Informationssikkerhedspolitik for Erhvervsakademi København

EK's informationssikkerhedspolitik er godkendt af EK's direktion 18.august 2025.

Denne politik danner den overordnede ramme for informationssikkerhed på EK.

For at bevare tilliden til EK skal kritiske informationer beskyttes med foranstaltninger, der sikrer den nødvendige informationssikkerhed. Vi arbejder ud fra tre grundsten:

- **Fortrolighed**: Kun personer med et legitimt behov må have adgang til informationer.
- **Integritet**: Informationer skal være konsistente og i en form, som man kan stole på.
- **Tilgængelighed**: Informationer skal være tilgængelige for de rette personer, når der er behov for det.

Alle som har en relation til EK, kan i informationssikkerhedspolitikken orientere sig om, hvilke principper der gælder for informationssikkerhed. Principperne afspejler krav fra lovgivning og relevante myndigheder, f.eks. Uddannelses- og Forskningsministeriet og fra den fælles informationssikkerhedsstandard for myndigheder, ISO 27001.

1.1 Informationssikkerhedspolitikkens anvendelsesområde

Informationssikkerhedspolitikken omfatter alle EK's informationsaktiver, dvs.:

- Enhver information, der tilhører EK.
- Informationer, som EK kan gøres ansvarlig for.
- Midler til at anvende, frembringe eller opbevare de informationer, der er omtalt i de forrige punkter.
- De forrige punkter gælder uanset formen af information herunder også mundtlig information.

Eksempler på informationsaktiver er:

- Informationer om ansatte og studerende.
- Informationer om finansielle forhold.
- Informationer, som bidrager til administrationen af EK.
- Informationer som er overladt til EK af andre.
- Labs, computere og computernetværk.
- Forsøgs- og forskningsdata.

Informationssikkerhedspolitikken gælder for:

- Alle ansatte uden undtagelse - dermed også personer, som arbejder midlertidigt for EK samt censorer og eksterne vejledere.
- Studerende, der i forbindelse med deres studie anvender, frembringer eller opbevarer EK's informationsaktiver.
- Andre, der anvender, frembringer eller opbevarer EK's informationsaktiver. f.eks. alumner, leverandører, konsulenter, håndværkere og gæster.

EK's ledelse har bestemt, at:

- EK's ledelse løbende skal holdes informeret om det aktuelle risikobillede for informationssikkerhed.
- EK's ledelse har ansvaret for, at EK's ISMS (ledelsessystem for informationssikkerhed) løbende tilpasses og forbedres, så det modsvarer det aktuelle trusselsbillede, som EK møder.
- EK's informationssikkerhedsansvarlige anbefaler målsætninger og rammer for informationssikkerhed, som informationssikkerhedsudvalget (ISU) og EK's ledelse godkender.
- EK's informationssikkerhedsansvarlige koordinerer arbejdet med informationssikkerhed med databeskyttelsesrådgiveren (DPO) samt andre relevante interessenter. Når det er nødvendigt, indhenter EK's informationssikkerhedsansvarlige godkendelse fra EK's ledelse.

- Risici mod informationssikkerheden på EK skal imødegås med passende beskyttelsesforanstaltninger. Foranstaltningerne skal begrundes i en risikovurdering, EK's risikotolerance og forretningsmæssige risici. Ved involvering af personoplysninger skal der desuden udføres en risikovurdering for de registrerede.
- EK ønsker at have en høj grad af åbenhed over for ansatte og studerende, der færdes på EK, både fysisk og digitalt, og i forhold til en række tætte samarbejdsrelationer med fx forskere, undervisere og virksomheder fra hele verden. Dette kræver på den ene side systemer, der er åbne for en bred kreds af brugere, men på den anden side også mulighed for ekstra beskyttelse af udvalgte data og systemer. Så vidt det er muligt inden for rammerne og ikke påvirker sikkerheden, skal EK's strategiske mål omkring samarbejde med erhvervslivet og mulighed for at afprøve ny teknologi altid prioriteres. Ønsket om åbenhed må ikke kompromittere ønsket om sikkerhed.
- Risikovurderinger skal opdateres årligt og ved betydelige ændringer i det generelle trusselsbillede eller i EK's organisering, strategi eller operationelle miljø.
- Foranstaltninger indrettes på en sådan måde, at EK overholder såvel kontraktuelle krav som lovkrav, herunder *Databeskyttelsesforordningen (GDPR)* og den danske databeskyttelseslov.
- Informationssikkerhedspolitikken udmøntes i en række retningslinjer, vejledninger og adfærdsregler inden for informationssikkerhed.
- Følgende sikkerhedsprincipper skal efterleves:
    - adgang til informationsaktiver skal gives efter behov.
    - sikkerhed skal designes ind i processer og løsninger.
    - nødvendig funktionsadskillelse skal indføres.

1.2 Ansvar og sikkerhedsbevidsthed

Følgende ansvar gør sig gældende ift. at beskytte EK's informationsaktiver:

- EK's ledelse har det overordnede ansvar for informationssikkerheden på EK.
- EK's ledelse er ansvarlig for, at medarbejdere og studerende bliver oplyst om deres ansvar i forhold til informationssikkerhed på EK.

1.3 Brud på informationssikkerheden, dispensationer og overtrædelse

Hvis en medarbejder eller studerende opdager trusler mod eller brud på informationssikkerheden, skal vedkommende orientere IT-afdelingen via de i organisationen udmeldte kanaler.
Dispensation fra at følge informationssikkerhedspolitikken kan undtagelsesvis gives af ved at sende en dispensationsanmodning til EK's informationssikkerhedsansvarlige på servicedesk@ek.dk, som udarbejder og fremlægger indstilling til Informationssikkerhedsudvalget.

Overtrædelse af informationssikkerhedspolitikken håndteres som en sikkerhedshændelse og sanktioneres hvis relevant med modsvarende foranstaltninger jf. ordensregler og ansættelsesretlige regler.

ERHVERVSAKADEMI KØBENHAVN

DOKUMENTOPLYSNINGER

Dokument navn	Informationssikkerhedspolitik for Erhvervsakademi København
Ejer	Rektor
Status	Godkendt
Version	3.0
Dato	20. august 2025

Dokumentversion:

Version	Dato	Forfatter	Godkender	Ændringer/bemærkninger
1.0	18.marts 2025	CRIB/JABE/MABR	LOKE/JEBE	
2.0	14.maj 2025	CRIB/JABE/MABR	Fælles ISU-/Sikkerhedsgruppe	
3.0	20. august 2025	CRIB/JABE/MABR/LOKE	Direktion	