IT- og Informationssikkerhed

Orientering til Bestyrelsen

Poul Halkjær Nielsen,
Informationssikkerhedschef,
15. juni 2020

UNIVERSITY OF COPENHAGEN

KU's risikoprofil – opdateret

Risikoprofilen viser i fem punkter det, der er vigtigst for at Københavns Universitet kan fungere, og dermed også hvad vi særligt skal passe på. Risikoprofilen kan bruges som udgangspunkt, når der skal tales om trusler, risiko og værdi for Københavns Universitet. Ordlyden i risikoprofilen understøtter både informationssikkerhedspolitikken, GDPR samt forsknings datamanagement.

De fem punkter er opsat i prioriteret rækkefølge.

1.Trusler mod KU's evne og muligheder for at tiltrække samarbejdspartnere, ansatte, studerende og forskningsmidler samt tab af renommé, som konsekvens af at personfølsomme og andre fortrolige oplysninger lækkes

2.Manglende evne til at kunne sikre integritet af og eftervise forskningsresultater på grund af brug af en forkert eller mangelfuld platform til datahåndtering, som ikke beskytter mod forsætlig eller uforsætlig forvanskning af data

3.Tab af renommé og validitet af eksamensbeviser grundet forvanskning af studiedata

4.Tab af renommé og evne til at udføre fremtidig forskning grundet tab eller destruktion af unikke og/eller ikke-genskabelige informationer

5.Trusler mod universitetets basale infrastruktur med deraf afledte økonomiske konsekvenser

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. Enhver standard eller ændring skal ske som en kulturændring båret af den daglige ledelse
- IT- og informationssikkerhed er fortsat i stigende kurs som image- og reelt konkurrenceparameter, men senest også som reel beskyttelse af universitetets værdier og fortsatte drift
- Ledelsen er, jævnfør politikken, generelt forpligtet 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 et væsentlig kriterie har ændret sig
- Gul betyder at der skal ekstra tiltag til eller opmærksomhed for at forblive sikker
- Grøn betyder at sikkerheden/opgaven er på rette spor

ISO 27001 informationssikkerhedspolitik

Emne	Trafiklys 15/6	Status	Kommentar
Risikoprofil og politik, retningslinjer og sikkerhedsvejledninger	●	Løbende vedligehold	Risikoprofilen, Informationssikkerhedspolitkken samt underliggende retningslinjer og sikkerhedsvejledninger er gransket og publiceret. Teksten er afpasset så de samme begreber benyttes i Forskningspolitikken. Vejledningernes afsnit vedrørende GDPR er tilrettet i samarbejde med Databeskyttelsesrådgiveren. De er tilgængelige for alle grupper på KU på DK og UK
Organisatorisk implementering og opfølgning	●	I gang	De tekniske, politik og organisatoriske tiltag, der udløb af Rigsrevisionens rapport, er under implementering. Det er en stor opgave at nå de mange ansatte, studerende og tilknyttede grundet den udskiftning, der naturligt foregår på et år. Derfor er målsætningen at sikkerhed er en del af den daglige ledelsesopgave en opgave som informationssikkerhed forfølger. Særligt opfølgningen på de mange lokale risikovurderinger skal være med til at styrke den organisatoriske bevidsthed.

Persondataforordningen (GDPR)

Emne	Trafiklys 15/6	Status	Kommentar
Privatlivspolitik, procedurer, vejledninger og skabeloner til persondata udarbejdet og i drift.	●	Løbende vedligehold	Overholdelsen af procedurer revideres af Deloitte i 2020 på områderne: • Databehandleraftaler på et institut på SAMF • Oplysningspligt i rekrutteringssager, SCIENCE-HR • Sletning af forskningsdata, Institut for Folkesundhed • Sikkerhed på S-drev, KU-IT
GDPR-Risikovurderingsværktøj for behandling af forskningsdata	●	Sat i drift i midlertidig papir-udgave primo marts 2020. Elektronisk formular forventet i drift primo juni 2020	GDPR-risikovurderingen indgår i samme proces som registrering af forskningsprojektet i fortegnelsen over behandling af persondata
5 klagesager i Datatilsynet	●	2 er endnu ikke afgjort 1 sag får KU medhold 2 begrænset kritik	
Sikkerhedshændelser indberettet til Datatilsynet	●	50 indberetninger i 2019 13 indberetninger til dato i 2020	Hovedsagelige menneskelige fejl. En kritisk sag – manglende fortrolighed i IT-servicedesk system for personnumre

Samlet risikobillede

Emne	Trafiklys 15/6	Kommentar
Ændring i risikooplevelse – "siden sidst" rapportering 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. Truslerne vurderes som: • Cyberspionage er meget høj • Cyberkriminalitet er meget høj • Cyberaktivisme er lav • Insidertruslen er meget høj Der er generelt udstedt varsler fra USA og UK sikkerhedstjenesterne om Corona-forsknings spionage fra statsmagter, samt en stigning i ransomware angreb af samme årsag. Senest er ransomware gået ud over Ruhr-Universität Bochum. Pga. Corona hjemmearbejdet er der også sket en stigning i phishing kampagner samt angreb mod VPN og andre systemer uden multifaktor-autentificeringsbeskyttelse.
Organisatorisk og teknisk forbedring		KU-IT's tekniske sikringsløsninger skal slå igennem i praksis, og der udestår fortsat, at en række tekniske forbedringer er tilgængelige for alle på KU eller anskaffet og idriftsat. Corona-hjemsendelsen har også udskudt eller sinket tiltag, der forudsætter lokal fysisk tilstedeværelse af brugere og/eller teknikere.
Rapporterings forbedring		Den forbedrede rapportering fra de enkelte enheder (jf. Rigsrevisionens påpegninger) skal i gang. Der udestår vedligehold lokalt af risikovurderingerne, Informationssikkerhed har udestående at få lavet en samlet risikovurdering for både forskningen samt de administrative fælles enheder.