Spørsmål ved revisjon

Informasjonssikkerhet – kapittel 6

…… AS

00.00.2019

MERKNAD:

Tilsynslaget fra NVE ønsker at deltagere fra virksomheten skal være forberedt på spørsmålene som blir stilt under tilsynet.

Spørsmålslisten er ikke uttømmende. NVE forbeholder seg retten til å endre på rekkefølge og formuleringer, unnlate å stille enkelte spørsmål, og stille tilleggsspørsmål.

NVE ber om at spørsmålene gjennomgås internt før tilsynsdagen, slik at svarene blir mest mulig presise. Svar på spørsmål skal ikke fremlegges skriftlig for NVE. Denne forberedelse er kun ment å danne best mulig grunnlag for samtalen mellom virksomheten og NVE.

Identifikasjon og beskyttelse av kraftsensitiv informasjon

- *§ 6-1.Identifisering av kraftsensitiv informasjon og rettmessige brukere*
- *§ 6-3.Beskyttelse, avskjerming og tilgangskontroll*

§ 6-1. ***Identifisering av kraftsensitiv informasjon og rettmessige brukere***	
KBO-enheter skal etter energiloven § 9-3 første ledd identifisere hva som er kraftsensitiv informasjon, hvor denne befinner seg og hvem som har tilgang til den. *Identifiseringen av hva som er kraftsensitiv informasjon og hvor denne befinner seg, skal omfatte oppbevaring på papir, lagring i elektronisk form eller lagring på annen måte.* *Med rettmessig bruker menes fysiske eller juridiske personer som har tjenstlig behov for kraftsensitiv informasjon. Den enkelte KBO-enhet skal selv avgjøre hvem som har tjenstlig behov for kraftsensitiv informasjon innenfor sin virksomhet.* *Den enkelte KBO-enhet kan avgjøre om det er tjenstlig behov for å videreformidle kraftsensitiv informasjon til andre utenfor egen virksomhet. Den som har fått tilgang til kraftsensitiv informasjon av en KBO-enhet kan ikke videreformidle den kraftsensitive informasjonen til andre. Beredskapsmyndigheten kan i tvilstilfeller avgjøre hvem som er rettmessig bruker.*	
KBO-enheter skal etter energiloven § 9-3 første ledd identifisere hva som er kraftsensitiv informasjon, hvor denne befinner seg og hvem som har tilgang til den. *Identifiseringen av hva som er kraftsensitiv informasjon og hvor denne befinner seg, skal omfatte oppbevaring på papir, lagring i elektronisk form eller lagring på annen måte.*	
Har dere identifisert hva som er kraftsensitiv informasjon?	
Har dere identifisert hvor denne befinner seg? - I hvilke systemer? - Geografisk?	
Den enkelte KBO-enhet kan avgjøre om det er tjenstlig behov for å videreformidle kraftsensitiv informasjon til andre utenfor egen virksomhet. Den som har fått tilgang til kraftsensitiv informasjon av en KBO-enhet kan ikke videreformidle den kraftsensitive informasjonen til andre.	
Formidler dere kraftsensitiv informasjon til andre utenfor egen virksomhet? - Hvilken type informasjon til hvem? - Hvorfor?	

Hvordan har dere vurdert mottakers tjenstlige behov? - Eksemplifiser.	
Har dere gjort tydelig for mottakere at de ikke kan ikke videreformidle den kraftsensitive informasjonen til andre? - Forklar. - Er kravet dokumentert? - Hvordan følger dere det opp?	

Beskyttelse av kraftsensitiv informasjon

- *§ 6-3.Beskyttelse, avskjerming og tilgangskontroll*
- *§ 6-4.Sikkerhetsinstruks*
- *§ 6-7.Personkontroll*
- § 6-8. *Sikkerhetskopier*

§ 6-3. *Beskyttelse, avskjerming og tilgangskontroll*	
Virksomheter som har eller behandler kraftsensitiv informasjon skal etablere, opprettholde og videreutvikle system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for kraftsensitiv informasjon. Beskyttelse skal omfatte tiltak mot avlytting og manipulering fra uvedkommende. *System og rutiner skal omfatte merking, oppbevaring, bruk og distribusjon, tilintetgjøring og tiltak for intern og ekstern rapportering av hendelser av betydning for informasjonssikkerheten.* *Særskilte regler og sikkerhetstiltak skal utarbeides ved bruk av mobile enheter som kan motta, sende og lese kraftsensitiv informasjon.*	
Virksomheter som har eller behandler kraftsensitiv informasjon skal etablere, opprettholde og videreutvikle system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for kraftsensitiv informasjon. Beskyttelse skal omfatte tiltak mot avlytting og manipulering fra uvedkommende.	
Har dere etablert, opprettholdt og videreutviklet system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for kraftsensitiv informasjon?	

