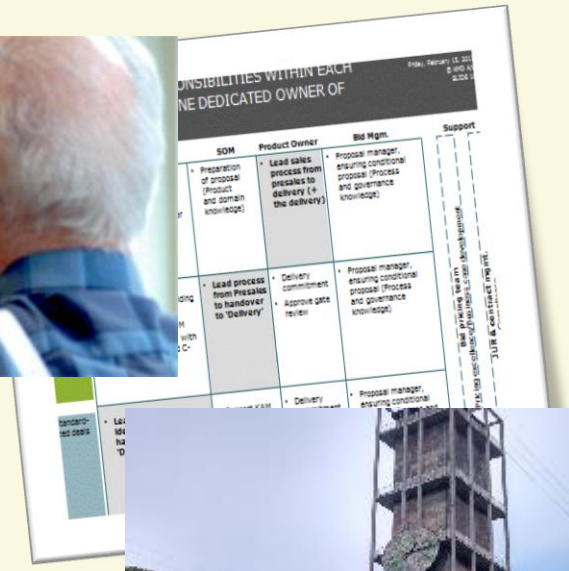
INFORMATIONSSIKKERHED

En rejsefortælling om funktioner, roller og ledelse



INDLEDNING

Indhold

Dette materiale beskriver de forskellige eksterne aktører samt interne roller og funktioner, der indgår i en organisations samarbejde om informationssikkerhed. Materialet er målrettet ledere, der skal danne sig et overblik over feltet, og som eventuelt har brug for at viderekommunikere området for informationssikkerhed, herunder principper i ISO27001.

Materielet bør tilpasses til din organisation

Dette materielle indeholder generelle beskrivelser, hvor det kan være nødvendigt at tilpasse præsentationen ved at fjerne eller tilføje dele, således at præsentationen gøres relevant til en specifik organisation.

Eksempler på hvad kan ændres:

- Farver og baggrund så at det passer ind i organisationens template
- Eksterne aktører som er irrelevante/relevante for organisationen kan fjernes/tilføjes
- Tilpasning af interne roller og titler som er relevante for organisationen
- Udvikling af nye informationssikkerhedsrejser som illustrerer organisationens virkelighed.

HVORFOR ER DET VIGTIGT?

30% af alle phishing-meddelelser blev åbnet af modtageren i 2015

Version2.dk

Sådan blev kommuner udsat for ransomware-angreb

Mails med vedhæftede filer sendt til kommunale medarbejdere i Gribskov og Nordfyns Kommune resulterede i et afpresningsforsøg og krypterede filer.

Computerworld.dk

Mindst 180 millioner kroner. Så mange penge er det lykkedes for hackere at fuppe sig til via såkaldt CEO Fraud eller 'direktør-svindel'

I 2016 har der været en stigning i forsøg på at narre virksomheder og organisationer til at overføre penge til udlandet

200.000 varianter af malware bliver registret hver dag hos Statens It

DR.dk

Fremmed stat spionerede mod dansk ministerium

flere danske myndigheder med følsomme oplysninger om dansk erhvervsliv
for målrettet cyber[illegible]e fra en fremmed stat [illegible]er hidtil

HVAD ER KONSEKVENSEN?

STIGENDE PROBLEM I DANMARK

- Flere kommuner har b.la. oplevet ransomware, der holder it-systemer som gidsel med nogle direkte konsekvenser
- Tabt arbejdstid
- Tab af data og information
- Økonomisk tab

DR.dk:

Ni ud af ti kommuner har været udsat for cyberangreb i år

TABT TILLID OG TRYGHED

- Generelt har borgere og virksomheder i Danmark stor tillid til myndigheder
- Hvis kritisk information går tabt, eller bliver uhensigtsmæssigt spredt, vil tilliden blive brudt

