POLITIK FOR INFORMATIONSSIKKERHED

26. oktober 2016

Konsekvenser af sammenlægningen

Pr. 1. januar 2017 bliver Statsbiblioteket og Det Kongelige Bibliotek sammenlagt i et nyt fælles Nationalbibliotek. Det betyder også, at der skal udarbejdes en ny fælles sikkerhedsorganisation og fælles procedurer og retningslinjer sikringsmæssigt. Dette arbejde kan ikke nå at blive afsluttet inden 1. januar, så derfor gælder alle sikringsmæssige retningslinjer også efter 1. januar og indtil der er fastsat et nyt fælles grundlag, som der vil blive henvist til i stedet.

Indledning

Dette er Statsbibliotekets politik for informationssikkerhed, som skal beskrive:

- Formål og baggrund om Statsbibliotekets hovedopgaver
- Mål og afgrænsning af Statsbibliotekets arbejde med informationssikkerhed
- Samspillet med de primære interessenter set i perspektiv af informationssikkerhed.

Statsbibliotekets opgaver og formål

Statsbibliotekets politik for informationssikkerhed knytter an til bibliotekets opgaver og mål, bl.a. udtrykt i Statsbibliotekets Strategi 2015-2018. Med arbejdstitlen 'Mere til flere' vil Statsbiblioteket:

- udbrede og dele bibliotekets mange services med flere
- være på flere platforme og i flere rum
- gøre det nemt at bruge tekst, lyd og billede i mangfoldige kombinationer og sammenhænge.

Dette stiller naturligvis høje krav informationssikkerheden. Hvis vi koger missionen ned til vores kerneopgaver og primære forretningsområder, så består dette i:

- samlingsopbygning
- bevaring og
- tilgængeliggørelse.

Der findes flere måder at udtrykke disse hovedopgaver på, men afgørende er det, at informationssikkerhed ikke er noget, vi kobler på vores forretning.

Det er selve forretningen at sikre de fysiske og elektroniske ressourcers autenticitet og ikke mindst sikre, at brugen af dem sker i overensstemmelse med gældende lovgivning. Overvejelser om niveau af informationssikkerhed og ønsket om at flere skal have adgang til mere er derfor en selvfølgelig samtale på Statsbiblioteket. Der sker en nøje afvejning af hensyn til beskyttelse og benyttelse.

Som det fremgår af missionen, har Statsbiblioteket mange forskellige roller, både som offentlig myndighed, der indsamler og forvalter kulturarv, og som leverandør

af it-infrastruktur mv., samt som kunde i faglige og driftsmæssige sammenhænge.

Samtidig er en anden væsentlig rolle den udadvendte kontakt med brugere, hvor det især drejer sig om udlån af materialer og service. Dette stiller forskellige krav til den måde, vi systematisk tilrettelægger og praktiserer informationssikkerhed. Fælles for opgaverne er, at Statsbiblioteket som offentlig myndighed skal levere meget forskelligartede ydelser af høj kvalitet og troværdighed.

Som eksempler på dette håndterer vi data om brugernes låneadfærd, vi tilgængeliggør licensbelagte biblioteksressourcer, som kræver systemer, der kan regulere brugen af den enkelte ressource, og mod betaling leverer vi infrastruktur til bevaring af kulturarv osv.

Samtidig henvender vores ydelser sig til såvel individer og organisationer og ad mange forskellige kanaler – senest udmøntet i en 'Strategi for informationsforsyning' (maj 2012) populært kalder 'Kanalstrategien'. Denne omtaler primært organisering af data, og hvordan vi tilgængeliggør dem i forhold til forskellige målgrupper på platforme, som i øget grad drives i organisatoriske fællesskaber med eksterne partnere.

På det administrative plan kan vi desuden konstatere et øget krav om brug af systemfællesskaber, webbaserede tjenester, applikationer m.m. Såvel medarbejdere som brugere forventer, at de kan løse opgaver og tilgå og genbruge diverse ressourcer via deres personlige arbejdstablets. Udfordringen for særligt IT består dagligt i afvejning af effektivitet, relevans og informationssikkerhed.

Målet med politik for informationssikkerhed

Politik for informationssikkerhed fungerer som et styringsredskab. Den sikrer, at der er et fælles grundlag for arbejdet med informationssikkerhed i hele organisationen og fastlægger vores ambitionsniveau for sikkerhedsarbejdet.

Politik for informationssikkerhed indeholder derfor de overordnede målsætninger og danner grundlag for udformning af Statsbibliotekets sikkerhedshåndbog, der er et arbejdsredskab til bibliotekets ledelse i forbindelse med styring og dokumentation af informationssikkerhed med de underliggende retningslinjer, procedurer og forretningsgange.