- Forklar og vis.	
Omfatter beskyttelsen tiltak mot avlytting og manipulering fra uvedkommende? - Beskriv tiltakene	
System og rutiner skal omfatte merking, oppbevaring, bruk og distribusjon, tilintetgjøring og tiltak for intern og ekstern rapportering av hendelser av betydning for informasjonssikkerheten.	
Har dere system og rutiner som omfatter merking, oppbevaring, bruk og distribusjon, samt tilintetgjøring av informasjon? - Vis.	
Har dere tiltak for intern og ekstern rapportering av hendelser av betydning for informasjonssikkerheten? - Beskriv. - Hvem rapporterer dere hva til?	
Særskilte regler og sikkerhetstiltak skal utarbeides ved bruk av mobile enheter som kan motta, sende og lese kraftsensitiv informasjon.	
Har dere utarbeidet særskilte regler og sikkerhetstiltak for bruk av mobile enheter som kan motta, sende og lese kraftsensitiv informasjon? - Vis dokumentasjon. - Kommuniseres disse reglene til brukerne? - Gis det brukeropplæring?	

§ 6-4. *Sikkerhetsinstruks*
Virksomheter som har eller behandler kraftsensitiv informasjon skal utarbeide og praktisere en sikkerhetsinstruks som sikrer at kravene til informasjonssikkerhet ivaretas. Sikkerhetsinstruksen skal beskrive hvilke system, rutiner og tiltak som er iverksatt for å etterleve kravene til informasjonssikkerhet, herunder krav til beskyttelse, avskjerming og tilgangskontroll.

Sikkerhetsinstruksen skal omfatte informasjon til ansatte og andre rettmessige brukere om taushetsplikten etter energilovens § 9-3 annet ledd og stille krav til undertegning av taushetserklæring. Sikkerhetsinstruksen skal også omfatte informasjon om at taushetsplikten medfører at kraftsensitiv informasjon ikke skal offentliggjøres.	
Virksomheter som har eller behandler kraftsensitiv informasjon skal utarbeide og praktisere en sikkerhetsinstruks som sikrer at kravene til informasjonssikkerhet ivaretas. Sikkerhetsinstruksen skal beskrive hvilke system, rutiner og tiltak som er iverksatt for å etterleve kravene til informasjonssikkerhet, herunder krav til beskyttelse, avskjerming og tilgangskontroll.	
Har dere utarbeidet en sikkerhetsinstruks som sikrer at kravene til informasjonssikkerhet ivaretas?	
Praktiseres denne sikkerhetsinstruksen? - Beskriv hvordan.	
Beskriver denne sikkerhetsinstruksen hvilke system, rutiner og tiltak som er iverksatt for å etterleve kravene til informasjonssikkerhet, herunder krav til beskyttelse, avskjerming og tilgangskontroll? - Er den dokumentert? - Vis sikkerhetsinstruksen.	
Sikkerhetsinstruksen skal omfatte informasjon til ansatte og andre rettmessige brukere om taushetsplikten etter energilovens § 9-3 annet ledd og stille krav til undertegning av taushetserklæring. Sikkerhetsinstruksen skal også omfatte informasjon om at taushetsplikten medfører at kraftsensitiv informasjon ikke skal offentliggjøres.	
Omfatter sikkerhetsinstruksen informasjon til ansatte og andre rettmessige brukere om taushetsplikten etter energilovens? - Er den kommunisert til alle aktuelle brukere, inklusive leverandører? - Beskriv	
Omfatter sikkerhetsinstruksen informasjon om at taushetsplikten medfører at kraftsensitiv informasjon ikke skal offentliggjøres?	

