Ledelsessystem for informationssikkerhed (ISMS)

Aarhus Universitets ledelsessystem for informationssikkerhed

1. Indledning

Informationssikkerheden har stor betydning for Aarhus Universitets omdømme, troværdighed og funktionsdygtighed.

For Aarhus Universitet er informationer og informationsaktiver nødvendige og livsvigtige, og de skal derfor beskyttes samt håndteres korrekt for at sikre, at vores fælles hverdag fungerer samt at værdifulde data ikke går tabt, forsvinder eller falder i hænderne på forkerte personer eller organisationer, hvor data vil kunne misbruges.

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 informations-sikkerheds-standard, ISO 27001. (uddrag fra informationssikkerhedspolitikken)

Vejen til opfyldelse af den overordnede informationssikkerhedspolitik er beskrevet i indeværende dokument samt visualiseret i et 'Årshjul' (under udarbejdelse), der beskriver vejen og ansvar for forskellige roller i deres arbejde med informationssikkerhed.

Arbejdet med informationssikkerhed kan inddeles i 5 modenhedsniveauer alt efter organisationens virke og kultur, risikovillighed og hvilke informationer, man har ansvaret for. ISMS'et kan bruges til at opnå modenhedsniveau 3 (Defineret), hvilket vil sige:

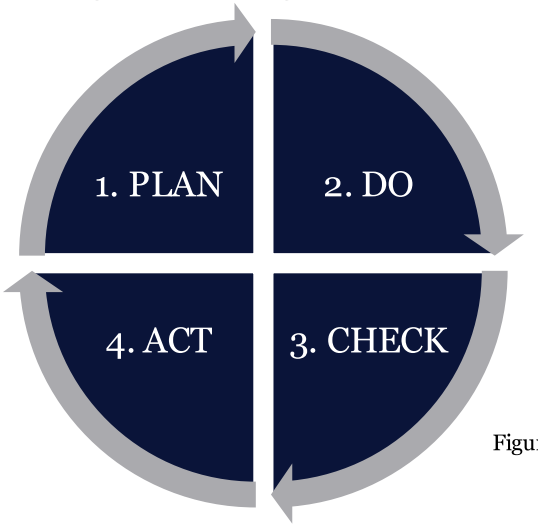
"Procedurer er standardiseret, dokumenterede og kommunikerede gennem træning. Det er bekendtgjort, at procedurerne skal overholdes, men det er usandsynligt, at afvigelser vil blive opdaget.
Procedurerne er typisk en formalisering af eksisterende praksis."

1.1 Definition på ledelsessystem for informationssikkerhed

Informationssikkerhedsarbejdet systematiseres på Aarhus Universitet gennem et ledelsessystem for informationssikkerhed (ISMS), der definerer, dokumenterer og driver aktiviteter for at sikre, at organisationen på fornuftig vis beskytter informationer og informationsaktiver mod trusler og sårbarheder.

Dette centrale ISMS angiver minimum for, hvilke aktiviteter der skal arbejdes med i de lokale ledelsessystemer, og hvem der er ansvarlig for at etablere og anvende ledelsessystemerne lokalt.

At sikre informationssikkerheden på Aarhus Universitet er kontinuerligt med løbende forbedringstiltag ud fra tankerne bag PDCA-cirklen (The Deming Cycle). PDCA, står for PLAN-DO-CHECK-ACT og dækker over følgende:



Figur 1 – PDCA-cirklen

1. I PLAN udarbejdes og vedligeholdes de grundlæggende dokumenter for arbejdet med informationssikkerhed.
2. I DO er implementering og driften af disse i praksis.
3. I CHECK evalueres og dokumenteres status på aktiviteter og informationssikkerhedstiltag samt identificeres forbedringsmulighed.
4. I ACT igangsættes tiltag og forbedringer.