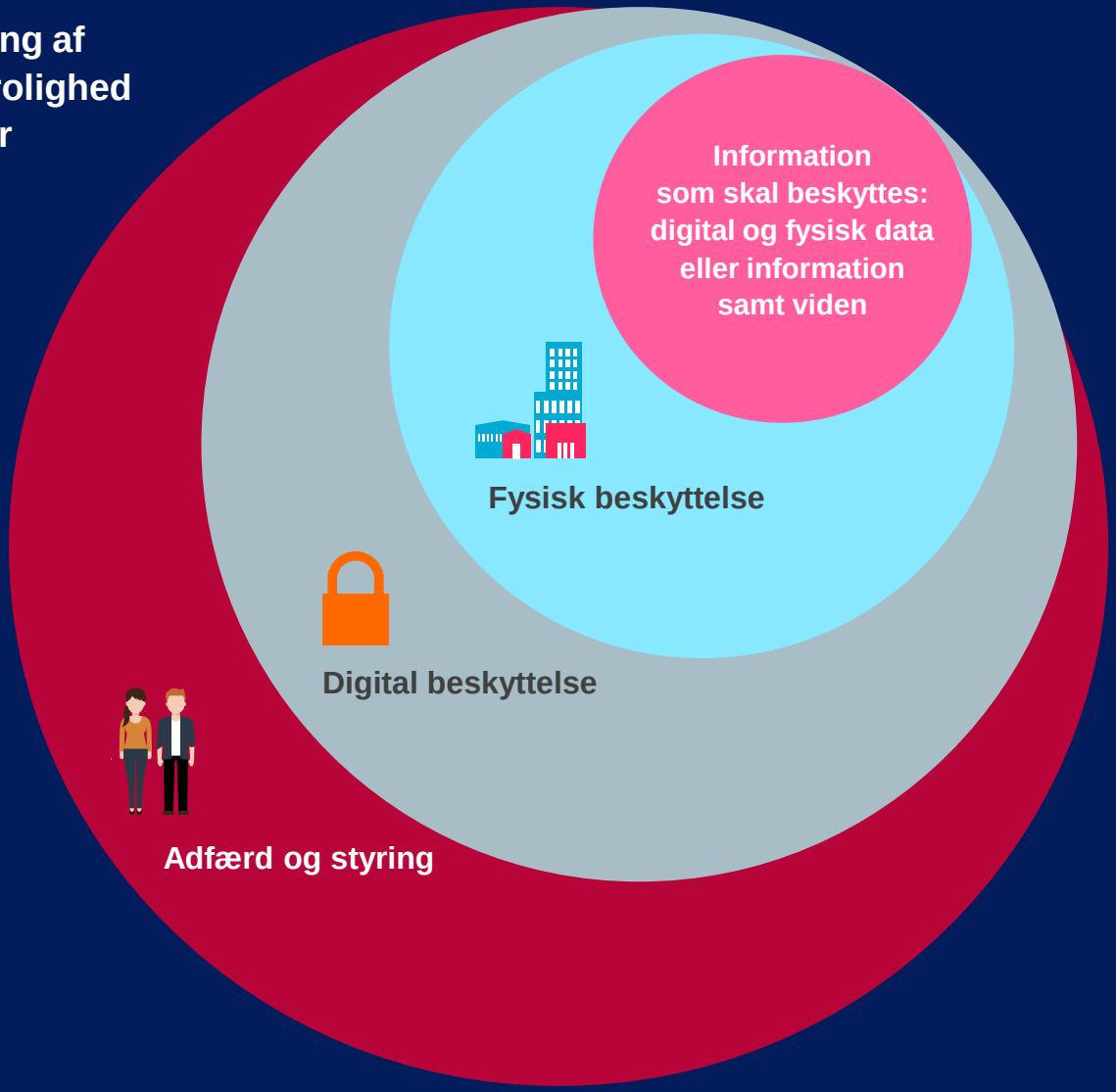
Børsen:

HVAD ER INFORMATIONSSIKKERHED?

Informationssikkerhed er sikring af informationens integritet, fortrolighed og tilgængelighed imod trusler

Sikkerhedsvariabler

- Teknologiudvikling
- Brugerbehov
- Økonomi



INTERNE ROLLER OG FUNKTIONER

Roller

Ledelse

Topledelse

- Har det overordnede ansvar for informationssikkerheden og sætter den strategiske retning
- Har overblik af risici og fordeler og placerer roller og ansvar i organisationen.

Mellemleder

- Sikrer forankring af informationssikkerhed i forretningsprocesser og aktiviteter.

Medarbejdere

Medarbejder

- Forstår at efterleve politikker og retningslinjer
- Agerer proaktivt og bidrager dermed til at sikre høj informationssikkerhed.

Funktioner

Informations-sikkerhedsudvalget

- Tværfaglig gruppe med topledelse som formand der sætter mål for sikkerheden
- Sørger for at informations-sikkerheden realiseres og efterleves i organisationen.

Dataejere

- En chef/leder som er ansvarlig for de data hans afdeling danner
- Sikrer hans medarbejdere håndterer data korrekt

- Data håndteres efter instruks fra systemejer.

Systemejerne

- En chef/leder, der er ansvarlig for de enkelte systemer og står for at identificere de mest sårbare dele af systemerne
- Udpeget af topledelsen.

Databeskyttelses-rådgiver (DPO)

- Overvåge, underrette og rådgive om overholdelsen af lovkrav vedr. følsomme persondata
- Udpeget af topledelsen.

Informationssikkerheds-koordinatoren

- Sekretær for sikkerheds-udvalget
- Organisationens tværgående daglige sikkerhedsleder.

STØTTEFUNKTIONER OG KERNEOPGAVER

Støttefunktioner

	HR	Økonomi	Jura/kontrakt	It-ansvarlig/arkitekt
Typiske kerneopgaver	Varetager: • Specialistopgaver, trivselsproblemer • Administrative opgaver såsom ansættelser, funktionsskifte, afskedigelser og vedligehold af stamdata • Forretningsorienterede opgaver, fx ressourcebemanding, jf. strategi.	Varetager: • Økonomiske forhold, herunder bogføring, udarbejdelse af interne og eksterne regnskaber, budgettering, ind- og udbetalinger, samt løn- og gageudbetalinger mv.	Varetager : • Kunde- og leverandørkontakt, omsætningsfastholdelse og -udvikling samt kontraktstyring • Rådgivning om indkøb i lyset af juridiske og kontraktuelle forhold.	Varetager: • Koblingen mellem forretning/forvaltning er it-understøttet, således der er den nødvendige sammenhæng mellem forretnings- og it-arkitektur • Sikringen af principper for systemernes design og udvikling og for deres indbyrdes sammenhæng.
Typiske opgaver i relation til informations-sikkerhed	• Forvaltning af sikkerhedsgodkendelser samt udarbejdelse og gennemførelse af awarenes-program. • Udarbejdelsen af brugerrettede sikkerhedspolitikker og HR-beredskabsplaner.	• Budgettering og opfølgning af informations-sikkerhedsaktiviteter • Økonomisk konkretisering af konsekvenser af risici • Evt. hensættelser af midler.	• Fortolkning af love og direktiver for persondata og informationssikkerhed generelt • Sikringen af kontrakter og juridisk bistand ved leverandørstyring.	• Etablering af sikkerhedsarkitektur og valg af sikkerhedsløsninger, herunder løsninger til monitorering, logning og rapportering • Beredskabsplan for it-arkitekturen.

