Spørreskjema om informasjonssikkerhet

Vi gjennomfører en evaluering av arbeidet med informasjonssikkerhet i statsforvaltningen og trenger svar fra deg som er leder av virksomheten.

Om respondenten

Virksomhetens navn:

Hvem svarer på undersøkelsen:	
Alternativ	**Sett kryss**
Virksomhetsleder (direktør)	
Andre (angi rolle):	

Kontaktinformasjon for eventuell oppfølging av undersøkelsen:	
Navn	
E-post	
Telefonnummer	

Del 1 – styring og kontroll på informasjonssikkerhetsområdet

1. I hvilken grad har virksomhetsleder gitt tydelige føringer for roller og ansvar i informasjonssikkerhetsarbeidet i virksomheten? **79**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	**0**	**18**	**61**	**0**	**0**
Gi gjerne noen eksempler på hvordan det er gitt tydelige føringer:					

2. I hvilken grad har virksomhetsleder gitt tydelige føringer for innholdet i de systematiske aktivitetene for styring og kontroll av informasjonssikkerhet? **78**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	**5**	**32**	**41**	**0**	**0**

Forklaring til spørsmål:
I informasjonssikkerhetsarbeidet kan disse aktivitetene være:

- ledelsens styring og oppfølging
- vurdering og håndtering av risiko
- måling, evaluering og revisjon
- overvåking og hendelseshåndtering
- kompetanse- og kulturutvikling

3. Hvem har det formelle ansvaret for å vurdere og håndtere risiko innen informasjonssikkerhet? **79**

Alternativ	Sett kryss (bare ett kryss)	
Ledere og mellomledere, som ledd i ordinær linjeledelse	**66**	**To kryss: 2**
Egen gruppe, fagansvarlig informasjonssikkerhet, eller lignende	**11**	

Forklaring til spørsmål:

Dersom det formelle ansvaret for beslutninger om informasjonssikkerhetsrisiko er en del av ledelsesansvaret for de ordinære virksomhetsprosessene, velger du det første alternativet.

Dersom det formelle ansvaret for beslutninger om informasjonssikkerhetsrisiko tas av spesialfunksjoner eller andre, velger du det andre alternativet.

Vær oppmerksom på at ledere med ansvar for styring av risiko kan få støtte av spesialfunksjoner og fagpersoner, uten at de mister ansvaret for beslutninger om risiko.

4. I hvilken grad er ressurser til arbeid med styring og kontroll og sikkerhetstiltak synliggjort i budsjetter og virksomhetsplaner? **79**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
3	**10**	**35**	**31**	**0**	**0**

Gi gjerne noen eksempler på hvordan arbeidet synliggjøres:

Forklaring til spørsmål:
Eksempel på ressurser er stillinger og budsjettmidler til

- gjennomføring av de systematiske aktivitetene for styring og kontroll (jf. spørsmål 2)
- iverksettelse og forvaltning av alle sikkerhetstiltak det er behov for

5. I hvilken grad ser virksomheten styring av informasjonssikkerhet i sammenheng med den øvrige risikostyringen i virksomheten? **79**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
0	**7**	**31**	**41**	**0**	**0**

Forklaring til spørsmål:
Her ønsker vi å få en forståelse av om virksomheten arbeider helhetlig med risikostyring. Eksempler på andre områder er for eksempel økonomistyring, HMS, personvern og virksomhetsstyring.

Del 2 – Beredskap, øvelser og hendelseshåndtering

6. I hvilken grad arbeider virksomheten systematisk med øvelser på informasjonssikkerhetsområdet? **79**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
6	**18**	**28**	**24**	**1**	**2**

Forklaring til spørsmål:
Øvelser på informasjonssikkerhetsområdet omfatter å trene på håndtering av hendelser som rammer digitale tjenester, IKT-infrastruktur eller andre utfordringer relatert til informasjonssikkerhet

7. Har virksomheten en IKT-beredskapsplan som er godkjent av virksomhetslederen? **78**

Ja	Nei	Vet ikke
54	**21**	**3**
Forklaring til spørsmål: Med IKT-beredskapsplan mener vi planer for etablering av midlertidige tiltak og håndtering av blant annet informasjonssikkerhetshendelser.		

