Årshjul

Formål

For at styre informationssikkerheden og for at sikre, at ledelsen har de rette styringsværktøjer, gentages en række aktiviteter løbende år efter år, men andre er enkeltstående aktiviteter.
Aktiviteter, der gentages, placeres i et årshjul med det formål at illustrere årets aktiviteter simpelt og overskueligt.
Enkeltstående aktiviteter, der kan variere hen over årene, beskrives i en årsplan.
De enkeltstående aktiviteter i en årsplan kan eksempelvis være:

- planlægning af hvilke områder, der skal gennemføres risikovurderinger på og gennemførsel af disse
- planlægning og gennemførsel af awareness kampagner/uddannelse
- gennemførsel af udbedringer afledt af sikkerhedshændelser

Kort sagt beskrives og planlægges mange af de opgaver, der efterfølgende kontrolleres/følges op på i årshjulet, i årsplanen.

Årshjulet indeholder aktiviteter, der skal gentages med passende intervaller. De er ikke i sig selv en sikkerhedsforanstaltning, men er ofte aktiviteter, der har karakter af opfølgning/evaluering, kontrol og rapportering, Det er alle aktiviteter, der skal sikre, at den gennemførte indsats er tilstrækkelig.
Det vil ofte være gennem disse aktiviteter, at der kan identificeres forbedringspotentialer og dermed fødes opgaver til årsplanen.

Forudsætninger for at årshjulet kan anvendes

For at kunne udføre årshjulets aktiviteter, der handler om opfølgning/evaluering og kontrol, er der en række forudsætninger, der skal være på plads. Hermed menes at det materiale, der kontrolleres og følges op på, selvfølgelig skal være til stede.
Årshjulet beskriver ikke etableringen af materialet, da dette forudsættes at være til stede.

Der skal være beskrevet procedurer, der sikrer, at der indhentes samtykke, at slettefrister overholdes og at sikkerhedshændelser håndteres. Der skal findes en sikkerhedspolitik, sikkerhedshåndbog og en beredskabsplan. Der skal være gennemført risikovurderinger på de vigtigste forretningsprocesser og de tilhørende it-systemer. Dette er blot eksempler på materiale, der forudsættes at være tilstede.
Kort sagt ligger der et stort arbejde forud for årshjulet med at sikre, at der findes processer, håndbøger, regler og retningslinjer som efterleves i organisationen og dermed sikrer, at der findes materiale at kontroller og følge op på.

Læsevejledning

Nedenfor er der givet forslag til en række opgaver, der kan indgå i et årshjul samt et forslag til hyppighed for opgaven.

Opgaverne vises dels i en oversigt, hvor formålet med den enkelte opgave er angivet og hvor der er mulighed for at dokumentere resultatet, samt i en grafisk udgave, hvor opgaverne er vist i kvartalsoversigter.

Opgaverne er opdelt i tre typer

- Opfølgning på dokumentation, beslutninger, risikovurderinger, awareness m.v. med det formål at vurdere, om der skal ske en opdatering
- Kontrol af brugerrettigheder, logninger, databehandlere, revision m.v.
- Rapportering til informationssikkerhedsudvalget og direktionen

Hyppigheden er angivet til årligt, halvårligt eller kvartårligt valgt ud fra opgavens kritikalitet ift. informationssikkerheden.
Jo mere kritisk en opfølgning er for informationssikkerheden, jo hyppigere vil opgaven skulle foretages.

Frekvens	Type	Opgave	Formål med opgaven	Opfølgning
Årligt	Kontrol	Tilsyn med databehandlere	Der skal ske tilsyn med databehandlere. Kan eventuelt ske gennem en fyldestgørende revisionserklæring.	
Årlig	Kontrol	It-revision	Ekstern revision at it-sikkerhed	
Årligt	Kontrol	Test af beredskab for informationssikkerhed	Beredskab for informationssikkerhed bør testes minimum en gang årligt, så beredskabsplanen validitet afprøves	
Årlig	Kontrol	Intern audit	Er sikkerhedsforanstaltningerne i overensstemmelse med sikkerhedspolitikken, er der indgået databehandleraftaler, er de eksisterende risikovurderinger tilstrækkelige, fungerer de beskrevne kontroller?	
Årligt	Kontrol	Måling af sikkerhedsniveau - julequiz/sikkerhedsmåling	Vurdering af viden om informations-sikkerhed og GDPR krav hos medarbejderne	