HVILKET ANSVAR HAR ROLLERNE?

		Styring af informations-sikkerhed	Udvikling af politik for informations-sikkerhed	Risiko-vurdering og håndtering	Leverandør-styring	Hændelses-håndtering	Beredskabs-planlægning	Uddannelse og oplysning	Planer for sikkerheds-aktiviteter	SOA-dokumentet
ROLLER	Topledelsen	A	A	A	A	A	A	A	A	A
	Mellemledere	A	A	A	A	A	A	A	A	A
	Medarbejdere					I	I	I	I	
FUNKTIONER	Informationssikker-hedsudvalget	R	R	R	I	R	R	R	R	R
	Informationssikker-hedskoordinatoren	S	S	S	S	S	S	S	S	S
	Systemejere			C	C	C	C	C	C	C
	Dataejere			C	I	C	C	I	C	C
	DPO		C	C	C	C	C	C	I	C
	Jura/Kontrakt		C	C	C	C	I	I	I	I
	HR		C	C		C	I	S	I	I
	It-ansvarlige, It-arkitekter		C	C	R	C	I	C	I	C
	Økonomi		C	C	I	C	I	I	I	I

R (Responsible): Er ansvarlig for at opgaven udføres

A (Accountable): Kan træffe beslutninger og står til regnskab for opgaven

S (Supportive): Hjælper og supporterer opgaven

C (Consulted): Har vigtig information og bør derfor konsulteres under udførelsen

I (Informed): Skal holdes informeret og er formentlig afhængig af opgavens udfald

TOPLEDELSE

Rolle i sikkerhedsarbejdet

- Topledelsen har det overordnede ansvar for informationssikkerheden i organisationen, herunder at fastlægge sikkerhedsniveauet
- Ansvaret inkluderer ansvaret for, at medarbejderne er kvalificerede til at arbejde sikkert med organisationens informationer
- Topledelsen træffer de overordnede beslutninger vedrørende informationssikkerhed og forholder sig til økonomiske, ressourcemæssige og organisatoriske konsekvenser.

Opgaver i sikkerhedsarbejdet

Topledelsen skal:

- Sikre, at arbejdet med informationssikkerhed har ledernes opbakning
- Holde sig ajour med det aktuelle risikobillede ved at samarbejde med sikkerhedskoordinatoren og de personer (entiteter), der har ansvar for informationsaktiverne
- Etablere et Information Security Management System (ISMS)/ledelsessystem for de politikker, procedurer, processer, organisatoriske beslutningsgange og aktiviteter, som udgør komponenterne i organisationens styring af informationssikkerhed
- Vurdere, om der er behov for ekstern rådgivning og bistand til sikkerhedsarbejdet.

MELLEMLEDER

Rolle i sikkerhedsarbejdet

- Mellemledere er ansvarlige for operativ implementering og løbende kontrol med overholdelsen af retningslinjer, procedurer, budget mv.
- De bidrager i øvrigt til at højne opmærksomheden omkring informationssikkerhed, og fungerer som daglig sparringspartner for medarbejderne i forhold til efterlevelse af sikkerhedsforanstaltningerne.

Opgaver i sikkerhedsarbejdet

Mellemlederne skal:

- Påtage sig ansvaret for at sikre udarbejdelser af de detaljerede procedurer, instrukser og tjeklister inden for rammerne af de sikkerhedsniveauer organisationens topledelse har fastlagt
- Sikre, at organisationens arbejde planlægges på en måde, så informationssikkerheden understøttes
- Opfølge på sikkerhedsinitiativer i forhold til medarbejdernes daglige arbejde, herunder sikre høj *awareness* om informationssikkerhed
- Som medarbejdere rapportere risici og hændelser.

MEDARBEJDER

Rolle i sikkerhedsarbejdet

- Medarbejdernes har den vigtigste rolle i forhold til informationssikkerheden, hvor medarbejderne sikrer, at de uddelegerede opgaver udføres på en måde, så organisationen efterlever lovgivningen og interne politikker
- Medarbejdergrupper har naturligvis meget forskellige berøring med data, information og fysisk sikkerhed. Dermed har medarbejdere forskellige roller i sikkerhedsarbejdet.

Opgaver i sikkerhedsarbejdet

Medarbejdernes opgaver i sikkerhedsarbejdet afhænger i høj grad af, hvor meget data mv. de er i berøring med i deres daglige arbejde. Generelt kan det dog siges, at de skal:

- Overholde gældende politikker
- Udpege mangler i gældende politikker og efterlevelsen af disse
- Rapportere risici og hændelser på en proaktiv måde.

