NVE
Reguleringsmyndigheten
for energi – RME

RME VEILEDER
Nr. 1/2022

# Veileder til sikkerhet i AMS

*Hanne Sæle, Maren Istad og Martin Gilje Jaatun*

# RME Veileder nr. 1/2022
# Veileder til sikkerhet i AMS


| | |
|---|---|
| **Utgitt av:** | Reguleringsmyndigheten for energi |
| **Redaktører:** | Øyvind A. A. Toftegaard og Catharina Hovind |
| **Forfattere:** | Hanne Sæle, Maren Istad og Martin Gilje Jaatun |
| **Forsidefoto:** | Tussafoten – Montering av instrumenter. Foto: Gustav Pless/NVE |
| **ISBN:** | 978-82-410-2229-6 |
| **ISSN:** | 2703-9757 |
| **Saksnummer:** | 202113977 |



**Sammendrag:** Oppdatert veileder til sikkerhet i AMS. Veilederen er oppdatert i henhold til endringer i avregningsforskriften § 4-6 som trådte i kraft 1. januar 2022. Veilederen bygger på tidligere veileder, samt strukturen til veileder for kraftberedskapsforskriften. Veilederen går systematisk til verks og tar for seg sikkerhetskravene slik de er oppdelt i avregningsforskriften § 4-1. Veilederen bygger på et arbeid utført av SINTEF, på oppdrag fra RME.



**Emneord:** AMS, Veileder, Sikkerhet, Smarte målere



Reguleringsmyndigheten for energi
Middelthuns gate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 22 95 95 95
E-post: rme@nve.no
Internett: www.reguleringsmyndigheten.no



Juni, 2022

# Innhold

**Forord** ..... **5**

**Sammendrag** ..... **6**

**1 Innledning** ..... **7**

**2 Veilederens virkeområde og omfang** ..... **8**

2.1 Virkeområde ..... 8
2.2 Omfang ..... 8
2.3 Struktur på veileder ..... 10

**3 Krav til sikkerhet i AMS etter avregningsforskriften** ..... **14**

3.1 Krav til nettselskapet i henhold til forskrift (§ 4-6 første og andre ledd) 14
3.1.1 Etablering og oppfølging av sikkerhetskrav ..... 16
3.1.2 Risiko- og sårbarhetsanalyse ..... 17
3.1.3 Sikkerhetsavtaler ..... 18
3.1.4 Tjenesteutsetting av utrulling og/ eller drift av AMS-løsningen til tredjepart ..... 19
3.1.5 Elektronisk beskyttelse mot ondsinnet programvare og inntrengning ..... 20
3.1.6 Beskyttelse mot uautorisert fysisk tilgang til AMS-utstyr ..... 21
3.2 Godkjenning av enheter og brukere som skal kommunisere til eller i AMS (§ 4-6 a) ..... 23
3.2.1 Tilgangskontroll for system ..... 23
3.2.2 Identifisering og autorisasjon av enheter ..... 25
3.2.3 Identifisering og autorisering av eksternt utstyr ..... 26
3.2.4 Fjerntilgang til AMS fra tredjepart eller leverandør ..... 26
3.3 Sporbarhet av endringer av programvare og konfigurasjon av dataprogram (§ 4-6 b) ..... 28
3.3.1 Kontroll med og sporing av endringer ..... 28
3.3.2 Oppdatert dokumentasjon av AMS-løsningen ..... 29
3.3.3 Kontroll med integriteten til programvare ..... 30
3.4 Beskyttelse av kommunikasjon mellom AMS-måler og sentralsystemet (§ 4-6 c) ..... 31
3.4.1 Sikkerhet i kommunikasjon i AMS-løsningen ..... 32
3.4.2 Oppbevaring av sikkerhetssertifikater og krypteringsnøkler ..... 32
3.5 Oppdatering av programvare (§ 4-6 d) ..... 34
3.5.1 Oversikt over versjoner i program- og maskinvare ..... 34
3.5.2 Kontroll av ekthet i programvare ..... 35
3.5.3 Kontroll med sårbarheter i programvare ..... 35
3.6 Sikkerhetsavtaler (§ 4-6 e) ..... 37
3.6.1 Logging og overvåking ..... 37
3.6.2 Uavhengighet ..... 38

