Aarhus Universitets informationssikkerhedspolitik

Denne politik danner den overordnede ramme for informationssikkerhed på Aarhus Universitet med udgangspunkt i universitetets overordnede strategi 2025:

> *Aarhus Universitet er et stærkt universitet, der markerer sig med forskning, forskningsbaserede uddannelser og myndighedsrådgivning af høj international kvalitet og værdiskabende samarbejde med private virksomheder, offentlige institutioner og civilsamfundet. Den nysgerrige skabelse af viden med rod i dybe fagligheder til gavn for samfundet er universitetets eksistensberettigelse.*

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

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

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

1.1 Informationssikkerhedspolitikkens anvendelsesområde

Informationssikkerhedspolitikken omfatter alle Aarhus Universitets informationsaktiver, dvs.:

1. enhver information, der tilhører Aarhus Universitet.
2. informationer, som Aarhus Universitet kan gøres ansvarlig for.
3. midler til at anvende, frembringe eller opbevare de informationer, der er beskrevet i punkt 1 og 2.
   Det gælder uagtet formen af information herunder også mundtlig information.

Aarhus Universitet
Nordre Ringgade 1
8000 Aarhus C

Tlf.: +45 8715 0000
E-mail: informationssikkerhed@au.dk
Web: informationssikkerhed.au.dk

Eksempler på informationsaktiver er:

- forsøgs- og forskningsdata.
- informationer om ansatte.
- informationer om finansielle forhold.
- informationer, som bidrager til administrationen af Aarhus Universitet.
- informationer som er overladt til Aarhus Universitet af andre.
- laboratorier, forskningsudstyr, computere og computernetværk.

Informationssikkerhedspolitikken gælder for:

- alle ansatte uden undtagelse - dermed også personer, som arbejder midlertidigt for Aarhus Universitet samt emeriti, censorer og eksterne vejledere.
- studerende, der i forbindelse med deres studie anvender, frembringer eller opbevarer Aarhus Universitets informationsaktiver.
- andre, der anvender, frembringer eller opbevarer Aarhus Universitets informationsaktiver. f.eks. alumner, leverandører, konsulenter, håndværkere og gæster.

Universitetsledelsen har bestemt, at:

- universitetsledelsen løbende skal holdes informeret om det aktuelle risikobillede for informationssikkerhed.
- universitetsledelsen har ansvaret for, at Aarhus Universitets ledelsessystem for informationssikkerhed løbende tilpasses og forbedres, så det modsvarer det trusselsbillede, som universitetet møder.
- Informationssikkerhedsafdelingen anbefaler målsætninger og rammer for informationssikkerhed, som det centrale sikkerhedsudvalg (CISU) og universitetsledelsen godkender.
- Informationssikkerhedsafdelingen koordinerer arbejdet med informationssikkerhed med databeskyttelsesrådgiveren (DPO), informationssikkerhedsudvalgene på fakulteterne (FISU) og i Enhedsadministrationen (EISU) samt andre relevante interessenter. Hvis det er nødvendigt, indhenter Informationssikkerhedsafdelingen godkendelse fra CISU og universitetsledelsen.

- risici mod informationssikkerheden på Aarhus Universitet skal imødegås med passende beskyttelsesforanstaltninger. Foranstaltningerne skal begrundes i en risikovurdering, universitetets risikoappetit og forretningsmæssige risici. Ved persondata skal der desuden udføres en risikovurdering for de registrerede.
- risikovurderinger skal opdateres årligt og ved betydelige ændringer i det generelle trusselsbillede eller i universitetets organisering, strategi eller operationelle miljø.
- foranstaltninger indrettes, så Aarhus Universitet overholder kontraktuelle krav samt lovkrav – f.eks. GDPR og universitetsloven.
- 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 Aarhus Universitets informationsaktiver:

- Universitetsledelsen har det overordnede ansvar for informationssikkerheden på Aarhus Universitet.
- Universitetsledelsen er ansvarlig for, at medarbejdere og studerende bliver oplyst om deres ansvar i forhold til informationssikkerhed på Aarhus Universitet.

1.3 Brud på informationssikkerheden, dispensationer og overtrædelse

Hvis en medarbejder eller studerende opdager trusler mod eller brud på informationssikkerheden, skal vedkommende orientere Informationssikkerhedsafdelingen.

Dispensation fra at følge informationssikkerhedspolitikken kan undtagelsesvis gives af ved at sende en dispensationsindstilling til Informationssikkerhedsafdelingen, der vil fremlægge indstillingen for CISU.

Overtrædelse af informationssikkerhedspolitikken håndteres som en sikkerhedshændelse og sanktioneres med modsvarende foranstaltninger.

1.4 Godkendelse

Aarhus Universitets informationssikkerhedspolitik godkendes af rektor på baggrund af CISU's anbefalinger.

Som et led i den overordnede sikkerhedsstyring tager universitetsledelsen, med udgangspunkt i den løbende ledelsesrapportering af risikobilledet, informationssikkerhedspolitikken op til revurdering minimum en gang om året.

Dato: 11. februar 2021

Rektor:

Brian Bech Nielsen