INFORMATIONSSIKKERHEDSUDVALGET

Rolle i sikkerhedsarbejdet

- Informationssikkerhedsudvalget sætter mål for sikkerheden og sørger for, at informationssikkerheden realiseres og efterleves i organisationen. Udvalget har således det daglige ansvar for styring af informationssikkerheden
- Udvalget udformer og beskriver sikkerhedspolitik, organisatoriske rammer, ansvarsfordeling, retningslinjer for kontrol og beredskab mv.
- Endelig er det udvalget, der sikrer, at sikkerhedsarbejdet har ledelsens opbakning
- Formanden (topledelsen) for informationssikkerhedsudvalget godkender oplæg af planlæggelse, procedurer, politikker, mv. udarbejdet af informationssikkerhedsudvalget.

Opgaver i sikkerhedsarbejdet

Informationssikkerhedsudvalget skal bl.a.:

- Sikre, at udvalget har den nødvendige viden om ISO27001, da medlemmernes indsigt i standardens indhold og dækningsområde er væsentligt for sikkerhedsudvalgets arbejde og succes
- Fastlægge organisationens styringsmodel for informationssikkerheden ud fra ISO-principperne
- Sikre, at beslutninger bygger på et afvejet helhedssyn – en balance mellem informationssikkerhed, brugervenlighed og økonomi
- Revidere og ajourføre informationssikkerhedspolitikken med udgangspunkt i den aktuelle risikovurdering for organisationen
- Formidle de trufne beslutninger til organisationen.

DATA OG -SYSTEMEJER

Roller i sikkerhedsarbejdet

- Dataejer har dispositionsret til data og ansvar for behandling af data
- Systemejer har ansvar for informationssikkerheden, for det/de systemer de ”ejer”, herunder ansvaret for at der bliver udarbejdet (detaljerede) procedurer, instrukser og tjeklister inden for rammerne af de sikkerhedsniveauer organisationens topledelse har fastlagt
- Det er ligeledes systemejernes ansvar at føre løbende kontrol med overholdelsen af retningslinjer og procedurer og at sikre vedligeholdelse af overblik af system, herunder processer, interessenter, aktiver, kontrakter etc.

Opgaver i sikkerhedsarbejdet

System- og dataejerne skal:

- Skabe sig et overblik over, hvilke forretningsprocesser systemer og data understøtter. Overblikket bruges til at sikre, at der stilles relevante sikkerhedsmæssige krav med udgangspunkt i organisationens sikkerhedsniveauer. Arbejdet inkluderer at:
  - Klassificere aktiver og specificere sikkerhedsmæssige krav samt godkende anskaffelser og installation af hvert aktiv
  - Give adgang til systemer og data
  - Godkende placering af kritiske aktiver samt udviklings- og hjælpemiljøer
  - Godkende beredskabsplaner og følge op på sikkerhedshændelser
- Systemejer kan delegere rutinemæssige opgaver til en person (entitet), der dagligt holder øje med aktiverne, men systemejeren har stadig det endelige ansvar for systemets informationssikkerhed i hele systemets levetid.

INFORMATIONSSIKKERHEDSKOORDINATOR

Rolle i sikkerhedsarbejdet

- Informationssikkerhedskoordinatoren er organisationens daglige sikkerhedsleder og sekretær for sikkerhedsudvalget
- Ideelt set bør sikkerhedskoordinatoren referere direkte til topledelsen, men uanset den organisatoriske placering er det vigtigt, at koordinatoren har direkte adgang til topledelsen
- Sikkerhedskoordinatorens ansvar og beføjelser præciseres af topledelsen.

Opgaver i sikkerhedsarbejdet

Informationssikkerhedskoordinatoren skal:

- Lede risikovurderinger og komme med forslag til opdatering af informationssikkerhedspolitikken
- Registrere og rapportere kritiske hændelser
- Evaluere og benchmarke organisationens sikkerhed
- Skabe opmærksomhed om informationssikkerhed blandt organisationens medarbejdere
- Indkalde til møder og være sekretær for Informationssikkerhedsudvalget
- Afklare grænsesnit med øvrige politikker i organisationen og vurdere behovet for drøftelse af informationssikkerhedspolitikken i fx teknologi-, samarbejds- og sikkerhedsudvalg.

DATABESKYTTELSESRÅDGIVER (DPO)

Rolle i sikkerhedsarbejdet

- Databeskyttelsesrådgiveren (”data protection officer”/DPO) skal overvåge, at organisationen overholder både lovgivningen og interne politikker ift. beskyttelse af følsomme persondata
- DPO’en involveres i alle spørgsmål vedrørende databeskyttelse og fungerer desuden som kontaktperson for registrerede og databeskyttelsesmyndighederne
- Loven beskriver, at den/de ansvarlige ikke må modtage instruktioner om opgaver og skal rapportere direkte til højeste ledelsesniveau.

Opgaver i sikkerhedsarbejdet

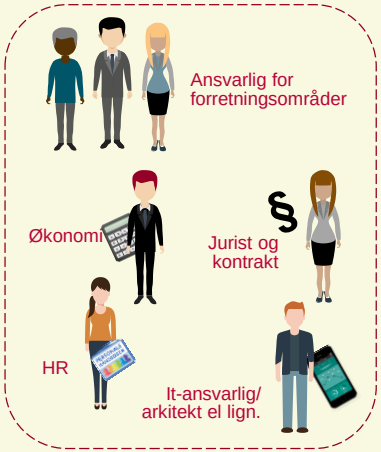
DPO’en skal bl.a.:

- Overvåge, underrette og rådgive organisationen med konsekvensanalyse, implementering og overholdelse af både lovgivningen og interne politikker ift. beskyttelse af følsomme persondata
- Indgå og støtte sikkerhedsudvalget i forvaltningen af interne politikker ift. beskyttelse af personoplysninger, således varetagelsen af følsomme persondata sikres ved kontrakt- og leverandørstyring mv.
- Rådgive om udvikling og vedligeholdelse af intern dokumentation om beskyttelse af personlige oplysninger
- Fungere som kontaktperson for registrerede og databeskyttelsesmyndighederne om både brud på datasikkerheden samt mere generel information omkring rettigheder
- Sikre at Privacy Impact Assessment (PIA) udføres, når det er nødvendigt, og resultatet af disse er implementeret i organisationen.

