IT- og Informationssikkerhed

Orientering til Bestyrelsen

Poul Halkjær Nielsen,
Informationssikkerhedschef,
6. december 2018

UNIVERSITY OF COPENHAGEN

KU's Risikoprofil

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 kommentar

- 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 reel konkurrenceparameter. Ikke mindst grundet eksterne pres fra samarbejdspartnere, revisioner og fra lovgivningen
- Ledelsen har, jævnfør politikken, generelt en pligt til at risikovurdere og sikre informationer på passende vis

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 følger det er på rette spor

ISO 27002 informationssikkerhedspolitik

Emne	Trafiklys 6/12	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. Den er nu 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 vinkel. Der er oprettet et program med Rektor som styregruppeformand til at samle, følge og sikre fremdrift i leverancerne i programmet.

EU's persondataforordning (GDPR)

Emne	Trafiklys 6/12	Trafiklys 12/6	Status	Kommentar
Privatlivspolitik procedurer, vejledninger og skabeloner til persondata			Løbende vedligehold	Der er lavet 30 GDPR konsekvensanalyser Modtaget 9 anmodninger om indsigt/sletning Afholdt 75 informationsmøder
Kvalitetssikring af administrative processer og værktøjer			Løbende vedligehold	PWC har gennemgået processer og materiale og vurderet det tilstrækkeligt og brugbart
Datahåndtering			I gang	Der er oprettet ca. 900 GDPR-sikrede drev. Der pågår fortsat dataoprydning.

Sikkerhedshændelser *

Emne	Trafiklys 6/12	Trafiklys 12/6	Status	Kommentar
Tilgængelighed			Ingen ændring	
Integritet			Ingen ændring	
Fortrolighed			Stigning	Der er sket en stor stigning i antallet af kendte fortrolighedsbrud. GDPR meldepligten har gjort at internt såvel som eksternt indberettede brud på sikkerheden er steget meget. Der er foretaget knap 30 lovpligtige indberetninger til Datatilsynet.

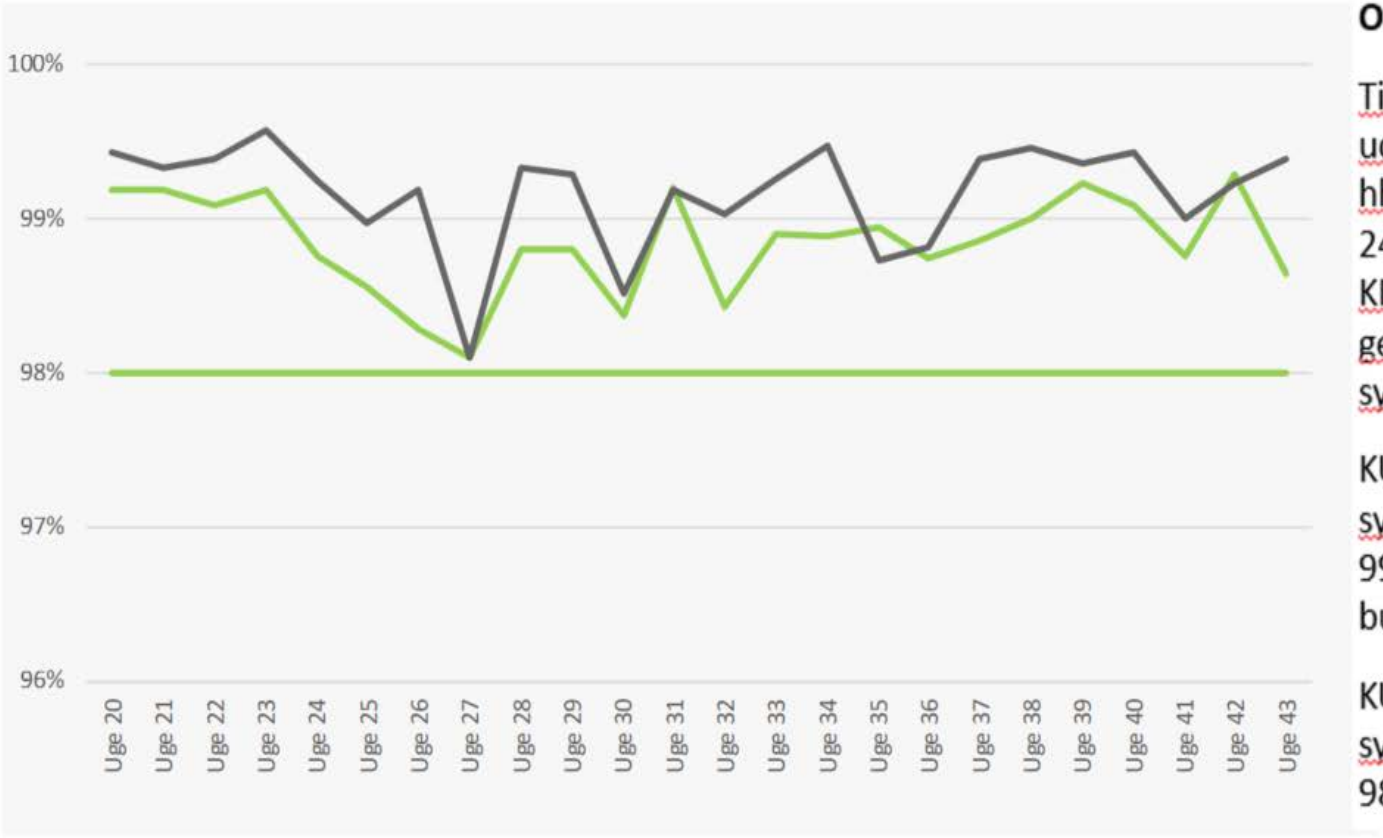
- Kun indrapporterede hændelser

Samlet risikobillede

Emne	Trafiklys 6/12	Trafiklys 12/6	Kommentar
Ændring i risikooplevelse – "siden sidst" rapportering			De eksterne krav til KU er hastigt stigende. Eksterne partnere vurderer KU ud fra en organiseringsmodel, der adskiller sig fra den vi har. Rigsrevisionen, ISO27002 benchmarking, brugen af security ratings samt security assessment firmaer udfordrer KU's frie tilgang til organisering meget og truer reelt set samarbejder og finansiering.
Organisatorisk forbedring			KU-IT's tekniske sikringsløsninger står foran at slå igennem i praksis. Dannelsen af en ny informationssikkerheds-organisering skal slå mere igennem. Begge dele vil afhjælpes Rigsrevisionens påpegninger.
Rapporterings forbedring			KU-IT resultater samt dannelsen af en ny informationssikkerhedsorganisering skal slå igennem. Rapportering fra de enkelte enheder skal også forbedres også jf. Rigsrevisionens påpegninger.
Organisatorisk parathed EU's persondataforordning			Med flere gennemløb af de administrative processer omkring GDPR er KU ved at finde et mere modent leje understøttet af vejledninger og procedurer

Tilgængelighed/oppetider for målte systemer

- målinger på centrale fællesovervågede KU systemer for Uddannelse, HR, Økonomi og Kommunikation samt fælles email



Om KPI'en:

Tilgængelighed dækker over udvalgte systemers oppetid i hhv. business hours (—) og 24×7 (—)
KPI'en her er baseret på et gennemsnit af de enkelte systemers måleresultater

KU-IT har et mål om at systemerne er tilgængelige 99% af tiden indenfor business hours (—)

KU-IT har et mål om at systemerne er tilgængelige 98% 24×7 (—)