Dermed skal politikken ligeledes understøtte bevidstheden om informationssikkerhed i Statsbibliotekets organisation og virke. De retningslinjer, procedurer og forretningsgange, der udformes for at understøtte politik for informationssikkerheds hovedmålssætninger, skal sikre, at alle medarbejdere arbejder med og forholder sig til informationssikkerhed i det daglige arbejde.

Statsbiblioteket ser ikke kun vores sikkerhedsniveau som et krav for at kunne overholde lov- og myndighedskrav, men også som et kvalitetsgrundlag i forhold til vores service over for brugere, myndigheder, samarbejdspartnere og leverandører.

Grundlaget for denne politik er udover de generelle lov- og myndighedskrav blandt andet de krav og kontroller, der er fastsat i ISO 27 001, samt i Kulturministeriets retningslinjer for udarbejdelse af planer for samlingssikring.

Denne politik skal ses i sammenhæng med Statsbibliotekets faglige politikker og strategier, som dels findes via bibliotekets hjemmeside og dels er dokumenteret i Statsbibliotekets ISMS (Information Security Management System) om informationssikkerhed.

Omfang

Politik for informationssikkerhed omfatter de informationsaktiver, der er kritiske for, at Statsbiblioteket kan nå sine mål. Det drejer sig om såvel forretningsmæssige som administrative fagsystemer samt fysiske materialer og data. Informationsaktiverne er opdelt i følgende hovedområder:

- It-infrastruktur
- Økonomisk forvaltning
- Kulturarvssamlinger.

Politik for informationssikkerhed er gældende for alle medarbejdere i Statsbiblioteket. Politikken og særligt regler for informationssikkerhed forventes udgivet, læst og efterlevet af alle medarbejdere. Der henvises til sikkerhedshåndbogen

Statsbiblioteket benytter forskellige typer af leverandører og samarbejdspartnere, som har fysisk eller digital adgang til kritiske informationsaktiver. Betingelser for adgang fastlægges i overensstemmelse med Håndbog om informationssikkerhed.

Informationssikkerhed må såvidt muligt ikke opleves af brugerne som en forhindring i hverdagen. Brugernes adgang til Statsbibliotekets ressourcer skal være så let og smidig, som det kan sikkerhedsmæssigt forsvares ved en afbalancering af hensynet til benyttelse og beskyttelse ved de forskellige typer materiale. Dog er der fx særlige krav til beskyttelse og anvendelse af login/password, som skal være eksplicitte, når man opretter sig som bruger. Sådanne beskyttende vilkår vil optræde i naturlig sammenhæng med benyttelse.

Sikkerhedsniveau og risikovurdering

Set i lyset af Statsbibliotekets kerneforretninger er der fokus på sikkerhedsniveau i udformninger af systemer og it-infrastruktur samt indsamling og bevaring af kulturarvssamlinger, samtidig med at vi tilpasser vores sikkerhedsniveau i forhold til at sikre høj tilgængelighed af data og materialer.

Udfordringen er at balancere sikkerheden i forhold til, at vi også har som ambition, at flere brugere skal kunne tilgå mere og gerne på en brugervenlig måde, formuleret ved vores vision om at skabe attraktive rum for forskning, uddannelse og oplevelse, hvor brugerne hurtigt og smart kan skaffe alt relevant indhold.

Informationssikkerheden på Statsbiblioteket skal være på et niveau, der tilgodeser lov- og myndighedskrav, kontraktlige forpligtelser samt forpligtelser over for

brugere og samarbejdspartnere, der anvender biblioteket.

Statsbiblioteket vil ikke sikre sine aktiver for enhver pris, men vil være bevidst om enhver risiko og forholde sig tilfredsstillende til disse, hvormed et tilstrækkeligt sikkerhedsniveau etableres.

Der er i den forbindelse lagt vægt på, at Statsbiblioteket har forholdsvis få værdifulde værker målt i pengeværdi. Stjålne eller bortkomne værker kan i de fleste tilfælde genanskaffes, såfremt det skønnes ønskeligt at gøre det. Betydningen af Statsbibliotekets samling ligger i samlingen som helhed. Derfor udgør hændelser, der kan medføre, at samlingen går til grunde, de største trusler mod biblioteket. Den største trussel mod biblioteket er derfor risikoen for brand. Vandskade vil ligeledes kunne medføre omfattende ødelæggelser af samlingerne. Når det gælder de fysiske samlinger er vurderingen, derfor at indsatsen skal koncentreres om forebyggelse af brand og vandskader.