3.7 Tilgjengelig funksjonalitet (§ 4-6 f)..... 39
3.7.1 Kontroll på sikkerhet med deaktivert eller ikke brukt funksjonalitet 39
3.7.2 Avviks- og hendelseshåndtering..... 40
3.7.3 Katastrofehåndtering og -øvelser ..... 41
3.7.4 Sikkerhetskopier og gjenoppretting ..... 42
3.8 Tilgangsbegrensning i målepunkt (§ 4-6 g) ..... 43
3.8.1 Beskyttelse mot uautorisert fysisk tilgang til AMS-utstyr..... 44
3.9 Opprettholdelse/ forbedring av sikkerhetsnivå i AMS ved tilkobling av andre enheter eller systemer (§ 4-6 fjerde ledd)..... 45
3.9.1 Tilkobling av eksternt utstyr..... 45
3.9.2 Tilkobling av utstyr i AMS lokalisert hos sluttbruker..... 46
3.10 Internkontrollsystem (§ 4-6 femte ledd) ..... 48
3.10.1 Internkontrollsystem for sikkerhet ..... 48
**4 Vedlegg - Sjekklister.....50**
4.1 Tabell 1 Krav til nettselskap i henhold til avregningsforskriften § 4-6 første og andre ledd (SKAL-krav er beskrevet i vanlig font, *BØR-krav* er beskrevet i kursiv)..... 50
4.2 Tabell 2 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 a 53
4.3 Tabell 3 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 b 56
4.4 Tabell 4 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 b 57
4.5 Tabell 5 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 d 58
4.6 Tabell 6 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 e 59
4.7 Tabell 7 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 f 61
4.8 Tabell 8 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 g 63
4.9 Tabell 9 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 fjerde ledd..... 63
4.10 Tabell 10 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 femte ledd..... 64
**5 Vedlegg – Kobling mellom sikkerhetskrav i avregningsforskriften og tiltak i NSM sine grunnprinsipper.....65**
5.1.1 Tabell 11 NSMs grunnprinsipper for IKT-sikkerhet..... 65
5.1.2 Tabell 12 Kobling mellom sikkerhetskrav i avregningsforskriften og tiltak i NSMs grunnprinsipper..... 66

# Forord

Reguleringsmyndigheten for energi i NVE (RME) har gitt Sintef Energi i oppdrag å omarbeide vår veileder til sikkerhet i avanserte måle- og styringssystem. Formålet med omarbeidelsen har vært tredelt. For det første skulle veilederen tilpasses de oppdaterte kravene til sikkerhet i AMS i avregningsforskriften § 4-6 som ble vedtatt av Olje- og energidepartementet sommeren 2021. For det andre skulle veilederen, som ble publisert tilbake i 2012, oppdateres med tanke på den teknologiske utviklingen de siste 10 årene. For det tredje skulle veilederen, som opprinnelig ble utarbeidet med fokus på AMS for sluttbrukere i lavspenningsanlegg, i fremtiden kunne benyttes for AMS i målepunkt for både uttak, innmating og utveksling i både høy- og lavspenningsanlegg.

Det enkelte nettselskap er ansvarlig for sikkerheten i AMS. Dette gjelder også ved tjenesteutsetting eller ved opprettelse av felles driftsallianser. Fristen for utrulling av AMS var 1. januar 2019. Nettselskapene har derfor gått fra en utrullingsfase til en driftsfase for AMS og fokuset bør derfor være på kontinuerlig forbedring av cybersikkerheten.

Innholdet i den omarbeidede veilederen er hovedsakelig basert på forarbeider til avregningsforskriften § 4-6, sikkerhetsveilederen fra 2012, Sintef sin evaluering av den forrige veilederen i 2017 og Sintef sin studie av forventet fremtidig utvikling for AMS i 2019. For å gjøre det så enkelt som mulig å lese veilederen, er dens struktur også omarbeidet. Den nye strukturen skal ligne mer på veiledningsmateriell for kraftberedskapsforskriften. Vi har også hatt som mål å henvise til annet relevant regelverk der det oppleves naturlig. For eksempel krav i personvernforordningen og kraftberedskapsforskriften. I tillegg har vi jobbet målrettet for at veilederen skal være forståelig for virksomheter med ulikt kompetansenivå og at veilederen skal kunne tåle fremtidig teknologiutvikling uten å bli utdatert for raskt.

