dispensere fra disse bestemmelser, hvis der foreligger usædvanlige forhold. Dispensationsansøgningen indsendes til Zealand via [www.zealand.dk/for-studerende/blanketter/](http://www.zealand.dk/for-studerende/blanketter/). Indskrivningen kan desuden bringes til ophør for studerende, der ikke kommer rettidigt i praktik, såfremt betingelserne i afsnit 5 er opfyldt.

Den studerende modtager en skriftlig henvendelse (varsling) fra Zealand før indskrivningen bringes til ophør. I den forbindelse gøres den studerende opmærksom på reglerne ovenfor. Det vil desuden fremgå af brevet, at den studerende har 2 uger til at indsende bemærkninger og dokumentation for perioder med orlov, barsel, adoption eller værnepligt, og der vil være oplyst en frist for ansøgning om eventuel dispensation. Ved ikke-bestået studiestartsprøve sker udskrivning dog direkte efter varsling.

Hvis den studerende ikke har reageret inden for den fastsatte frist, udskrives vedkommende. Hvis den studerende anmoder om, at indskrivningen ikke bringes til ophør, har anmodningen opsættende virkning, indtil sagen er afgjort af studielederen.

Den studerende kan klage til Zealand over den trufne afgørelse senest 2 uger efter modtagelsen af afgørelsen. Klagen indgives til Zealand via [www.zealand.dk/for-studerende/](http://www.zealand.dk/for-studerende/), og klagen har ikke opsættende virkning.

Hvis afgørelsen fastholdes afgiver Zealand en udtalelse, som klageren skal have mulighed for at kommentere inden for en frist på normalt en uge. Zealand sender klagen, udtalelsen og klagerens eventuelle kommentarer til Uddannelses- og Forskningsstyrelsen. Styrelsen meddeler den studerende den endelige afgørelse efter behandling af klagen. Styrelsens afgørelse kan ikke indbringes for en højere administrativ myndighed.

### **9.3. Dispensationsregler**

Zealand kan dispensere fra reglerne i den fælles del af studieordningen, der alene er fastsat af institutionerne, når det findes begrundet i usædvanlige forhold. Institutionerne samarbejder om en ensartet dispensationspraksis.

Zealand kan fravige, hvad institutionen eller institutionerne selv har fastsat i studieordningen, hvis det er begrundet i usædvanlige forhold.

## **10. Økonomi**

Alle aktiviteter, der påføres den studerende, skal betragtes som egenbetaling, medmindre andet er påført.

## **11. Ikrafttrædelse og overgangsordninger**

Denne lokale institutionsdel af studieordningen træder i kraft august 2026, med virkning for studerende indskrevet på uddannelsen efter 01.08.2026 og frem til næstkommende studieordning.

Studerende som er optaget før 01.08.2026 følger den studieordning, de er optaget på eller efterfølgende overflyttet til.

I tilfælde af orlov kan det være nødvendigt at overføre den studerende til gældende studieordning.