2. Formål

Formålet med et ISMS på Aarhus Universitet er at beskrive, hvordan kravene til informationssikkerhed skal efterleves, og hvordan ledelsen på universitetet og især den enkelte enhed og bruger har en væsentlig rolle i beskyttelse af Aarhus Universitets informationsaktiver. ISMS på Aarhus Universitet har fokus på at sikre, at alle bidrager til, at kritiske og følsomme informationer og informationsaktiver bevarer deres:

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.

3. Organisering

På Aarhus Universitet bygger arbejdet med informationssikkerhed på kravene i ISO27001 (fælles international ledelsesstandard for informationssikkerhed), hvor rammerne består af følgende:

- Informationssikkerhedspolitikken
- Centralt ISMS
- Underliggende politikker for informationssikkerhed
- Skabeloner og vejledning for lokale procedurer

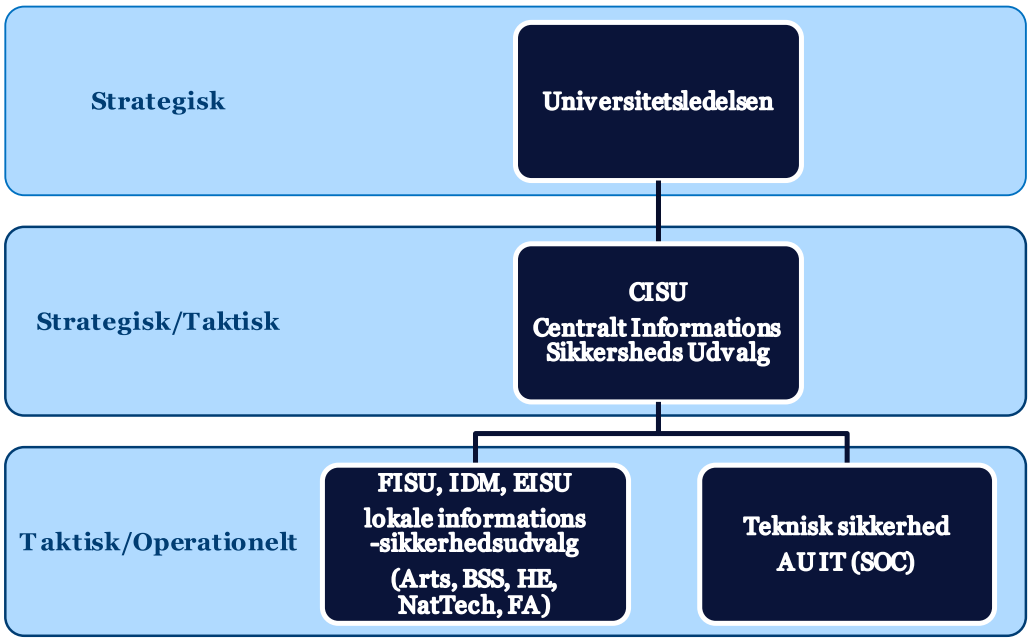
Informationssikkerhedspolitik: Aarhus Universitets informationssikkerhedspolitik angiver, at universitets centrale ISMS løbende skal tilpasses og forbedres, så det modsvarer det trusselsbillede, som universitetet møder.

Ledelsessystem (ISMS): Arbejdet med informationssikkerhed er et ledelsesansvar, der styres gennem det centrale ISMS på Aarhus Universitet og gælder for hele universitetet, dækker samtlige brugere af data, informationer og informationsaktiver tilhørende universitetet.

Politikker og procedurer: En forudsætning for, at arbejdet med informationssikkerhed skal virke, er, at informationssikkerhedsaktiviteter integreres i den nuværende organisation med hensyntagen til eksisterende arbejdsgange, organisering og ansvarsfordeling.

For at leve op til informationssikkerhedspolitikken skal alle aktiviteter i ISMS gennemføres mindst én gang årligt.

Ifølge Aarhus Universitets informationssikkerhedspolitik udarbejder og anbefaler Informationssikkerhedsafdelingen de overordnede målsætninger og tiltag for informationssikkerhed, som det centrale informationssikkerhedsudvalg (CISU) og universitetsledelsen godkender.