Siden 2012 har sikkerhet knyttet til brytefunksjonen i AMS blitt flyttet til kraftberedskapsforskriften. Vår veileder er knyttet til vår rolle som Reguleringsmyndighet for energi og vil derfor ha et fokus på å beskytte AMS sine kjernefunksjoner som beskrevet i avregningsforskriften. Vårt hovedfokus er dermed å sikre at AMS til enhver tid fungerer etter sin hensikt. Personvern dekkes først og fremst av personvernforordningen som følges opp av Datatilsynet, mens målenøyaktighet i stor grad dekkes av forskrift om krav til elektrisitetsmålere som følges opp av Justervesenet.

Denne veilederen er utarbeidet av Sintef på oppdrag for RME. Sintef har benyttet egen fagkompetanse i tillegg til å samarbeide med bransjeaktører, RME og andre relevant aktører i arbeidet med veilederen.

Tore Langset
direktør
Reguleringsmyndigheten for energi

Jørund Krogsrud
fungerende seksjonssjef
Seksjon for energimarkedsrett

*Dokumentet sendes uten underskrift. Det er godkjent i henhold til interne rutiner.*

# Sammendrag

Oppdatert veileder til sikkerhet i AMS.

Veilederen er oppdatert i henhold til endringer i avregningsforskriften § 4-6 som trådte i kraft 1. januar 2022. Veilederen bygger på tidligere veileder, samt strukturen til veileder for kraftberedskapsforskriften. Veilederen går systematisk til verks og tar for seg sikkerhetskravene slik de er oppdelt i avregningsforskriften § 4-1.

Veilederen bygger på et arbeid utført av SINTEF, på oppdrag fra RME.

# 1 Innledning

Reglene om avanserte måle- og styringssystemer (AMS) skal bidra til korrekt avregning, nødvendig informasjon til styring av eget strømforbruk og økt mulighet for nettselskapet til å effektivisere driften av nettet. Disse er gitt i avregningsforskriften[1].

Innføringen AMS gir en rekke fordeler, hvor en av de tydeligste er å opprette direkte kommunikasjon mellom kundenes strømmålere og nettselskapet for oversendelse av målerdata ved automatisk avlesning av målerne[2]. Nettselskapene skal sørge for at AMS er installert i hvert målepunkt, dvs. at det er nettselskapene som har ansvaret for å innføre og drifte AMS-systemet i sitt forsyningsområde.

Denne veilederen er utarbeidet for å vise hvordan et nettselskap kan tilfredsstille kravene gitt i avregningsforskriften § 4-6 om krav til sikkerhet for AMS. Veilederen er inndelt tilsvarende som kravene i § 4-6 bokstav a til g.

Veilederen gir noen eksempler på sikkerhetstiltak som kan implementeres i AMS-løsninger for å kunne bidra til oppfyllelse av forskriftens krav.

[1] Forskrift av 11. mars 1999 nr. 301 om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv. (avregningsforskriften).
[2] I denne sammenhengen er automatisk avlesning synonymt med fjernavlesing.

# 2 Veilederens virkeområde og omfang

## 2.1 Virkeområde

Veilederens virkeområde er sikkerhet i AMS for nettselskap, som definert i avregningsforskriften § 1-3.