Et tilstrækkeligt niveau for informationssikkerhed opnås igennem sikringsforanstaltninger, der sikrer:

1. Fortrolighed, integritet og tilgængelighed af Statsbibliotekets systemer og data i forhold til den risikovurdering, der er fastsat for de kritiske informationsaktiver.
2. Beskyttelse af informationsaktiver, medarbejdernes kompetencer, organisationens image og informationer/data i Statsbibliotekets varetægt.

   Vores politik for informationssikkerhed skal endvidere rettes mod alle trusler, der kan komme såvel internt som eksternt fra: Bevidst skadevoldende handlinger og misbrug eller hændelige uheld og fejl.

   Det skal sikres, at risici er afdækket gennem en systematisk risikovurdering, og at der er forebygget og taget initiativer til at minimere risici. Konsekvenserne af en eventuel sikkerhedshændelse skal reduceres til et acceptabelt niveau.

   Sikringsudvalget er ansvarlig for risikovurdering og for at vurdere trusler, konsekvenser og risici. Risikovurderingen opdateres mindst én gang årligt samt ved eventuelle større ændringer i opgaver, leverandører, it-systemer eller anvendelsen deraf.

   Når det gælder de fysiske samlinger er vurderingen at der i tilfælde af brand og vandskader ikke skal foretages en redning af enkelte genstande, men derimod fokuseres på at indsatsen skal redde samlingerne som helhed. Derfor er udgangspunktet for indsatsen en forudsætning om, at materialerne bliver på stedet. Der foretages naturligvis altid en konkret vurdering udfra situationen, idet de mest værdifulde og unikke værker er tydeligt adskilt fra de øvrige samlinger og placeret i Sikringsrum.

   I forhold til reduktion af risikoen for skader på de fysiske samlinger arbejdes der især systematisk med brandstrategi og vandskadeforebyggelse som et supplement til de øvrige sikringsforanstaltninger i forhold til de generelle sikringsforanstaltninger vedrørende bl.a. fysisk sikring, overvågning, adgangs-

styring, awareness mv.

For at fastholde det tilstrækkelige sikkerhedsniveau på Statsbiblioteket skal følgende overholdes:

- Der skal forefindes retningslinjer, procedurer og forretningsgange, som sikrer, at informationssikkerhed er en integreret del af Statsbibliotekets drift og daglige arbejde.
- Statsbiblioteket skal igennem kontrakt- og leverandørstyring sikre, at brugen af eksterne konsulenter, samarbejdspartnere og leverandører ikke svækker Statsbibliotekets niveau for informationssikkerhed.
- Statsbiblioteket skal følge op på informationssikkerheden ved løbende vedligehold og optimering af politikken og de dertil hørende retningslinjer, procedurer og forretningsgange. Målet er at sikre en struktureret og kontinuerlig forbedringsproces.

I sikkerhedshåndbogen er arbejdet med håndtering af risici og muligheder uddybet.

Organisation og ansvar

Den øverste ansvarlige for informationssikkerheden på Statsbiblioteket er direktøren. Det overordnede grundlag for sikkerhedsarbejdet behandles af SLG, som er den øverste ledelse. Den konkrete gennemførelse af sikkerhedsarbejdet varetages af et sikringsudvalg som er sammensat med stor ledelsesrepræsentation.

Planlægning, implementering og kontrol af informationssikkerhed er defineret af Statsbibliotekets ledelse, og arbejdet gennemføres af Sikringsudvalget. Udvalget har følgende hovedopgaver (jf. besluttet kommissorium september 2015):

- at udvikle og vedligeholde institutionens sikringspolitik, -retningslinjer og instrukser gældende for alle typer af samlinger/data, bygninger, it-systemer og de procedurer, der anvendes til at administrere samlingerne; herunder sikre:
  - at kravene til informationssikkerhed (ISO27001) bliver implementeret i alle områder.
  - at beredskabsplan og bygningssikring er opdateret og implementeret; herunder gennemføre revision af Statsbibliotekets 'Værdiredningsplan'.
  - at det daglige sikringsarbejde er organiseret optimalt.
  - at afrapportere og drøfte indtrufne sikringsmæssige hændelser og fremlægge forslag til eventuelle justeringer.
  - at gennemføre kvalitetskontrol og dermed sikre, at det daglige arbejde udføres i overensstemmelse med de udarbejdede retningslinjer, politikker og instrukser.
  - at udbrede sikringsarbejdet til hele Statsbiblioteket og sikre involvering af medarbejder, fx gennem formidling og tilrettelæggelse af relevant uddan-

nelse.