Figur 2 - Organisering af informationssikkerhedsudvalgene

Universitetsledelsen: Det centrale ISMS er forankret hos universitetsledelsen, der

- løbende skal holdes informeret om det aktuelle risikobillede for informationssikkerhed i alle enheder.
- har ansvaret for, at Aarhus Universitets centrale ISMS løbende tilpasses og forbedres, så det modsvarer det trusselsbillede, som universitetet møder.
- er ansvarlig for, at alle enheder og brugere bliver oplyst om deres ansvar i forhold til informationssikkerhed på Aarhus Universitet.

Universitetsledelsen kan i forlængelse heraf uddelegere mandat og opgaver, så kravene til informationssikkerhed implementeres lokalt og fungerer i praksis.

Informationssikkerhedschef: Det overordnede operationelle ansvar for den daglige styring og koordinering af informationssikkerhedsindsatsen på hele Aarhus Universitet er placeret hos Informationssikkerhedschefen i AU IT, herunder

- vedligeholdelse af det centrale ISMS og dokumentation.
- opfølgning, på vegne af universitetsledelsen, på aktiviteter, standarder, retningslinjer, kontroller og foranstaltninger vedhørende informationssikkerhed samt at disse gennemføres og efterleves.

Enhedsleder: Enhedslederen har det samlede ansvar for informationssikkerheden i sin respektive enhed, hvor aktiviteter omfatter

- lokalt arbejde med awareness, som skal udføres hele året.
- at sikre, at alle brugere i den respektive enhed har fået den rette information, træning mv.
- at informationssikkerhedspolitikken, ISMS og de underliggende politikker, procedurer, adfærdsregler og alle øvrige centrale informationer omhandlende informationssikkerhed kommunikeres, implementeres og efterleves af alle brugere uden undtagelse i den pågældende enhed.
- at udarbejde og anvende et tilpasset lokalt ISMS, der efterleves i praksis og på et modenhedsniveau 3.
- at udarbejde og implementere lokale politikker og procedurer.

Aarhus Universitets centrale ISMS angiver minimum for de lokale ledelsessystemer, som enhedslederne skal etablere og benytte.

For en mere udførlig beskrivelse af aktiviteter og vejen til modenhedsniveau 3 lokalt henvises til 'Årshjul' (under udarbejdelse) på informationssikkerhed.au.dk.

4. 'PLAN' - planlægning (ISO27001-reference: sektion 4, 5, 6 og 7)

PLAN-fasen dækker over nedenstående aktiviteter, hvor enhedslederen har ansvaret for:

- at beskrive enhedens sammenhæng/virkemåde, herunder at fastlægge interessenter og deres krav til informationssikkerheden.
- at etablere et lokalt ISMS, med udgangspunkt i dette centrale ISMS, der som minimum efterlever kravene i ISO27001.
- at der udvises lederskab og engagement, fastlægges politikker, og sikres at ISMS opnår de tilsigtede resultater samt delegerer og kommunikerer roller, beføjelser og ansvar i forbindelse hermed.
- at anvende Aarhus Universitets risikostyringsproces for risikovurderinger, herunder systemklassifikation.
- at udarbejde liste/dokument, på baggrund af begrundende til- og fravalg baseret på risikovurderingen, for opfølgning af kontroller på sikkerhedstiltag (også kaldet SoA dokument).
- at planlægge beredskabsaktiviteter.
- at udarbejde og godkende plan for håndtering af informationssikkerhedsrisici.
- at fastlægge målsætninger for informationssikkerhed for enheden med fokus på fortrolighed, integritet og tilgængelighed.
- at de nødvendige ressourcer, kompetencer og bevidsthed er til stede samt kommunikation og dokumenteret information.