§ 6-7. *Personkontroll*	
KBO-enheter skal gjennomføre en bakgrunnssjekk av personer før ansettelse. *KBO-enheter kan kreve at personer som skal få tilgang til anlegg, system eller annet i klasse 2 og 3 skal fremlegge kredittsjekk.* *KBO-enheter skal før de fremsetter krav etter annet ledd foreta en risikovurdering. Kredittsjekk skal ikke anvendes dersom det kan iverksettes andre egnede sikkerhetstiltak.* *Bakgrunnssjekken etter første og annet ledd skal brukes som grunnlag for å vurdere en persons egnethet til å få tilgang til klassifiserte anlegg, system eller annet. Kredittsjekk skal slettes når egnethetsvurderingen er gjennomført.* *Krav om personkontroll etter første til fjerde ledd gjelder ikke personer som er sikkerhetsklarert og autorisert etter den til enhver tid gjeldende lov om nasjonal sikkerhet (sikkerhetsloven).* *Beredskapsmyndigheten kan etter søknad gi unntak fra kravene i første til fjerde ledd i denne bestemmelsen. Beredskapsmyndigheten kan ved vedtak fastsette krav om bakgrunnssjekk etter første til fjerde ledd for bestemte anlegg, system og annet.*	
Gjennomfører dere bakgrunnssjekk av personer før ansettelse? - Hvordan gjennomføres den?	
Gjennomfører dere kredittsjekk ved ansettelser av personer som skal få tilgang til anlegg, system eller annet i klasse 2 og 3? - Eventuelt andre tiltak?	
Hvordan gjennomfører dere egnethetsvurdering?	
Sletter dere kredittsjekken når egnethetsvurderingen er gjennomført?	

§ 6-8. *Sikkerhetskopier*
Virksomheter skal ha oppdaterte sikkerhetskopier av nødvendig informasjon, programvare og konfigurasjoner av driftskontrollsystemet som er av betydning for drift, sikkerhet og gjenoppretting av kraftforsyningen. Sikkerhetskopiene skal fjernlagres på et sikkert sted, som er lett tilgjengelig for virksomheten.

Nødvendig dokumentasjon om energisystemet og som lagres på datamedia, skal også foreligge som papirutskrifter. Disse skal oppdateres årlig og oppbevares på et sikkert sted som er lett tilgjengelig for virksomheten.	
Virksomheter skal ha oppdaterte sikkerhetskopier av nødvendig informasjon, programvare og konfigurasjoner av driftskontrollsystemet som er av betydning for drift, sikkerhet og gjenoppretting av kraftforsyningen. Sikkerhetskopiene skal fjernlagres på et sikkert sted, som er lett tilgjengelig for virksomheten.	
Hva har dere identifisert som den nødvendige informasjonen dere må ha en sikkerhetskopi av?	
Har dere oppdaterte sikkerhetskopier av nødvendig informasjon, programvare og konfigurasjoner av driftskontrollsystemet som er av betydning for drift, sikkerhet og gjenoppretting av kraftforsyningen?	
Er dataene fjernlagret på et sikkert sted, som er lett tilgjengelig for virksomheten? - Hvor er disse lagret? - «Kaldt eller varmt» lager? - Hvordan er dataene sikret mot tap, - uautorisert tilgang og manipulasjon? - Oppdateringssyklus?	
Nødvendig dokumentasjon om energisystemet og som lagres på datamedia, skal også foreligge som papirutskrifter. Disse skal oppdateres årlig og oppbevares på et sikkert sted som er lett tilgjengelig for virksomheten.	
Foreligger nødvendig dokumentasjon om energisystemet som lagres på datamedia, også som papirutskrifter?	
Er dokumentasjonen oppdatert årlig og oppbevart på et sikkert sted som er lett tilgjengelig for virksomheten?	