– at kommunikere sikringsarbejdet til de forskellige målgrupper ved skriftlig information, oplæg, informationsbreve, opslag på medier mm.

Udvalget er organiseret på en sådan måde, at der er en stærk kobling mellem de strategiske, taktiske og operationelle sider af informationssikkerhed.

Udvalget har følgende faste medlemmer:

- Sikringschef/daglig sikringskoordinator af administration; May Dalsgaard
- Ledelsesrepræsentant NO/daglig sikringskoordinator af samlinger; Tonny Skovgård Jensen
- Ledelsesrepræsentant IT/daglig sikringskoordinator for it-systemdrift; Klaus Kjærgård
- Daglig sikringskoordinator for bygningssikring/beredskabsplan; Thomas M. Larsen
- Daglig sikringskoordinator for kundeservice og logistik; Inge Dyrlund Steensen
- Konsulent for sikringskvalitet, -kontrol og –jura; Hanne Birgitte Johansen
- Implementeringskonsulent; Lise Thusgaard Skovager.

Sikringschefen er ansvarlig for implementering og vedligeholdelse af informationssikkerhedssystemet på Statsbiblioteket og er ansvarlig for opfølgning på sikkerhedshændelser. Sikringschefen er en del af Statsbibliotekets strategiske ledelse (SLG) og har særligt fokus på informationssikkerhed i forhold til væsentlige beslutninger omkring forretningsområder og administration.

Politik for informationssikkerhed og risici revurderes af Sikringsudvalget og godkendes én gang årligt eller i forbindelse med eventuelle situationer, der tilsiger det. Fx ved større organisatoriske eller forretningsstrategiske forandringer.

Politikken fremsendes til Den Strategiske Ledergruppe (SLG) for endelig beslutning, inden den formidles til øvrige interessenter, medarbejdere, partnere m.fl.

Sikringsudvalget foretager en årlig afrapportering til SLG om effekten af ledelsessystemet for informationssikkerhed.

Sikkerhedsbevidsthed

Ledere og medarbejdere er ansvarlige for at efterleve retningslinjer og procedurer for sikkerhed i det daglige arbejde.

Den nødvendige viden og kompetence omkring informationssikkerhed kommunikeres til alle medarbejdere, og der bliver løbende arbejdet med holdninger og viden omkring informationssikkerhed. Ledelsen er ansvarlig for, at informationssikkerheden overholdes.

Brud på informationssikkerheden

Alle medarbejdere på Statsbiblioteket er forpligtet til at efterleve den til enhver tid

gældende politik for informationssikkerhed med tilhørende retningslinjer, procedurer og forretningsgange. En overtrædelse kan, efter omstændighederne, medføre sanktioner.

Hvis man som medarbejder oplever eller har mistanke om, at der sker brud på politik for informationssikkerhed, er man forpligtet til at rapportere dette til egen nærmeste leder, som sikrer videreformidling til Sikringsudvalget; typisk ved henvendelse til sikringschef eller øvrige udvalgsdeltagere. Man opfordres også til at henvende sig direkte til Sikringsudvalget. Sikringshændelser kan omhandle bl.a. overtrædelse af regler eller misbrug udført af bruger eller medarbejder samt systemfejl.

Mistanke og iagttagelser bør formidles hurtigt, så skaden ikke vokser, og eventuel indsats sættes i værk. Det vil efter indrapportering være op til Sikringsudvalget at udrede og dokumentere hændelsen og revurdere relevante sikringsforanstaltninger.

Sådanne sager bliver behandlet i Sikringsudvalget som sikringshændelser.

Hvis det ikke er muligt at reducere risikoen for sikringshændelser til et acceptabelt niveau underrettes Kulturministeriet. Det samme gælder, hvis der opstår tilfælde af større sikringshændelser, som truer samlingen.

Afvigelser

Hvis der opstår situationer, hvor kravene i politik for informationssikkerhed ikke kan efterleves, skal der skriftligt anmodes om dispensation af Statsbibliotekets sikringschef. Eventuelle afvigelser fra kravene skal dokumenteres, og der skal indføres alternative sikringsforanstaltninger.

Udarbejdelse og ikrafttrædelse

Håndtering af ændringer i sikkerhedsdokumentationen foretages på følgende måde:

- Politik for informationssikkerhed udarbejdes og godkendes af Sikringsudvalget. SLG skal godkende politikken for informationssikkerhed og årsrapport om informationssikkerhed.
- Håndbog om informationssikkerhed og retningslinjer, procedurer og forretningsgange udarbejdes og godkendes af Sikringsudvalget, som også sikrer implementering.
- Operationelle procedurer sikres af Sikringsudvalget.

Godkendt:

Dato og underskrift