Indhold

1 Informationssikkerhedspolitik

Dette dokument fastlægger Københavns Universitets generelle politik for informationssikkerhed.

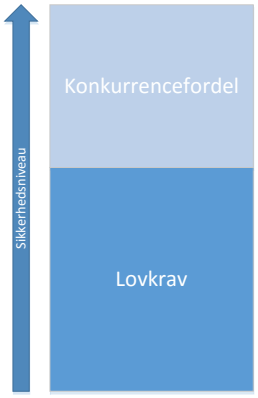
Politikken er gældende for hele KU, både som myndighed, arbejdsgiver og forskningsinstitution.

1.1 Hvorfor vil vi sikre vores informationer?

Først og fremmest bør vi udvise basal respekt for vores egne medarbejdere og andre personer der har betroet deres personoplysninger til KU, enten direkte eller indirekte. Den tillid må vi ikke misbruge.

Dernæst har det en række konsekvenser for KU hvis informationer misbruges, forvanskes eller mistes, og det er en vurdering af disse konsekvenser der danner grundlag for hvor stærk beskyttelse af informationerne vi ønsker.

Grundlæggende skal KU leve op til gældende lovgivning. Det betyder at der er en række sikkerhedskrav der bliver pålagt KU udefra. Dette er den nedre grænse for hvor stærk vores sikkerhed må være.



Men hvis vi ønsker at KU skal opretholde sin status og funktion som internationalt anerkendt universitet og attraktiv samarbejdspartner, så må vi også anerkende at informationssikkerhed i stigende grad er en forudsætning for at tiltrække samarbejdspartnere og forskningsmidler, og for at få adgang til de eksterne informationer vi baserer vores forskning på.

Samtidig har vi på KU store mængder af informationer som vi baserer nuværende og fremtidig forskning på; forskning der besværliggøres, umuliggøres eller ikke kan eftervises hvis informationerne går tabt eller mister troværdighed.

1.2 Hvad dækker begrebet "informationer"?

Umiddelbart forbinder man ofte ordet "informationer" med digitale data. Men dette er kun en del af billedet – vi har også en lang række informationer der er forbundet med fysiske objekter. Eksempler herpå er:

- Unika som eksempelvis museumseksemplarer
- Biologisk materiale; biobanker, herbarier og levende organismer
- Dokumentsamlinger
- Is-borekerner og andre geologiske specialsamlinger
- Lyd-, film- og billedmateriale, eventuelt med følsomt indhold

For at kunne sikre informationer i KU's varetægt, har vi udstukket en række principper for informationssikkerhed, som det forventes at alle med tilknytning til KU efterlever.

2 Principper

Disse grundlæggende principper for informationssikkerhed skal efterleves af alle:

2.1 Styret af KU's strategiske behov

Ejerskab af politik og retningslinjer

KU's Ledelse har defineret behovet for informationssikkerhed; det vi herefter vil kalde det ønskede sikkerhedsniveau.

På baggrund heraf har Direktionen vedtaget denne informationssikkerhedspolitik og tilhørende retningslinjer, som vedligeholdes af Informationssikkerhedschefen og udleves af alle på KU.

KU's behov

Det er KU's behov, herunder efterlevelse af gældende lovgivning og beskyttelse mod aktuelle risici, der fastlægger sikkerhedsniveauet på KU. Formålet er at sikre KU's evne til at opretholde sin status og funktion som internationalt anerkendt universitet og attraktiv samarbejdspartner i forhold til et ledelsesmæssigt accepteret risikoniveau.

Dataklassifikation

Alle KU's informationer har værdi i varierende grad. Ved at klassificere informationerne kan vi synliggøre deres værdi på en systematisk måde, så vi kan beskytte dem i nødvendig og tilstrækkelig grad på et ensartet grundlag.

Risikostyring og –vurdering

KU's informationssikkerhed er baseret på risikovurderinger af konkrete systemer, projekter, kontroller og sårbarheder.

Informationshåndtering og –behandling foretages i høj grad decentralt, og løbende risikovurderinger er derfor en nødvendig forudsætning for at opretholde et samlet billede af informationssikkerheden.

2.2 Implementering af sikkerhedstiltag

Sikkerhedsmiljø

Sikkerhedsmiljøet er fællesbetegnelsen for alle de tiltag der beskytter KU's informationer. Det er dermed alle de tekniske og organisatoriske sikkerhedstiltag, både centralt og decentralt, der sammen skal sikre at sikkerhedsniveauet er opretholdt.

Fordi KU er en levende organisation hvis arbejdsgange og behov konstant ændres, er det vigtigt løbende at vurdere risici så sikkerhedsmiljøet kan justeres.

2.3 Afvigelser dokumenteres

Kompenserende foranstaltninger

Hvis der opstår et behov for informationsbehandling, som ikke i tilstrækkelig grad kan beskyttes af det eksisterende sikkerhedsmiljø, medfører det en øget risiko. Denne risiko skal mindskes gennem yderligere tiltag, som vi kalder kompenserende foranstaltninger.