Anskaffelser og tjenesteutsetting

- § 6-5.*Anskaffelser*
- § 6-6.*Begrenset anbudsinnbydelse*
- § 6-9.*Digitale informasjonssystemer, bokstav e*

- *§ 7-14.Særskilte krav til driftskontrollsystem klasse 2, bokstav k Krav til leverandører (kun klasse 2 og 3 systemer)*

§ 6-5. ***Anskaffelser***	
KBO-enheter har ansvaret for at bestemmelsene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon ivaretas i anskaffelser. KBO-enheter skal i anskaffelser påse at leverandører er forpliktet til å etterleve bestemmelsene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon. *Det skal i avtale sikres at KBO-enheter gis rett til å kontrollere, herunder revidere, leverandørens etterlevelse av disse bestemmelsene.* *Plikten til å påse innebærer at det skal iverksettes system og rutiner for å undersøke, og om nødvendig, følge opp at reglene om informasjonssikkerhet og taushetsplikt etterleves.* *Bestemmelsene i første og annet ledd gjelder tilsvarende når KBO-enheter setter ut oppdrag for prosjektering, installering, vedlikehold og feilretting av driftskontrollsystemet.*	
KBO-enheter har ansvaret for at bestemmelsene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon ivaretas i anskaffelser. KBO-enheter skal i anskaffelser påse at leverandører er forpliktet til å etterleve bestemmelsene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon.	
Påser dere at leverandører er forpliktet til å etterleve bestemmelsene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon? - I prekvalifisering? - I forhandlinger og kontraktsinngåelse? - Under levetiden av leveransen?	
Må leverandørene signere på taushetserklæring? Inngås det sikkerhetsavtale med leverandøren?	
Det skal i avtale sikres at KBO-enheter gis rett til å kontrollere, herunder revidere, leverandørens etterlevelse av disse bestemmelsene.	
Inngår det i avtalen med leverandørene at dere gis rett til å kontrollere, herunder revidere, leverandørens etterlevelse av disse bestemmelsene?	

Reviderer dere leverandørens etterlevelse av kravene?	
Plikten til å påse innebærer at det skal iverksettes system og rutiner for å undersøke, og om nødvendig, følge opp at reglene om informasjonssikkerhet og taushetsplikt etterleves.	
Har dere system og rutiner for å undersøke at informasjonssikkerhet og taushetsplikt etterleves? - Forklar. - Vis rutiner og dokumentasjon.	
Har dere system og rutiner for å følge opp at reglene om informasjonssikkerhet og taushetsplikt etterleves? - Forklar. Vis rutiner og dokumentasjon.	

§ 6-6. *Begrenset anbudsinnbydelse*	
Anbudsinnbydelser og lignende skal begrenses når det er nødvendig for å hindre at sikkerhetsgradert eller kraftsensitiv informasjon blir offentlig tilgjengelig gjennom anbudsdokumentene. *Forståelsen av begrenset anbudsinnbydelse bygger på anskaffelsesregelverket.*	
Begrenser dere anbudsinnbydelser og lignende når det er nødvendig for å hindre at sikkerhetsgradert eller kraftsensitiv informasjon blir offentlig tilgjengelig gjennom anbudsdokumentene? - Forklar hvordan. - Gi eksempler.	
Kjenner dere til anskaffelsesregelverket?	

§ 6-9 e. Tjenesteutsetting	
e. Tjenesteutsetting	

Virksomheter skal sørge for at sikkerhetsnivået opprettholdes eller forbedres ved utsetting av tjenester.	
Sørger dere for at sikkerhetsnivået opprettholdes eller forbedres ved utsetting av tjenester? - *Forklar*	
Gjør dere risikovurdering før og etter tjenesteutsettelsen? - Landrisikovurdering? - Risikoanalyse av leveransen? - Er det dokumentert?	
Gjør dere revisjon før og etter? - Er det dokumentert?	
Tester dere teknisk sikkerhet før og etter? - Er det dokumentert?	
Følger dere opp loggstatistikk før og etter? - Er det dokumentert?	
Har dere god nok sikkerhetskompetanse for å følge opp tjenesteutsettingen, både kravspesifikasjoner, kontrakten og leverandøren? - Hvis ikke, bruker dere innleide eksperter?	

Leverandører og leveranser av driftskontrollsystemer – gjelder kun klasse 2 og 3 driftskontrollsystem

- *Særskilte krav til driftskontrollsystem klasse 2 - § 7-14 k. Krav til leverandører*

§ 7-14 k. Krav til leverandører	
For leveranser til driftskontrollsystemer tillates kun utenlandske leverandører fra land som er medlem i EFTA, EU eller NATO. En leveranse omfatter levering av utstyr, komponenter, programvare, data, programmeringstjenester, oppdateringer, feilretting, service og vedlikehold.	
Har virksomheten leveranser til driftskontrollsystemet fra utenlandske leverandører utenfor EFTA, EU eller NATO? - Hvilke leverandører gjelder det?	