5. 'DO' - drift (ISO27001-reference: sektion 8)

I denne efterfølgende implementeringsfase (DO-fasen) skal enhedslederen sikre:

- at planlægge, etablere, implementere, drifte og efterleve det lokale ISMS samt de politikker, procedurer mv., der er behov for.
- at implementere planer for at opfylde målsætningerne for informationssikkerhed.
- at opbevare dokumenteret information i det omfang, det er nødvendigt, for at kunne have tillid til, at aktiviteter med relevans for informationssikkerheden er udført som planlagt.
- at planlagte ændringer med potentiel betydning for informationssikkerheden styres, at konsekvenserne af utilsigtede ændringer gennemgås, og at der foretages handlinger for at afbøde eventuelle negative virkninger af ændringer, hvor det er nødvendigt.
- at eventuelle outsourcede processer og underleverancer med relevans for informationssikkerheden fastlægges og styres.
- at der gennemføres lokale vurderinger af informationssikkerhedsrisici med planlagte mellemrum (mindst en gang om året), eller når væsentlige ændringer finder sted, herunder at disse aggregeret formidles til universitetsledelsen via informationssikkerhedsudvalgene.
- at der er implementeret planer og handlinger for håndtering af informationssikkerhedsrisici, og at disse formidles til universitetsledelsen via informationssikkerhedsudvalgene.
- at de løbende lokale awareness aktiviteter gennemføres, så alle relevante er informeret om deres opgaver og ansvar.
- at implementere tiltagene fra risikohåndteringsplanen (såvel tekniske som organisatoriske), at reagere på sikkerhedshændelser med planlagte mellemrum samt at genbesøge risikoprocessen.

6. 'CHECK' - evaluering (ISO27001-reference: sektion 9)

Enhedslederen er ansvarlig for, at informationssikkerhedstiltagene løbende evalueres (i CHECK-fasen), herunder:

- at det er fastlagt, hvad der lokalt skal overvåges og måles for at verificere, at informationssikkerhedstiltagene virker.
- at metoder til overvågning, måling, analyse og evaluering kan give valide resultater.
- at fastsætte hvornår den lokale overvågning og måling skal udføres og af hvem, herunder test af beredskabsplaner.
- at resultaterne fra overvågningen og målingen analyseres og evalueres.
- at der lokalt opbevares hensigtsmæssig, dokumenteret information som bevis for resultaterne.
- at der lokalt udføres interne audits med planlagte mellemrum for at informere om, hvorvidt der i enheden leves op til Aarhus Universitets krav til informationssikkerhed.
- at sikre overvågning, måling, analyse og evaluering på, at ISMS og tiltagene omkring informationssikkerhed virker efter hensigten.
- at sikre intern audit samt eventuel ekstern revision.

- at gennemgå ISMS med planlagt mellemrum for at sikre, at det virker efter hensigten, herunder resultater af overvågning og måling, og audits resultater.
- at gennemgangen skal omfatte beslutninger vedrørende løbende forbedringsmuligheder og behov for ændringer i ISMS.
- at opbevare dokumenteret information som bevis for gennemgang.
- at der rapporteres til universitetsledelsen (via informationssikkerhedsudvalgene), så universitetsledelsen kan forsikre sig om, at ovenstående fungerer tilfredsstillende i de lokale enheder.

7. 'ACT' - forbedring (ISO27001 -reference: sektion 10)

Under ACT-fasen har enhedslederen fokus på tiltag og forbedringer (identificeret i tidligere fase), som sikres gennem:

- at konkrete lokale sikkerhedshændelser styres, og at der reageres på disse.
- at der evalueres på sådanne hændelser og der, hvor nødvendigt, indføres korrigerende handlinger i henhold til konsekvensen, så der efter en lokal vurdering forebygges gentagelser.
- at der foretages lokal opfølgning på, at ovenstående virker i praksis.
- at lokale forbedringsforslag implementeres lokalt, og forslag til forbedringer af nærværende centrale ISMS drøftes og eskaleres efter behov gennem CISU til universitetsledelsen.
- at hvis/når der opstår en afvigelse, foretager enhedslederen handlinger for at styre og korrigere den, forholder sig til konsekvenserne samt fjerner årsagen til afvigelsen, således det ikke opstår igen (gælder både ISMS og konkrete informationssikkerhedstiltag).
- at opbevare dokumenteret information som bevis for arten af afvigelser, eventuelle efterfølgende foretagne handlinger og resultaterne af en eventuel korrigerende handling.
- at gennemføre løbende forbedringer i ISMS, for at sikre dets fortsatte egnethed, samt at det virker efter hensigten.