## 2.2 Omfang

Veiledningen omfatter innsamlingssystemet – fra målepunktet hos kunden til sentralsystemet hos nettselskap, samt tilhørende kommunikasjonssystem mellom disse. Veilederen følger definisjon av AMS, som definert i avregningsforskriften § 1-3:

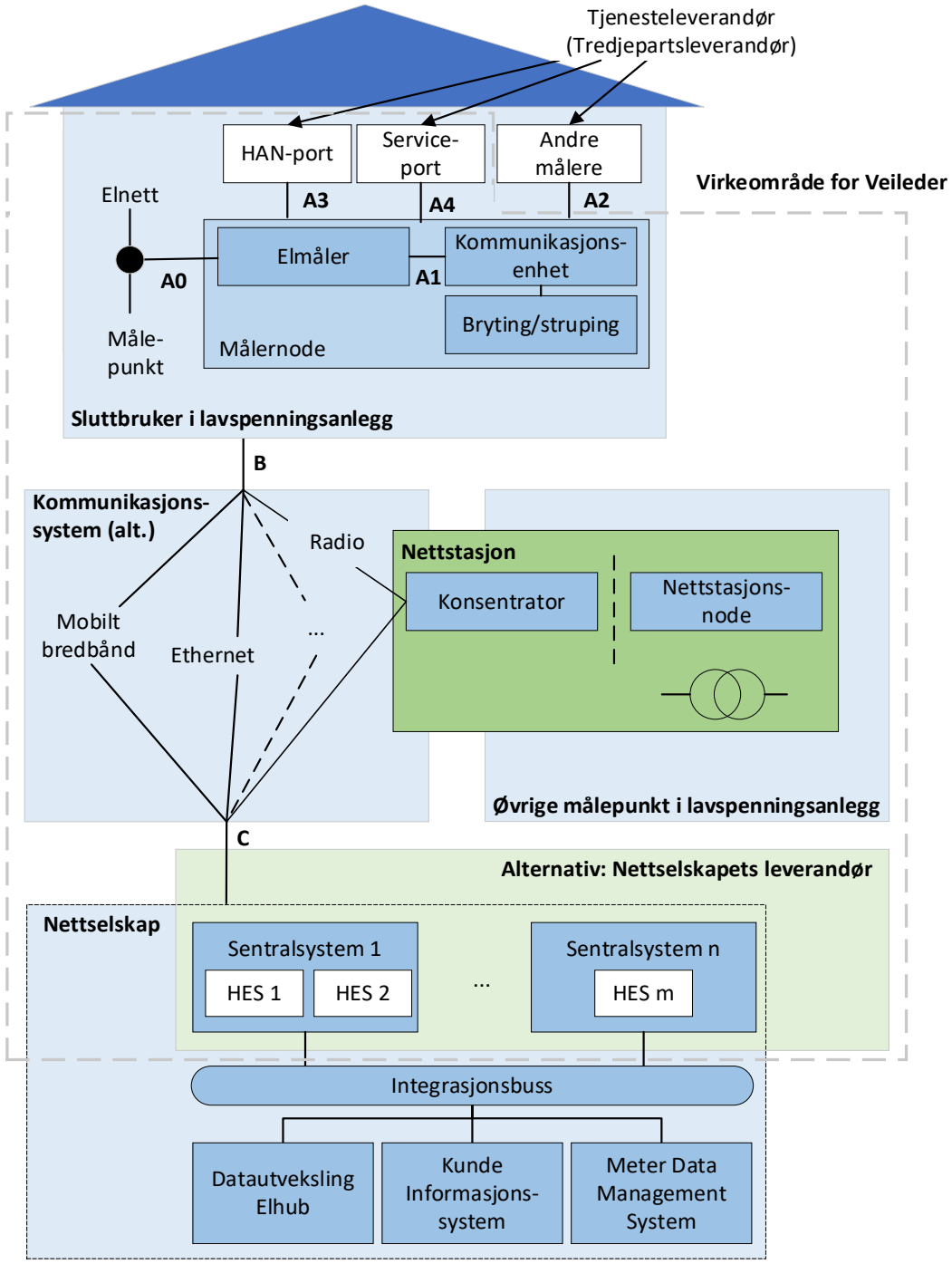
*Avanserte måle- og styringssystemer (AMS): Toveis informasjons- og kommunikasjonssystem fra og med elektrisitetsmålere som danner grunnlag for avregning av utveksling, innmating og uttak, til og med sentralsystemet hos nettselskapet eller nettselskapets leverandør.*

Definisjonen inkluderer alle målepunkt benyttet for avregning i lav- og høyspenningsanlegg, inkludert alle målepunkt for uttak, innmating og utveksling mellom nettområder. Der ikke annet er spesifisert, er det denne definisjonen av AMS som gjelder. Hvis det er spesielle forhold knyttet til AMS lokalisert hos sluttbruker eller i det øvrige strømnettet, er dette særskilt beskrevet.