Informationssikkerhedsrejse
Procesforløb for risikovurdering

Ansvarlige for centrale forretningsområder og støttefunktioner afdækker:

- Hvilke risici der findes på deres område
- Hvilken konsekvens og sandsynlighed
- Hvordan hver risici håndteres



Centrale forretningsområder og støttefunktioner

Sikkerheds-koordinator Rikke udarbejder forslag til at eksekvere risikovurdering

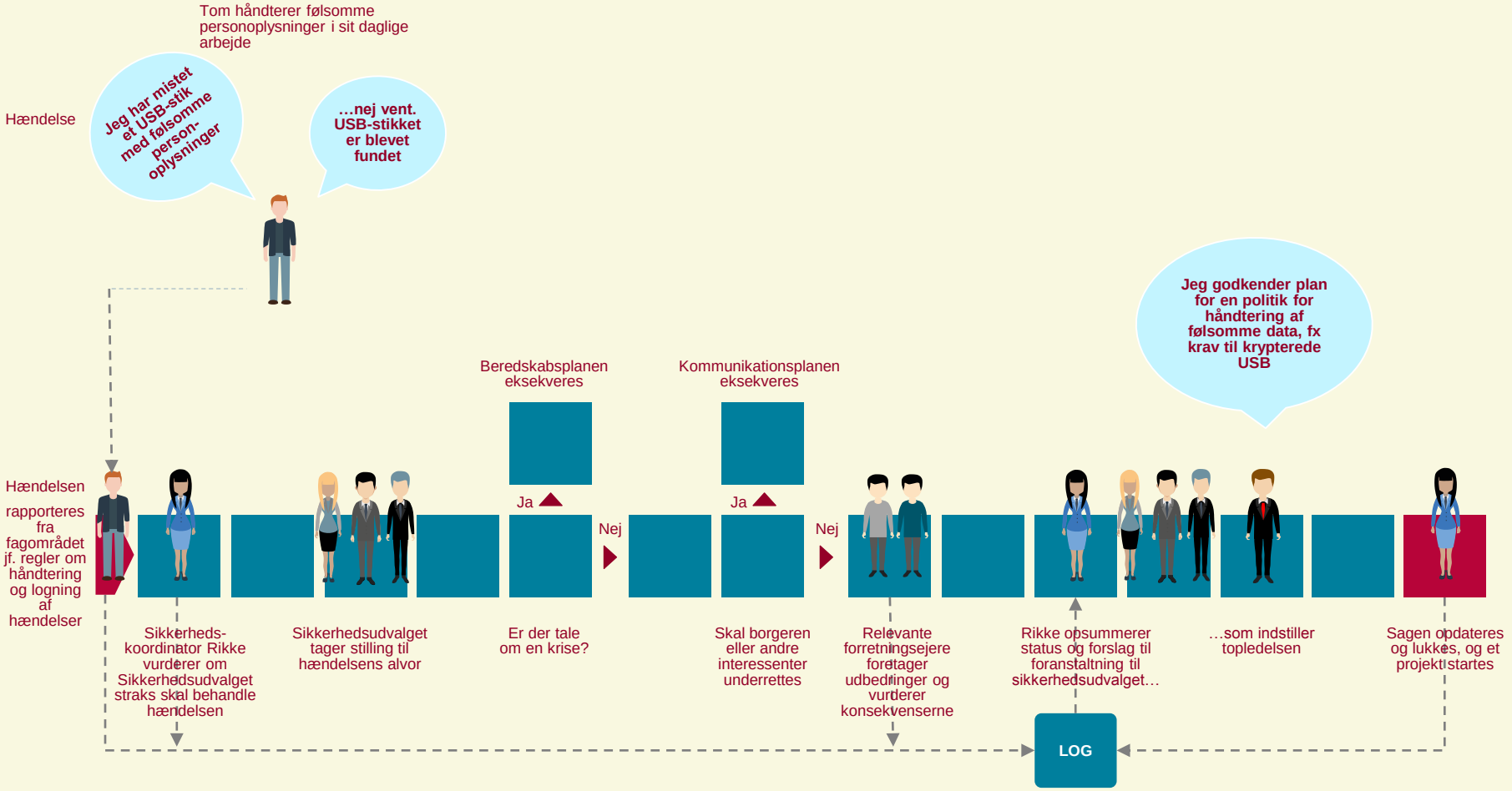
Rikke står for den overordnede koordination af risikovurderingen og risikoanalyse

Rikke opsummerer og dokumenterer risici og kontroller

Rikke eller repræsentant fra informations-sikkerhedsudvalget fremlægger for ledelsen

Rikke følger op og igangsætter aktiviteter

Informationssikkerhedsrejse
Procesforløb for hændelseshåndtering



Informationssikkerhedsrejse
Ny politik for følsomme oplysninger

Ansvarlige for centrale forretningsområde og støttefunktioner:

- Afdækker, hvilke Gaps der findes på deres område
- Vurderer, hvilken konsekvens den nye politik vil have for deres forretningsområde eller støttefunktion, fx budget, processer og opgaver
- Vejleder foranstaltninger og planlæggelse af disse.