Hvilke leveranser gjelder det? - Er dette systemleveranser? - Har leverandøren gjennom leveransen tilgang til data i driftskontrollsystemet? - Har leverandøren gjennom leveransen tilgang til driftskontrollsystemet og kan styre brytere og vern eller påvirke datatrafikk? - Er dette leveranser der rettigheter er oppdelt gjennom samarbeid med flere leverandører innenfor disse områdene?	

AMS Brytefunksjonalitet i avanserte måle- og styringssystem (AMS)

- *§ 6-10.Brytefunksjonalitet i avanserte måle- og styringssystem (AMS)*

§ 6-10. **Brytefunksjonalitet i avanserte måle- og styringssystem (AMS)**
Nettselskap som har avanserte måle- og styringssystem (AMS) med brytefunksjonalitet, skal sikre dette mot uønsket tilgang. Brytefunksjonalitet som definert i forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv. § 1-3, inkluderer i denne bestemmelsen begrensning av energi- og effektuttaket i det enkelte målepunkt. Nettselskap skal etablere og opprettholde egne sikkerhetstiltak for brytefunksjonaliteten, herunder: *a. Det er kun nettselskap som har tillatelse til å utføre fjernstyring av brytefunksjonaliteten. Fjernstyring av brytefunksjonaliteten skal utføres fra en adgangskontrollert sone.* *b. Leverandør med fjerntilgang til brytefunksjonaliteten, skal være lokalisert i et land som er medlem i EFTA, EU eller NATO. Leverandør lokalisert i andre land kan få tidsavgrenset fjerntilgang til brytefunksjonalitet under løpende oppsyn av kvalifisert personell fra nettselskapet eller kvalifisert personell fra leverandør lokalisert i land som er medlem i EFTA, EU eller NATO.* *Før leverandør lokalisert i land utenfor EFTA, EU eller NATO får fjerntilgang til brytefunksjonaliteten, skal nettselskapet foreta en risikovurdering som inneholder en vurdering av landrisiko.* *c. Nettselskap har ansvar for at det etableres kontrollordninger for bruk av bryte- og oppdateringsfunksjonaliteten som hindrer at en enkelt person eller enkelt bruker kan koble ut flere målepunkt samtidig.* *d. Fjernoppdatering av programvaren i AMS skal utføres fra en adgangskontrollert sone hos nettselskap eller leverandør. Ved bruk av leverandør skal vilkårene i bokstav b være oppfylt.*

e. Hver enkelt måler skal ha en individuell sikkerhetsløsning for bryte-, og oppdateringsfunksjonen, som forhindrer at hendelser som kompromitterer sikkerheten i en måler, kompromitterer sikkerheten i en annen måler.	
Nettselskap som har avanserte måle- og styringssystem (AMS) med brytefunksjonalitet, skal sikre dette mot uønsket tilgang. Brytefunksjonalitet som definert i forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv. § 1-3, inkluderer i denne bestemmelsen begrensning av energi- og effektuttaket i det enkelte målepunkt.	
Har dere sikret det avanserte måle- og styringssystem (AMS) med brytefunksjonalitet mot uønsket tilgang? - Forklar.	
a Det er kun nettselskap som har tillatelse til å utføre fjernstyring av brytefunksjonaliteten. Fjernstyring av brytefunksjonaliteten skal utføres fra en adgangskontrollert sone.	
Er det kun nettselskapet som har tillatelse til å utføre fjernstyring av brytefunksjonaliteten?	
Utføres fjernstyring av brytefunksjonaliteten fra en adgangskontrollert sone? - Beskrive hvordan adgang er kontrollert.	
b. Leverandør med fjerntilgang til brytefunksjonaliteten, skal være lokalisert i et land som er medlem i EFTA, EU eller NATO. Leverandør lokalisert i andre land kan få tidsavgrenset fjerntilgang til brytefunksjonalitet under løpende oppsyn av kvalifisert personell fra nettselskapet eller kvalifisert personell fra leverandør lokalisert i land som er medlem i EFTA, EU eller NATO.	
Hvilken leverandør har dere? Har leverandør fjerntilgang til brytefunksjonaliteten? - Admin rettigheter? - Master key? - Ifm. service? - Hvor er leverandøren lokalisert?	
Dersom utenlandsk leverandør er lokalisert utenfor EFTA, EU eller NATO, har leverandøren fjerntilgang til brytefunksjonaliteten? - Forklar. - Har kvalifisert personell fra nettselskapet løpende oppsyn mens leverandøren har fjerntilgang?	