Figur 1 er en illustrasjon av hvilke systemer som overfører AMS-data i forbindelse med driften av AMS, og ikke en detaljert beskrivelse av IT-strukturen for AMS. Fokus i illustrasjonen er på AMS tilknyttet målepunkt i lavspenningsanlegg. Grensesnitt A-C er basert på tidligere skisser av AMS-infrastruktur[3]. Figuren viser målepunkt i lavspenningsanlegg – både for sluttbruker og øvrige målepunkt, slik det er definert i avregningsforskriften.

Målerne som er inkludert i AMS-figuren, er direktekoblede målere i lavspenningsanlegg. For måler hos sluttbruker er det angitt hvilke interne deler som inngår, og ulike grensesnitt A0-A3 er vist. Målere med måletrafo (for kunder i lavspenningsanlegg, men uten brytefunksjonalitet) og presisjonsmålere med målertrafo for høyspenningsanlegg er ikke inkludert i figuren selv om disse målertypene også kan levere verdier over samme infrastruktur.

[3] M. Bartnes, G. I. Johansen og H. Sæle, «SINTEF-rapport A22318 "Risikovurdering AMS"» https://infosec.sintef.no/informasjonssikkerhet/2012/02/risikovurdering-av-ams/




**Figur 1 Illustrasjon av AMS-infrastruktur**

I forbindelse med kommunikasjon fra kunde til nettstasjon (mellom grensesnitt B og C), benyttes noen ganger en master/ konsentrator i nettstasjon. Denne enheten samler inn data fra alle underliggende målere og overfører dette samlet inn til sentralsystemet hos nettselskapet. Ulike kommunikasjonsløsninger kan brukes, og dette er illustrert ved å ta med flere alternativer i figuren. Det er ikke gjort forsøk på å lage en uttømmende oversikt, og derfor er det også inkludert en stiplet linje. Noen

løsninger bruker konsentrator f.eks. plassert i en nettstasjon, for å samle opp måledata fra AMS-målere, for deretter å sende disse videre inn til sentralsystemet hos nettselskap. Ved f.eks. bruk av radio-mesh, kan en måler installert hos sluttbruker fungere som en konsentrator.