Fastholdelse af KU's behov for sikkerhed

Afvigelser fra sikkerhedsmiljøet kan godkendes, forudsat at KU's behov for sikkerhed opfyldes dels ved kompenserende foranstaltninger, og dels ved ledelsesmæssig accept af den resterende risiko.

Dispensationer

En dispensation dokumenterer, at en specifik afvigelse fra sikkerhedsmiljøet er accepteret og godkendt. Dispensationer gives på baggrund af risikovurderinger, og kan stille krav om kompenserende foranstaltninger. Dispensationer er altid midlertidige.

Omgåelse af sikkerhedsmiljø

Bevidst eller ubevidst tilsidesættelse af sikkerhedsmiljøet håndteres som sikkerhedshændelser, uanset intentionerne. Hændelserne dokumenteres, og der skal løbende rapporteres og følges op, så KU's behov for sikkerhed opretholdes.

2.4 Fælles ansvar

Alle på KU har et ansvar

Det forudsættes at alle på KU agerer professionelt og udviser sund fornuft. Vi bestræber os på KU for at skabe et sikkerhedsmiljø der er transparent og giver os alle mulighed for at agere forsvarligt i dagligdagen.

Udvise opmærksomhed og reagere ved afvigelser

På KU har du ikke kun ansvar for dine egne handlinger; hvis du bliver opmærksom på at sikkerhedsniveauet forringes, er det dit ansvar at reagere og synliggøre problemet.

Ansvar og accept

I forbindelse med din adgang til KU’s informationer følger et ansvar. Det er vigtigt at du forholder dig til - og accepterer - dette ansvar.

Som leder skal du ydermere sikre, at dine medarbejdere har forstået og accepteret det ansvar, de pålægges ved adgangstildelingen. Dette omfatter også eksterne konsulenters adgange.

2.5 Arbejdsbetinget behov

Tildeling og administration af adgange

Adgang til informationer på KU baseres på et dokumenteret arbejdsbetinget behov, der godkendes både af nærmeste leder og af den enhed, der ejer informationerne. Et arbejdsbetinget behov dokumenterer de nødvendige og tilstrækkelige rettigheder der skal tildeles. Nærmeste leder skal løbende sikre, at adgangen afspejler det aktuelle behov.

Funktionsadskillelse

Funktionsadskillelse betyder på KU at du ikke kan godkende eller hemmeligholde dine egne handlinger. Det er en proaktiv foranstaltning mod svig og bedrageri, som samtidig beskytter dig mod uberettiget mistanke. I KU's sikkerhedsmiljø opretholdes funktionsadskillelse i det omfang, det begrundes af forretningsmæssige behov.

2.6 Digital identitet

Digital identitet på KU

KU's systemer identificerer dig ved hjælp af din digitale identitet og gør dine handlinger personhenførbare. Dine arbejdsbetingede behov afspejles i de rettigheder, der tildeles din digitale identitet. Hvis en anden person benytter din digitale identitet, bliver handlingerne dermed udført i dit navn. En digital identitet er derfor personlig og må ikke overdrages eller anvendes af andre.

2.7 Sporbarhed

Dokumenteret historik

På KU er sporbarhed viden om hvem der har udført en given handling hvornår. Dette danner grundlag for efterforskning af historiske handlinger, for at fjerne uberettiget mistanke og afdække hvorvidt uregelmæssigheder er opstået som følge af fejl eller misbrug. Samtidig er sporbarhed en forudsætning for nødvendig periodisk opfølgning og kontrol.

2.8 Uden for KU

Sikkerhedsniveauet gælder alle

Alle, der behandler informationer for KU, skal efterleve forretningens krav til sikkerhed. Hvis informationer behandles uden for KU's sikkerhedsmiljø, f.eks. hos en ekstern samarbejdspartner, skal denne partner være informeret om og efterleve de samme krav, der stilles internt på KU.

Dette gælder også når du som ansat transporterer eller anvender informationer uden for KU, både logisk og fysisk.

3 Organisering og rapportering

På strategisk niveau udstikkes retningen for KU af Direktionen, dvs. det defineres hvad KU's behov for informationssikkerhed er.

Dette oversættes af Informationssikkerhedsgruppen til overordnede retningslinjer for hvordan sikkerhedsbehovet kan opfyldes.

Alle der drifter et system som anvendes til at opbevare eller behandle informationer har pligt til at designe og implementere løsningen sådan at den lever op til retningslinjerne.

Det er også et krav at der som en del af løsningen designes hvordan man kan kontrollere at løsningen lever op til retningslinjerne.

Endelig er det et krav til løsningen at der jævnligt rapporteres i hvilken grad retningslinjerne efterleves.

Informationssikkerhedsgruppen har til opgave at samle rapporteringen, opretholde et samlet overblik og foretage periodisk ledelsesrapportering.

Ledelsesrapporteringen giver Direktionen mulighed for at agere og prioritere i forhold til udfordringer på tværs af hele KU.