Frekvens	Type	Opgave	Formål med opgaven	Opfølgning
Årligt	Rapportering	Ledelsesmæssig rapportering til direktionen	Topledelsen skal overveje og betragte igangværende tiltag og resultater for informationssikkerhed	
Årligt	Rapportering	DPO-rapportering til kommunal-bestyrelsen på GDPR efterlevelse	Opfølgning på opfyldelse af GDPR krav	
Årligt	Opfølgning	Revision af informationssikkerhedspolitik	Er informationssikkerhedspolitikken stadig dækkende eller skal den revideres?	
Årligt	Opfølgning	Revision af it-sikkerhedshåndbogen	Er it-sikkerhedshåndbogen dækkende eller skal den revideres?	
Årligt	Opfølgning	Revision af beredskabsplaner	Beredskabsplan skal revideres ift. indhøstede erfaringer. Sker typisk efter en beredskabstest	
Årligt	Opfølgning	Opfølgning på databehandleraftaler	Er de eksisterende databehandleraftaler gyldige og fyldestgørende?	
Årligt	Opfølgning	Opfølgning på at slettefristen, som er dokumenteret i KLE, overholdes	Opfyldelse af GDPR krav	
Årligt	Opfølgning	Opfølgning på samtykke	Opfyldelse af GDPR krav. Opfølgning på eksisterende dokumentation af samtykke. Eventuel stikprøvekontrol på at der findes samtykke, hvor der ikke er hjemmel til behandling.	
Årligt	Opfølgning	Opfølgning på at de registreredes rettigheder	Opfyldelse af GDPR krav. Opfølgning på at oplysningspligt, ret til indsigt, berigtigelse og sletning kan opfyldes	
Årligt	Opfølgning	Opfølgning på om der er hjemmel til de behandlinger, der foretages	Opfyldelse af GDPR krav. Opfølgning på eksisterende dokumentation, der er udfærdiget på en given behandling jævnfør fortegnelserne. Der bør tages udgangspunkt i en risikobaseret vurdering, dvs. dem der har den højeste risiko også er dem, der gennemgås.	
Årligt	Opfølgning	Opfølgning på eventuelle udarbejdede konsekvensanalyser (DPIA)	Opfyldelse af GDPR krav. DPIA skal kun udarbejdes, hvis kommunen selv udvikler nye løsninger, der opfylder Datatilsynets krav til, hvornår en DPIA skal udarbejdes.	
Årligt	Kontrol	Stikprøver på brugernes anvendelse af ikke følsomme personoplysninger	Opfyldelse af GDPR krav. Kan ske via logningsgennemgang	

Frekvens	Type	Opgave	Formål med opgaven	Opfølgning
Halvårligt	Kontrol	Stikprøver på brugernes anvendelse af følsomme personoplysninger	Opfyldelse af GDPR krav. Kan ske via logningsgennemgang	
Halvårligt	Opfølgning	Opfølgning på brugerrettigheder til systemer med ikke følsomme personoplysninger	Opfyldelse af GDPR krav	
Halvårligt	Opfølgning	Opdatering af trusselsbilledet og mulige forbedringer	Det beskrevne trusselsbillede vurderes og eventuelle forbedringer i risikovurderingerne beskrives	
Halvårligt	Opfølgning	Opfølgning på risikovurderinger	Findes de nødvendige risikovurderinger, er de stadig gældende og er de ajourførte ift. det aktuelle trusselsbillede	
Halvårligt	Opfølgning	Opfølgning på kontroller (SOA dokument)	Gennemføres de besluttede kontroller og er de tilstrækkelige	
Halvårligt	Opfølgning	Opfølgning på administratorrettigheder	Sikring af at kun relevante medarbejdere har administratorrettigheder	
Halvårligt	Opfølgning	Awareness kampagne/uddannelse målrettet faggrupper	Er planlagte kampagner/uddannelse gennemført? Skal noget ændres og hvad er planen for det kommende halvår?	
Halvårligt	Opfølgning	Opfølgning på fortegnelse over behandlingsaktiviteter	Opfyldelse af GDPR krav	
Kvartårligt	Opfølgning	Opfølgning på hændelser	Ud fra loggen over hændelsen følges der op på, hvilken type hændelser der er sket i perioden - omfang, type, konsekvens. Herunder status på udbedring og forebyggende foranstaltninger. Er der besluttet forebyggende foranstaltninger og er de påført årsplanen.	
Kvartårlig	Opfølgning	Opfølgning på årsplan for sikkerhedsaktiviteter	Er sidste kvartals aktiviteter gennemført i henhold til planen og skal planen opdateres?	
Kvartårligt	Opfølgning	Opfølgning på brugerrettigheder til systemer med følsomme personoplysninger	Opfyldelse af GDPR krav	
Kvartårlig	Rapportering	Sikkerhedskoordinatoren rapporterer til informations-sikkerhedsudvalget		