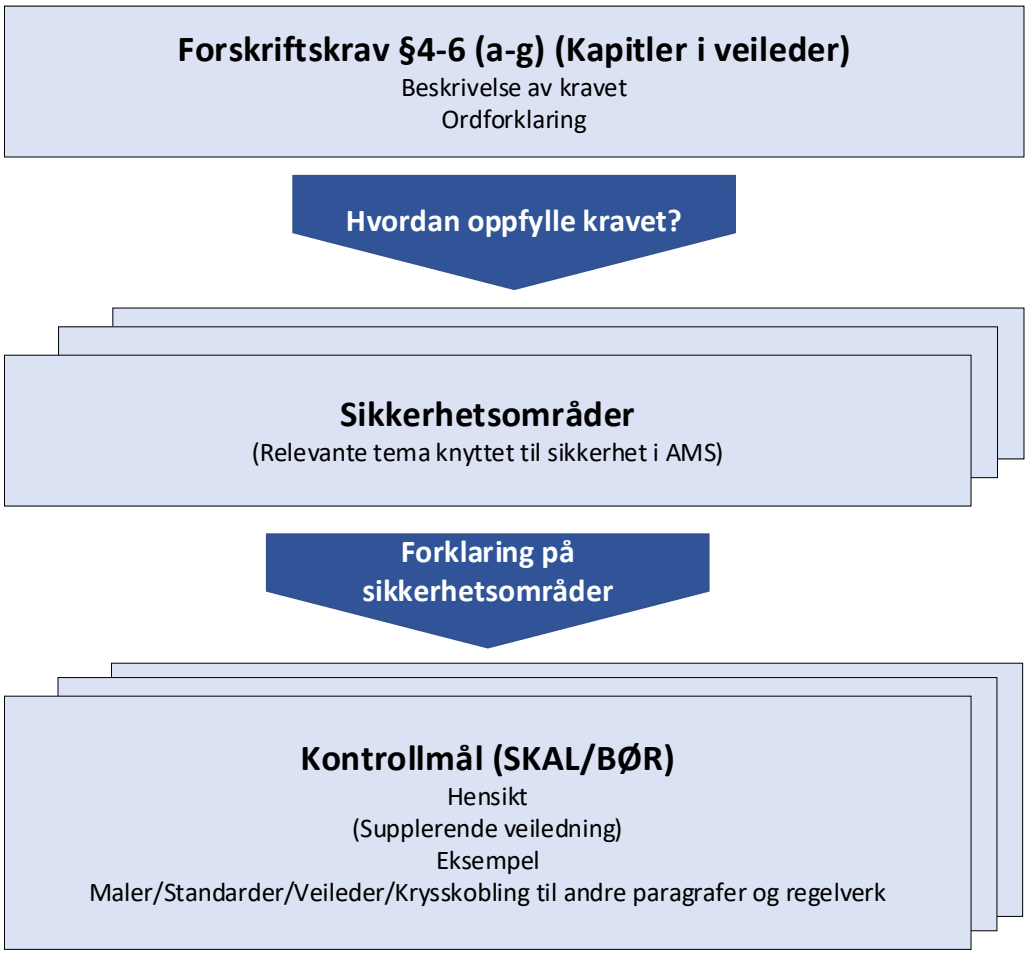
Måledata samles inn til innsamlingssystemet hos nettselskapet. Dette er vist som HeadEnd System (HES) i figuren. Et sentralsystem kan bestå av ett eller flere innsamlingssystemer, og et nettselskap kan ha ett eller flere sentralsystem. Sentralsystemet kan driftes av/outsources til en ekstern leverandør, og med en slik løsning vil nettselskapet motta/hente ut måleverdiene og bruke disse videre i egne systemer. Dette er vist i figuren som en alternativ boks.

Veilederen er utarbeidet for å ivareta sikkerhet knyttet til myndighetspålagt AMS-infrastruktur for innsamling av kWh-verdier til bruk for avregning, og de andre funksjonskravene gitt i avregningsforskriften § 4-2 og § 4-3. AMS-infrastruktur kan også benyttes til å samle inn nettnyttedata, men dette er ikke regulert gjennom avregningsforskriften, og dermed er det i liten grad vurdert i forbindelse med utarbeidelse av veileder.

## 2.3 Struktur på veileder

Veileder tar utgangspunkt i definisjonen av AMS gjengitt i veilederens virkeområde og omfang (kapittel 2.1 og 2.2). Systemer som evt. kobles til bak sentralsystemet, eller foran elektrisitetsmåler, er ikke en del av AMS, men sikkerhetsnivået skal likevel opprettholdes.

Oppbyggingen av veileder er presentert i figur 2. De ulike delene er beskrevet i teksten etter figuren.




**Figur 2 Oppbygging av veileder**

### Kapitler

Kapittelinndelingen i veilederen er gjort med utgangspunkt i kravene (a-g) i § 4-6 Krav til sikkerhet for AMS i forskrift for måling og avregning (avregningsforskriften).

### Forskriftskrav § 4-6 a-g

Veiledningen gjengir forskriftsteksten til hvert krav (a-g), etterfulgt av en kort beskrivelse av kravet, ordforklaringer der dette er vurdert som nødvendig, og råd om hvordan kravene kan oppfylles i praksis. Disse er organisert etter tematiske sikkerhetsområder som beskrevet under.

For noen forskriftskrav er det gitt oversikt over relevante maler, standarder, veiledere og eventuelle krysskoblinger til andre paragrafer og regelverk, og der det er spesielle behov for presiseringer, benyttes gule Obs-bokser. Det gjelder spesielt der det er viktig å presisere om kravene gjelder måler hos sluttbruker eller måler lokalisert andre steder i strømnettet.