- Har kvalifisert personell fra annen leverandør lokalisert i EFTA, EU eller NATO løpende oppsyn mens leverandøren har fjerntilgang?	
Før leverandør lokalisert i land utenfor EFTA, EU eller NATO får fjerntilgang til brytefunksjonaliteten, skal nettselskapet foreta en risikovurdering som inneholder en vurdering av landrisiko.	
Har nettselskapet foretatt en risikovurdering som inneholder en vurdering av landrisiko før leverandøren lokalisert i land utenfor EFTA, EU eller NATO får fjerntilgang til brytefunksjonaliteten? - Er denne dokumentert? - Vis.	
c. Nettselskap har ansvar for at det etableres kontrollordninger for bruk av bryte- og oppdateringsfunksjonaliteten som hindrer at en enkelt person eller enkelt bruker kan koble ut flere målepunkt samtidig.	
Har nettselskapet etablert kontrollordninger for bruk av bryte- og oppdateringsfunksjonaliteten som hindrer at en enkelt person eller enkelt bruker kan koble ut flere målepunkt samtidig? - Forklar	
d. Fjernoppdatering av programvaren i AMS skal utføres fra en adgangskontrollert sone hos nettselskap eller leverandør. Ved bruk av leverandør skal vilkårene i bokstav b være oppfylt.	
Utføres fjernoppdatering av programvaren i AMS fra en adgangskontrollert sone hos nettselskap eller leverandør? - Er dette regulert i kontrakt? - Hvordan kontrollerer dere at det skjer?	
e. Hver enkelt måler skal ha en individuell sikkerhetsløsning for bryte-, og oppdateringsfunksjonen, som forhindrer at hendelser som kompromitterer sikkerheten i en måler, kompromitterer sikkerheten i en annen måler.	
Har hver enkelt måler en individuell sikkerhetsløsning for bryte-, og	

oppdateringsfunksjonen, som forhindrer at hendelser som kompromitterer sikkerheten i en måler, kompromitterer sikkerheten i en annen måler? - Forklar	

Sikring av digitale informasjonssystemer – NSMs grunnprinsipper for IKT-sikkerhet

§ 6-9. *Digitale informasjonssystemer, 1, 2 og 3. ledd, bokstav a,b,c,d og f*

§ 6-9. *Digitale informasjonssystemer*
Virksomheter skal sikre digitale informasjonssystemer slik at konfidensialitet, integritet og tilgjengelighet ivaretas. *Det er den enkelte virksomhets ansvar å planlegge, gjennomføre og vedlikeholde sikringstiltak etter det digitale informasjonssystemets type, oppbygging og funksjon.* *Virksomheter skal ha en grunnsikring for digitale informasjonssystemer i henhold til anerkjente standarder og normer, herunder:* *a. Identifisere og dokumentere* *Virksomheter skal identifisere og dokumentere verdier, leveranser, tjenester, systemer og brukere i sine digitale informasjonssystemer. Dokumentasjonen skal holdes oppdatert.* *b. Risikovurdering* *Virksomheter skal gjennomføre risikovurdering ved systemendringer. Risikovurderingen skal holdes oppdatert.* *c. Sikre og oppdage* *Virksomheter skal sikre sine digitale informasjonssystemer for å motstå eller begrense skade fra uønskede hendelser. Virksomheter skal overvåke sine digitale informasjonssystemer slik at uønskede hendelser oppdages og registreres. Virksomheten skal varsle uønskede hendelser i sine digitale informasjonssystemer til den beredskapsmyndigheten bestemmer.* *d. Håndtere og gjenopprette* *Virksomheter skal håndtere uønskede hendelser i sine digitale informasjonssystemer og gjenopprette normaltilstand uten ugrunnet opphold.* *f. Sikkerhetsrevisjon* *Virksomheter skal jevnlig gjennomføre revisjoner av iverksatte sikringstiltak for digitale informasjonssystemer. Revisjoner skal påse at tiltakene faktisk er etablert og fungerer etter sin hensikt. Hver revisjon kan ta for seg deler av sikringstiltakene.*
Virksomheter skal sikre digitale informasjonssystemer slik at konfidensialitet, integritet og tilgjengelighet ivaretas.