8. Ordliste:

A.5 - A.18	Forkortelse for de afsnit og generelle krav til politikker der er i ISO27001 anneks A.
Awareness	Bevidsthed/At være bevidst om… Her handler det om gennem forskellige tiltag at skabe bevidsthed om informationssikkerhed, så vi alle aktivt er med til at beskytte informationer tilhørende Aarhus Universitet.
Bruger	Betegnelsen 'Bruger' dækker bredt og gælder alle, der kan påvirke informationssikkerheden på Aarhus Universitet. Det værende fastansatte, studerende, forskere samt andre interne eller eksterne (konsulenter/leverandører/samarbejdspartnere/mv.), som i en kort eller længere periode anvender informationer og/eller informationsaktiver tilhørende Aarhus Universitet.
Enhedsleder	I informationssikkerhed benyttes benævnelsen/rollen til at dække over personer med ansvar for et område eller en afdeling med adgang til informationer tilhørende Aarhus Universitet, fx Institutleder, Vicedirektør.
FISU, IDM og EISU-udvalg	FISU: Fakulteternes lokale informationssikkerhedsudvalg. IDM: Nat og Tech Fakulteternes lokale informationssikkerhedsudvalg. EISU: Enhedsadministrationens (Fællesadministrationens - FA) lokale informationssikkerhedsudvalg.
Fortrolighed	Indenfor informationssikkerhed betyder Fortrolighed, at kun personer med et legitimt behov må have adgang til informationer.
Informationer	Fælles betegnelse for informationer uanset form (mundtlig, skriftlig, elektronisk) som tilhører Aarhus Universitet.
Informationsaktiv	Ordet 'Informationsaktiv' dækker over ethvert "medie", som kan indeholde og/eller transportere informationer, såsom dokumenter, en skrevet note, en mobiltelefon, en bærbar, USB mv.
Integritet	Indenfor informationssikkerhed betyder Integritet, at informationer skal være konsistente og i en form, som man kan stole på.
ISMS	ISMS står for 'Information Security Management System', på dansk 'Ledelsessystem for informationssikker-

	hed' og dækker over, hvordan man som organisation definerer, administrerer og implementerer forskellige foranstaltninger for at sikre, at man på fornuftig vis beskytter Fortroligheden, Integriteten og Tilgængeligheden af sine informationer og aktiver mod trusler og sårbarheder.
ISO27001	International standard der fastsætter god skik for, hvordan man organiserer og styrer informationssikkerhed.
Modenhedsniveau	Modenhedsniveau er et udtryk for organisationens styring af informationssikkerhed, altså hvorvidt organisationen har et veludbygget kontrolmiljø med en høj grad af automatiserede sikringstiltag, er i opbygningen heraf med mange manuelle foranstaltninger eller ligger et sted midt imellem. Indenfor informationssikkerhed arbejdes med 5 niveauer med 5 som det højeste.
SoA	(Statement of Applicability) Dokument som angiver hvilke kontroller en organisation har besluttet sig for, at der skal følges op på i relation til kravene i ISO27001 annekserne A.5 til A.18.
SOC	Security Operation Center
Tilgængelighed	Indenfor informationssikkerhed betyder Tilgængelighed, at informationer skal være tilgængelige for de rette personer, når der er behov for det.

9. Dokument revision:

Version:	Dato:	Udarbejdet/ ændret af:	Ændring:	Dato godkendelse:	Godkendt af:	Gyldig til:
V0.2	21.10.2021	Sinna Bygballe	Tilrettet efter gennemgang			
V0.3	25.10.2021	Ændret af Steen Ilsø	Kommentarer til dokumentet			
V0.4	25.10.2021	Sinna Bygballe	Tilrettet efter indkomne kommentarer			
V0.5	26.10.2021	Sinna Bygballe	Tilrettet efter indkomne kommentarer			