Centrale forretningsområder og støttefunktioner

Udarbejder tiltag på hver deres område fx:

It-ansvarlig/arkitekt

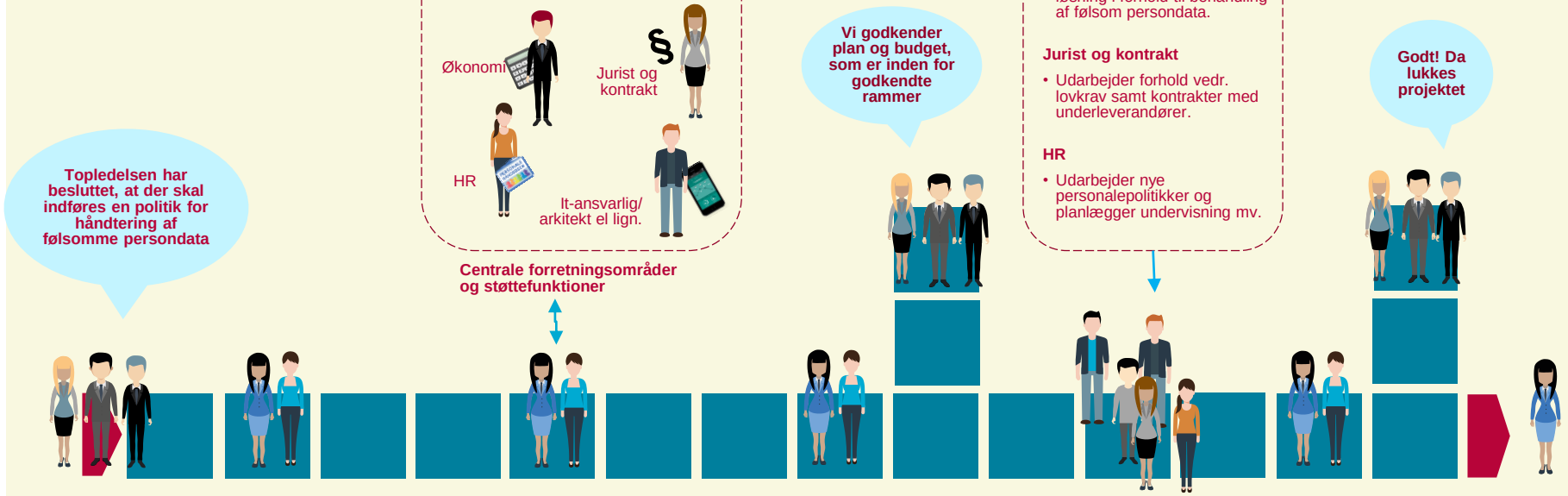
- Implementerer relevant løsning i forhold til behandling af følsom persondata.

Jurist og kontrakt

- Udarbejder forhold vedr. lovkrav samt kontrakter med underleverandører.

HR

- Udarbejder nye personalepolitikker og planlægger undervisning mv.



Informations-sikkerhedsudvalget kommunikerer topledelsens beslutning

En projektleder (som kan være Rikke eller anden person) allokeres

Projektlederen gennemfør en gapanalyse sammen med relevante mellemledere (DPO) og udarbejder en plan for implementering

Projektlederen fremlægger plan inklusive budget og ressourcer for informations-sikkerhedsudvalget

De relevante mellemledere sikrer implementering

Projektledere følger op på status af implementering og informerer ledelsen

Projektet afsluttes og Rikke planlægger aktiviteter for måling af effektivitet, fx audit