8. Virksomhetens håndtering av informasjonssikkerhetshendelser er basert på at: **79**

Svar	Sett kryss
Virksomheten har tydelig definerte roller, ansvar og prosedyrer for hvordan hendelser skal håndteres.	**69**
Virksomheten har **ikke** tydelig definerte roller, ansvar og prosedyrer. Metoden for håndtering blir bestemt ved hver enkelt hendelse.	**10**
Forklaring til spørsmål: Informasjonssikkerhet handler om å sikre at informasjonen: • ikke blir kjent for uvedkommende (konfidensialitet) • ikke blir endret utilsiktet eller av uvedkommende (integritet) • er tilgjengelig ved behov (tilgjengelighet) Informasjonssikkerhetshendelser er i denne sammenheng uønskede hendelser som kan påvirke, eller har påvirket, konfidensialitet, integritet eller tilgjengelighet på informasjon.	

9. Benyttes erfaringene fra hendelseshåndteringen til kontinuerlig forbedring av informasjonssikkerhetsarbeidet? **78**

Ja	Nei	Vet ikke
70	**3**	**5**
Forklaring til spørsmål: Eksempler på oppgaver og områder som kan forbedres ved hjelp av resultatet fra hendelseshåndteringen er risikovurderinger, sikkerhetstiltak og kompetanseheving.		

10. I hvilken grad har virksomheten oversikt over kostnadene som følge av informasjonssikkerhetshendelser? **78**

I ingen grad	I liten grad	I moderat grad	I stor grad	Ikke relevant	Vet ikke
3	**28**	**27**	**11**	**9**	**0**

Forklaring til spørsmål:
Informasjonssikkerhetshendelser er i denne sammenheng uønskede hendelser som kan påvirke, eller har påvirket, konfidensialitet, integritet eller tilgjengelighet på informasjon.

Informasjonssikkerhet handler om å sikre at informasjonen

- ikke blir kjent for uvedkommende (konfidensialitet)
- ikke blir endret utilsiktet eller av uvedkommende (integritet)
- er tilgjengelig ved behov (tilgjengelighet)

Del 3 - Nasjonale felleskomponenter

11. Har virksomheten vurdert om den er avhengig av nasjonale felleskomponenter? **78**

Ja	Nei	Vet ikke
69	**5**	**4**

Forklaring til spørsmål:

Virksomheten er avhengig av en felleskomponent hvis måloppnåelsen blir påvirket dersom felleskomponenten ikke er tilgjengelig.

Dette er de nasjonale felleskomponentene og deres forvaltere:

- ID-porten (Difi)
- Altinn (Brønnøysundregistrene)
- Digital postkasse til innbyggere (Difi)
- Kontakt- og reservasjonsregisteret (Difi)
- Det sentrale folkeregisteret (Skatteetaten)
- Enhetsregisteret (Brønnøysundregistrene)
- Matrikkelen (Statens kartverk)

Del 4 – Sikkerhetskultur og kompetanse

12. Har ledelsen kartlagt eller målt sikkerhetskultur i egen virksomhet i løpet av de siste tre årene? **77**

Ja	Nei	Vet ikke
31	**43**	**3**
Hvordan vurderer du sikkerhetskulturen i virksomheten din:		
Forklaring til spørsmål: Den enkeltes kunnskap, adferd og holdninger er en del av organisasjonens kultur. Den enkeltes kunnskap, adferd og holdninger til informasjonssikkerhet vil være en del av dette – en del av virksomhetens sikkerhetskultur.		

13. Har virksomhetsledelsen i løpet av 2017 tatt initiativ til at det blir gjennomført tiltak for å styrke sikkerhetskulturen i virksomheten for noen av disse gruppene? **78**

For alle ansatte	For grupper av ansatte	For ledergruppen	Ikke gjennomført tiltak	Ikke relevant	Vet ikke
29	**7**	**1**	**7**	**0**	**0**
5	**5**		**To kryss**		
	4	**4**			
10		**10**			
15	**15**	**15**	**Tre kryss**		
59	**31**	**30**	**Totalt**		
Gi ett eller flere eksempler på tiltak som er gjennomført og virkemidler som er benyttet:					

Del 5 - Etatsstyringsdialogen

14. Har informasjonssikkerhet vært et eget tema i etatsstyringsdialogen i 2017? **78**

Ja	Nei	Vet ikke
50	**19**	**9**

15. Vil informasjonssikkerhet bli omtalt i årsrapporten for 2017? **76**

Ja, som eget tema (sett kryss)	Ja, under et annet tema (angi tema)	Blir ikke omtalt i årsrapporten (sett kryss)
47	**23**	**5**
1	**1**	**To kryss**

Har du noen ytterligere kommentarer til • deres arbeid med informasjonssikkerhet i virksomheten • arbeidet med informasjonssikkerhet i statsforvaltningen • informasjonssikkerhetsarbeid du ønsker å synliggjøre som du er spesielt fornøyd med • annet

Tusen takk for ditt bidrag til undersøkelsen!