1. kvartal

Opfølgning		Kontroller	Hyppighed		Rapportering	Hyppighed
	Januar			Januar		
Opfølgning på samtykke		Revision af informationssikkerhedspolitik	Årligt			
Opfølgning på at slettefristen, som er dokumenteret i KLE, overholdes						
Opfølgning på at de registreredes rettigheder (oplysningspligt, ret til indsigt, berigtigelse og sletning) kan opfyldes						
	Februar			Februar		
Opfølgning på administratorrettigheder		Revision af it-sikkerhedshåndbogen	Årligt		Sikkerhedskoordinatoren rapporterer til informations-sikkerhedsudvalget	Kvartårligt
		Gennemgang af brugerrettigheder til systemer med følsomme personoplysninger	Kvartårligt			
	Marts			Marts		
Opdatering af trusselsbilledet og mulige forbedringer						

2.kvartal

Opfølgning		Kontroller	Hyppighed		Rapportering	Hyppighed
	April			April		
Opfølgning på risikovurderinger		Gennemgang af databehandleraftaler	Årligt			
Opfølgning på kontroller (SOA dokument)		Tilsyn med databehandlere , herunder indhentning af revisorerklæringer	Årligt			
	Maj			Maj		
Awarenesskampagne/ uddannelse/kurser målrettet faggrupper		Intern audit	Årligt		Sikkerhedskoordinatoren rapporterer til informations-sikkerhedsudvalget	Kvartårligt
Opfølgning på fortegnelse over behandlingsaktiviteter		Gennemgang af brugerrettigheder til systemer med følsomme personoplysninger	Kvartårligt			
	Juni			Juni		
Opfølgning på hændelser		Stikprøver af brugernes anvendelse af følsomme personoplysninger (logningsgennemgang)	Halvårligt			
Opfølgning på handlingsplan for sikkerhedsaktiviteter						

3. kvartal

Opfølgning	Kontroller	Hyppighed	Rapportering	Hyppighed
Juli			Juli	
August			August	
Opfølgning på administratorrettigheder	Gennemgang af bruger-rettigheder til systemer med følsomme personoplysninger	Kvartårligt	Sikkerhedskoordinatoren rapporterer til informations-sikkerhedsudvalget	Kvartårligt
September			September	
Opdatering af trusselsbilledet og mulige forbedringer	Test af beredskab for informationssikkerhed	Årligt		
	Revision af beredskabsplaner	Årligt		

4.kvartal

Opfølgning		Kontroller	Hyppighed		Rapportering	Hyppighed
	Oktober			Oktober		
Opfølgning på risikovurderinger		It-revision	Årlig			
Opfølgning på kontroller (SOA dokument)						
	November			November		
Awarenesskampagne/ uddannelse målrettet faggrupper		Gennemgang af bruger-rettigheder til systemer med følsomme personoplysninger	Kvartårligt		Sikkerhedskoordinatoren rapporterer til informations-sikkerhedsudvalget	Kvartårligt
Opfølgning på fortegnelse over behandlingsaktiviteter						
	December			December		
DPO-rapport på GDPR efterlevelse		Måling af sikkerhedsniveau - julequiz/sikkerhedsmåling	Årligt		Ledelsesmæssig rapportering til direktionen	Årligt
Opfølgning på evt. udarbejdede konsekvensanalyser (DPIA)		Stikprøver af brugernes anvendelse af følsomme personoplysninger (logningsgennemgang)	Halvårligt			