Sikrer dere digitale informasjonssystemer slik at konfidensialitet, integritet og tilgjengelighet ivaretas? - Forklar.	
Det er den enkelte virksomhets ansvar å planlegge, gjennomføre og vedlikeholde sikringstiltak etter det digitale informasjonssystemets type, oppbygging og funksjon.	
Planlegger, gjennomfører og vedlikeholder dere sikringstiltak etter det digitale informasjonssystemets type, oppbygging og funksjon? - Forklar hvordan.	
a. Identifisere og dokumentere *Virksomheter skal identifisere og dokumentere verdier, leveranser, tjenester, systemer og brukere i sine digitale informasjonssystemer. Dokumentasjonen skal holdes oppdatert.*	
Har dere identifisert og dokumentert verdier, leveranser, tjenester, systemer og brukere i deres digitale informasjonssystemer? - Forklar. - Bruker dere NSMs Grunnprinsipper i dette arbeidet eller andre standarder og retningslinjer? Forklar.	
Er dette dokumentert? Hvordan holder dere dokumentasjonen oppdatert?	
b. Risikovurdering *Virksomheter skal gjennomføre risikovurdering ved systemendringer. Risikovurderingen skal holdes oppdatert.*	
Gjennomfører dere risikovurdering ved systemendringer? - Er de dokumentert? - Vis og eksemplifiser.	
Er risikovurderingene oppdatert? - Når var siste oppdatering?	
c. Sikre og oppdage	

Virksomheter skal sikre sine digitale informasjonssystemer for å motstå eller begrense skade fra uønskede hendelser. Virksomheter skal overvåke sine digitale informasjonssystemer slik at uønskede hendelser oppdages og registreres. Virksomheten skal varsle uønskede hendelser i sine digitale informasjonssystemer til den beredskapsmyndigheten bestemmer.	
Har dere sikret deres digitale informasjonssystemer for å motstå eller begrense skade fra uønskede hendelser? - Forklar. - Bruker dere NSMs Grunnprinsipper i dette arbeidet eller andre standarder og retningslinjer? Forklar og eksemplifiser tiltak.	
Overvåker dere de digitale informasjonssystemene slik at uønskede hendelser oppdages og registreres? - Forklar.	
d. Håndtere og gjenopprette *Virksomheter skal håndtere uønskede hendelser i sine digitale informasjonssystemer og gjenopprette normaltilstand uten ugrunnet opphold.*	
Håndterer dere uønskede hendelser i digitale informasjonssystemer? - Forklar. - Bruker dere NSMs Grunnprinsipper i dette arbeidet eller andre standarder og retningslinjer? Forklar og eksemplifiser Er dere medlem av KraftCERT eller NorCERT? Er dere ikke medlem av KraftCERT men benytter noen av KraftCERTs tjenester?	
Gjenoppretter dere til normaltilstand uten ugrunnet opphold? - Eksempler på hendelser og hendelseshåndtering?	
f. Sikkerhetsrevisjon *Virksomheter skal jevnlig gjennomføre revisjoner av iverksatte sikringstiltak for digitale informasjonssystemer. Revisjoner skal påse at tiltakene faktisk er etablert og fungerer etter sin hensikt. Hver revisjon kan ta for seg deler av sikringstiltakene.*	

Gjennomfører dere jevnlig revisjoner av iverksatte sikringstiltak for digitale informasjonssystemer? - Forklar prosessen. - Benytter dere leverandører til arbeidet?	
Påser dere i revisjonen at tiltakene faktisk er etablert og fungerer etter sin hensikt? - Forklar hvordan.	
Har dere eksempler på at revisjoner tar for seg deler av sikringstiltakene? - Gi eksempler.	