# IT- og Informationssikkerhed

Orientering til Bestyrelsen

Poul Halkjær Nielsen,
Informationssikkerhedschef,
9. december 2019

UNIVERSITY OF COPENHAGEN

# KU's risikoprofil

Risikoprofilen viser overordnet de værdier, der af KU anses for at være de vigtigste for universitetets drift. Derfor er det også de kategorier der skal tilsikres beskyttelse af.

1. Trusler mod KU's evne og muligheder for at tiltrække samarbejdspartnere og forskningsmidler samt **tab af image**, som konsekvens af at personhenførbare oplysninger lækkes
2. **Fejl i forskningsresultater** som konsekvens af dårlig indledende datakvalitet, samt manglende evne til at kunne eftervise resultater grundet efterfølgende forvanskning af datagrundlag
3. Tab af image og **validitet af eksamensbeviser** grundet forvanskning af studiedata
4. Tab af image og evne til at udføre fremtidig forskning grundet **destruktion af unikke og/eller ikke-genskabelige informationer**

# Indledende kommentarer

- IT- og informationssikkerhed er i den universitære verden (verden over) en svær størrelse grundet den type organisering sektoren arbejder ud fra og de ret frie vilkår forskningen generelt fordrer
- IT- og informationssikkerhed er i høj grad lagt i hænderne på slutbrugeren, hvorfor enhver opstramning eller ændring reelt set skal ske som en kulturændring dvs. igennem daglig ledelse
- IT- og informationssikkerhed er dog fortsat i stigende kurs som image- og reelt konkurrenceparameter. Ikke mindst grundet eksternt pres fra samarbejdspartnere, revisioner og fra lovgivningen
- Ledelsen har, jævnfør politikken, generelt en pligt til at risikovurdere og sikre informationer på passende vis. Politikken følger den ministerielt stærkt anbefalede ISO 27001 standard

# Læsevejledning til Trafiklys

- Rød betyder at niveauet er faldet eller at en væsentlig leverance er overskredet
- Gul betyder at der skal ekstra tiltag til for at komme i mål
- Grøn betyder at opgaven er på rette spor

# ISO 27001 informationssikkerhedspolitik

| Emne | Trafiklys 12/6 | Status | Kommentar |
|---|---|---|---|
| Risikoprofil og politik, retningslinjer og sikkerheds-vejledninger | ● | Løbende vedligehold | Ved egen intern revision samt Rigsrevisionens gennemgang er politikken med tilhørende underdokumenter fortsat godkendt og gældende.<br><br>Den er tilgængelig for alle grupper på KU. |
| Organisatorisk implementering og opfølgning | ● | I gang | Rigsrevisionen påpeger, at både den IT-tekniske såvel som den ledelsesmæssige forankring og efterlevelse ikke er tilstrækkelig. Der arbejdes på at rette dette forhold igennem flere tiltag af både teknisk som organisatorisk karakter. Der blev afgivet særskilt status på dette d. 17. juni.<br><br>Det er fortsat en stor opgave at nå de mange ansatte, studerende og tilknyttede grundet den udskiftning, der naturligt foregår på et år. Derfor er målsætningen at gøre sikkerhed til en del af den daglige ledelsesopgave. Der er foretaget en række tiltag for at understøtte og fastholde denne udvikling. |

# Persondataforordningen (GDPR)

| Emne | Trafiklys 9/12 | Status | Kommentar |
|---|---|---|---|
| Privatlivspolitik-procedurer, vejledninger og skabeloner til persondata udarbejdet og i drift. Undtaget værktøj til GDPR-risikovurderinger, som forventes implementeret ved årsskiftet 2019/2020 |  | Løbende vedligehold | Der er planlagt interne kontroller i 2020. |
| Online kursus udbudt til alle fastansatte medarbejdere |  | Løbende tilgængeligt | Det overvejes at gøre kurset obligatorisk |
| Klagesager |  | 5 klagesager i Datatilsynet – endnu ikke afgjort | |
| Datatilsynets sanktioner |  | Datatilsynet har i en enkelt sag udtalt alvorlig kritik af KU, på grund af en studerendes tab af persondata | Datatilsynet ændrer praksis, således at universitetet er ansvarlig for studerendes håndtering af persondata, når universitetet beslutter hvornår og hvordan studerendes skal indsamle og håndtere persondata |

# Sikkerhedshændelser indberettet til Datatilsynet

| Emne | Trafiklys 9/12 | Status | Kommentar |
|---|---|---|---|
| Tilgængelighed | ● | Ingen ændring | |
| Integritet | ● | Ingen ændring | |
| Fortrolighed | ● | Stigning | Der er sket en lille stigning i antallet af anmeldte fortrolighedsbrud. Der er foretaget knap 50 lovpligtige indberetninger til Datatilsynet i 2019 – (24 i 2018 fra 25. maj til årsskiftet.<br><br>9 af anmeldelserne skyldes tekniske forhold. Resten er menneskefejl som typisk sker ved mailafsendelser eller fejlopslag. |

# Samlet risikobillede

| Emne | Trafiklys 9/12 | Kommentar |
|---|---|---|
| Ændring i risikooplevelse – "siden sidst" rapportering<br><br>Risiko måles ved at bedømme, hvor stor sandsynlighed der er for, at en trussel indtræffer, samt hvor store konsekvenser det kan have. |  | Truslen mod sektoren er vurderet af DK-CERT i en trusselsvurdering fra august 2019. Truslerne vurderes som:<br><br>• Cyberspionage er meget høj<br>• Cyberkriminalitet er meget høj<br>• Cyberaktivisme er lav<br>• Insidertruslen er meget høj<br><br>Truslerne og deres vurderingsniveau er på samme niveau som andre tidligere vurderinger fra Politiets Efterretningstjeneste, Center for Cybersikkerhed samt UK's National Cyber Security Centre. KU's informationssikkerhedschef er enig i disse trusler, og nogle af dem er konkret oplevet mod KU i år.<br><br>De eksterne krav til KU er fortsat stigende. Eksterne parter vurderer KU ud fra en strammere organiseringsmodel, end den vi har., Eksterne parters brug af security ratings samt security assessment-firmaer udfordrer KU's tilgang på udvalgte forskningsområder. |
| Organisatorisk og teknisk forbedring |  | KU-IT's tekniske sikringsløsninger er ved at slå igennem i praksis, og der udestår fortsat, at en række tekniske forbedringer er udbredt til alle på KU eller anskaffet og idriftsat. |
| Rapporterings forbedring |  | Den forbedrede rapportering fra de enkelte enheder (jf. Rigsrevisionens påpegninger) skal i gang. Der udestår få risikovurderinger, hvorefter et samlet KU-billede dækkende både administrative data og forskningsdata kan udarbejdes. De første 47 forskningsenheder samt alle fakulteter har modtaget en risikovurdering. Det skal nu vedligeholdes i Informationssikkerhedsudvalget og følge dets årshjul. |