TVÆRGÅENDE ROLLER OG AKTIVITETER I INFORMATIONSSIKKERHEDSARBEJDET

	Informations-sikkerheds-udvalget	Informations sikkerheds-koordinator	Systemejere	Dataejere	DPO	Jura/kontrakt	HR	It-ansvarlig/ arkitekt	Økonomi
Skaber forretnings-overblik	Sikrer det nødvendige forretningsoverblik	Overordnet koordination	Systemer, inventar, interessenter og processer	Data, interessenter og processer	Data som beskyttes, teknologi, standarder	Lovgivning, Indkøbsproces, interessenter til indkøb	Ansættelses-processer, -vilkår og aktiver	It-arkitektur, interessenter, andre lovgivninger og standarder	Budget og investeringer
Rolle i udarbejdelsen af politikker/ instrukser	Godkender overordnede politikker	Udarbejder forslag til overordnede politikker	Udarbejder brugerinstrukser	Ansvarlig for dataadgang	Overholdelse af databeskyttelse	Ansvarlig for indkøbspolitikker og ansættelsesvilkår	Ansvarlig for ansættelses-kontrakter og HR-politikker	Sikrer, at it-arkitekturen støtter mål og politikker	Vurderer budgetmæssige konsekvenser
Rolle i leverandørstyring	Godkender anvendelsen af leverandører og fastlægger omfang for tilsyn	Supporterer efter behov	Identificerer nye leverandørkrav	Identificerer nye leverandørkrav	Overholdelse af databehandler-aftale	Opdaterer kontrakter	N/A	Opdaterer indkøbsstrategien	Vurderer budgetmæssige konsekvenser
Rolle i hændelses-håndtering	Godkender rapportering og proces for håndtering af hændelser	Procesejere for rapportering og håndtering af hændelser	Rapporterer hændelser på eget område	Rapporterer hændelser på eget område	Underrette ved hændelser for følsomme persondata	Kommerciel beskyttelse v. hændelser	Håndterer kommunikation til medarbejdere og eksterne	Rapporterer hændelser på eget område	Vurderer økonomiske konsekvenser
Rolle i beredskabs-planlægningen	Godkender beredskabsplaner	Procesejere og koordinator	Beredskabsplan for system tilgængelighed	Beredskabsplan for datatilgængelighed	Beredskabsplan for databeskyttelse	Beredskabsplan for juridisk beskyttelse	Beredskabsplan for HR-relaterede	Beredskabsplan for it-arkitekturen	Vurderer budgetmæssige konsekvenser
Rolle i sikring af awareness og uddannelse	Godkender awareness-planen	Sikrer, at awareness-plan findes og eksekveres	Afdækker behov for uddannelse og oplysning på eget område	Afdækker behov for uddannelse og oplysning på eget område	Afdækker behov for uddannelse og oplysning på eget område	Afdækker behov for uddannelse og oplysning på eget område	Koordinering og plan for uddannelse og oplysning	Afdækker behov for uddannelse og oplysning på eget område	Ansvarlig for budgettet for uddannelse
Rolle i opdatering af risikovurdering og SoA	Godkender SOA-dokumentet og risikovurdering	Opdaterer dokumenterne	Giver input inden for eget område	Giver input inden for eget område	Giver input inden for eget område	Giver input inden for eget område	Giver input inden for eget område	Giver input inden for eget område	Vurderer økonomiske konsekvenser
Rolle i planlægning af sikkerheds-aktiviteter	Godkender planer for sikkerheds-aktiviteter	Procesejere for årshjul og målings-aktiviteter	Planlægger systemtest	Planlægger audits	Planlægger test af databeskyttelses-niveauet	Planlægger revurderings-processen for leverandør-kontrakter	Ansvarlig for beredskabstræning, videreuddannelse osv.	Planlægger tests-arkitekturområdet	Budgetansvarlig

FORVENTET OUTPUT FRA INFORMATIONSSIKKERHEDSARBEJDET

	Definering af processer og principper	Implementering af principper	Eksekvering som konsekvens af principper	Evaluering af efterlevelse af effektivitet (evaluering og opfølgning)
Forretningsoverblik og informations-sikkerheds-ledelsessystem	Der er et dokumenteret overblik over organisationen samt dens kontekst og interessenter	Informationssikkerhedsledelses-systemet er afledt af et aktuelt forretningsoverblik	Roller, ansvar og opgaver er defineret med udgangspunkt i forretningsoverblikket	Forretningsoverblikket revurderes en gang om året og i forbindelse med større ændringer
Politikker/instrukser	Overordnede politikker og mål for informationssikkerhed er beskrevet	Overordnede politikker og mål er kommunikerede til organisationen	Politikkerne er forankrede i instrukser, kontrakter, det daglige arbejde, processer, osv.	Politikkerne revurderes en gang om året og i forbindelse med større ændringer
Leverandørstyring	Der er beskrevet en proces for leverandørstyring	De valgte kontroller og leverandørkrav er opdaterede i forhold til det nyeste risikobillede	Der følges op på om leverandørerne kan dokumentere deres kapabilitet	Leverandørernes produkter testes og det verificeres, at de efterlever relevante krav
Hændelses-håndtering	Der er beskrevet en proces for hændelseshåndtering	Hændelser bliver rapporteret via faste kanaler	Rapporterede hændelser bliver vurderet og behandlet inden for en acceptabel tidsramme	Effektiviteten af processen bliver målt i opnået læring (fx øget antal af hændelsesrapporteringer)
Beredskabsplan	Der er beskrevet en proces for planlægningen og styringen af beredskabet	Der er etableret beredskabsplaner	Medarbejdere, leverandører og interessenter har modtaget undervisning i beredskabsplanen	Effektiviteten af beredskabet bliver testet
Awareness og uddannelse	Der er beskrevet et awareness-program	Uddannelse og kommunikation eksekveres i overensstemmelse med planen	Opdateringer til awareness-programmet sker i overensstemmelse med de evt. ændrede behov	Effektiviteten af awareness-program bliver verificeret
Opdatering af risikovurdering og SoA	Der er beskrevet en proces for risikovurderinger	Risikovurderinger gennemføres i henhold til processen og risici	Risikoejere følger op på handleplaner, der er afledt af risikovurderingerne	Effektiviteten af kontroller bliver verificeret
Planer for sikkerheds-aktiviteter	Der er bekrevet en proces for måling af informationssikkerheden	Målinger gennemføres i henhold til processen	Handleplaner bliver eksekveret baseret på identificerede mangler	Effektiviteten af kontroller bliver verificeret

ALMENDELIGE FORBEDRINGSMULIGHEDER I INFORMATIONSIKKERHEDSARBEJDET

	Definering af processer og principper	Implementering af principper	Eksekvering som konsekvens af principper	Evaluering af efterlevelse af effektivitet
Forretningsoverblik	Der er et dokumenteret overblik over organisationen, dens kontekst og interessenter	Informationssikkerhedsledelses-systemet er afledt af et aktuelt forretningsoverblik	Roller, ansvar og opgaver er defineret med udgangspunkt i forretningsoverblikket	Forretningsoverblikket revurderes en gang om året og i forbindelse med større ændringer
Politikker/instrukser	Overordnede politikker og mål for informationssikkerhed er beskrevet	Overordnede politikker og mål er kommunikeret til organisationen	Politikkerne er forankrede i instrukser, kontrakter, det daglige arbejde, processer, osv.	Politikkerne revurderes en gang om året og i forbindelse med større ændringer
Leverandørstyring	Der er beskrevet en proces for leverandørstyring	De valgte kontroller og leverandørkrav er opdaterede i forhold til det nyeste risikobillede	Der følges op på leverandørerne kan dokumentere deres kapabilitet	Leverandørernes produkter testes og det verificeres, at de efterlever relevante krav
Hændelses-håndtering	Der er beskrevet en proces for hændelseshåndtering	Hændelser bliver rapporteret via faste kanaler	Rapporterede hændelser bliver vurderet og behandlet inden for en acceptabel tidsramme	Effektiviteten af processen bliver målt i opnået læring (fx øget antal af hændelsesrapporteringer)
Beredskabsplan	Der er beskrevet en proces for planlægningen og styringen af beredskabet	Der er etableret beredskabsplaner	Medarbejdere, leverandører og interessenter har modtaget undervisning i beredskabsplanen	Effektiviteten af beredskabet er blevet testet
Awareness og uddannelse	Der er beskrevet et awareness-program	Uddannelse og kommunikation eksekveres i overensstemmelse med planen	Opdateringer til awareness-programmet er sket i overensstemmelse med de evt. ændrede behov	Effektiviteten af awareness-program er blevet vurderet
Opdatering af risikovurdering og SoA	Der er beskrevet en proces for risikovurderinger	Risikovurderinger gennemføres i henhold til processen og risici	Risikoejere følger op på handleplaner, der er afledt af risikovurderingerne	Effektiviteten af kontroller er blevet verificeret
Planer for sikkerheds-aktiviteter	Der er beskrevet en proces for måling af informationssikkerheden	Målinger gennemføres i henhold til processen	Handleplaner bliver eksekveret baseret på identificerede mangler	Planer for sikkerhedssaktiviteter er blevet opdateret

RAPPORT

Version: x

Dato: DD.MM.YY

Status på Informationssikkerhedsarbejdet

Definering	Implementering	Eksekvering	Evaluering
			
[Kommentarer]	[Kommentarer]	[Kommentarer]	[Kommentarer]

	Definering af processer og principper	Implementering af principper	Eksekvering som konsekvens af principper	Evaluering af efterlevelse of effektivitet (løbende eller årlig evaluering og opfølgning)
Forretningsoverblik og styring af den organisatoriske informations-sikkerhed	Der er et dokumenteret overblik over organisationen samt dens kontekst og interessenter	Ledelse/styring af informationssikkerhed er afledt af det aktuelle forretningsoverblik	Roller, ansvar og opgaver er defineret med udgangspunkt i forretningsoverblikket	Forretningsoverblikket revurderes en gang om året og i forbindelse med større ændringer
Politikker/instrukser	Overordnede politikker og mål for informationssikkerhed er beskrevet	Overordnede politikker og mål er kommunikerede til organisationen	Politikkerne er forankrede i instrukser, kontrakter, det daglige arbejde, processer, osv.	Politikkerne revurderes en gang om året og i forbindelse med større ændringer
Leverandørstyring	Der er beskrevet en proces for leverandørstyring	De valgte kontroller og leverandørkrav er opdaterede i forhold til det nyeste risikobillede	Der følges op på om leverandørerne kan dokumentere serviceleverancer	Leverandørernes serviceleverancer testes, og det verificeres en gang om året, at de efterlever relevante krav
Hændelses-håndtering	Der er beskrevet en proces for hændelseshåndtering	Hændelser bliver rapporteret via faste kanaler	Rapporterede hændelser bliver vurderet og behandlet inden for en acceptabel tidsramme	Effektiviteten af processen bliver målt i opnået læring (fx øget antal af hændelsesrapporteringer)
Beredskabsplan	Der er beskrevet en proces for planlægningen og styringen af beredskabet	Der er etableret beredskabsplaner	Medarbejdere, leverandører og interessenter har modtaget undervisning i beredskabsplanen	Effektiviteten af beredskabet testes og plan ajourføres en gang årligt
Awareness og uddannelse	Der er beskrevet et program for awareness	Uddannelse og kommunikation eksekveres i overensstemmelse med planen	Opdateringer til awareness-programmet sker i overensstemmelse med de evt. ændrede behov	Effektiviteten af awareness bliver målt i opnået adfærdsændring en gang årligt
Opdatering af risikovurdering og SoA	Der er beskrevet en proces for risikovurderinger	Risikovurderinger gennemføres i henhold til processen og risici	Risikoejere følger op på handleplaner, der er afledt af risikovurderingerne	Risikovurdering og SoA gennemgås og ajourføres en gang årligt
Planer for sikkerheds-aktiviteter	Der er bekrevet en proces for måling af informationssikkerheden	Målinger gennemføres i henhold til processen	Handleplaner bliver eksekveret baseret på identificerede mangler	Effektiviteten af kontroller er blevet verificeret
STATUS				

FOKUS PÅ KULTUR OG RAMMEVÆRK ER AFSÆTTET FOR INFORMATIONSSIKKERHED