**Sikkerhetsområde og kontrollmål**

For hvert forskriftskrav er det beskrevet sikkerhetsområder, som er en oversikt over hvilke temaer som er relevante knyttet til etablering av sikkerhet i AMS.

Videre i veilederen er det for hvert sikkerhetsområde utarbeidet egne kontrollmål som er målbare krav/ anbefalinger til sikkerhet. Kontrollmålene er beskrevet som SKAL- eller BØR-krav, hvor "SKAL-krav" må gjennomføres for å tilfredsstille forskriftskrav, mens "BØR-krav" er anbefalinger som kan gjøres for å øke sikkerheten i AMS, samt øke sannsynligheten for at forskriftskravene er oppfylt.

For hvert kontrollmål er det gitt en begrunnelse, eller hensikt, og også en supplerende veiledning der det er funnet hensiktsmessig.

Til kontrollmålene er det gitt eksempler på tiltak, prosedyrer og lignende for å oppnå det enkelte kontrollmål. Disse er **kun** ment som eksempler og skal gi en pekepinn på hvilke tiltak som kan iverksettes for å bidra til å oppnå kontrollmålet. Nettselskapet står fritt til å velge andre tiltak.

En oversikt over sammenhengen mellom forskriftskrav, sikkerhetsområde og kontrollmål er gitt i sjekklistene i vedlegg 1.

Nettselskapet må selv vurdere hvilke kontrollmål som skal prioriteres, gitt AMS-løsningens størrelse (f.eks. antall kunder), kompleksitet, teknologiske valg, og andre relevante forhold, forutsatt at forskriftskrav tilfredsstilles.

Veilederen har tilsvarende struktur som veileder til kraftberedskapsforskriften[4], med tilsvarende bruk av følgende symboler:

| Krav | Eksempel | Sjekkliste | Obs! | Mer info |
|---|---|---|---|---|
| | | | | |

Nettselskapet må kunne begrunne om enkelte obligatoriske kontrollmål (SKAL-krav) utelates. Det er derfor lagt ved (vedlegg 1) en tabellarisk fremstilling av kontrollmålene med eksemplene, der selskapet selv kan begrunne hvorfor/ hvorfor ikke et kontrollmål er valgt. Nettselskapene er hele tiden ansvarlige for at forskriftskrav tilfredsstilles.

I denne veilederen henviser RME videre til andre dokumenter, for eksempel kraftberedskapsforskriften[5], avregningsforskriften, NSMs veiledere på sikkerhet, temarapporter utarbeidet av NVE eller andre myndigheter og organisasjoner, maler og skjema fra NVE, og nasjonale og internasjonale standarder. RME anbefaler at brukere av denne veilederen innhenter mer kunnskap og råd i disse refererte dokumentene når virksomheten mener det er relevant. Merk at RME fører tilsyn med etterlevelsen av

[4] NVE - Veiledning til kraftberedskapsforskriften https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap/veiledning-til-kraftberedskapsforskriften/

[5] Forskrift av 1. november 2018 nr. 1641 om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften)

forskriftskravene, ikke med etterlevelse av veilederen, standarder og andre temadokumenter det er henvist til i denne veilederen.

# 3 Krav til sikkerhet i AMS etter avregningsforskriften

## 3.1 Krav til nettselskapet i henhold til forskrift (§ 4-6 første og andre ledd)

§

**§ 4-6.** ***Krav til sikkerhet for AMS***
Nettselskapet er ansvarlig for å sikre AMS. Nettselskapet er ansvarlig for at sikkerhet vurderes ved oppstart og gjennomføring av endringsprosesser tilknyttet AMS. Nettselskapet skal velge løsninger som gir høyest sikkerhetsnivå i AMS så lenge kostnaden er forsvarlig etter en kost/nytte-vurdering.

Sikkerhetsløsninger i AMS skal oppfylle kravene til digitale informasjonssystemer i kraftberedskapsforskriften.

**Beskrivelse av kravet**

Dette kravet presiserer at det er nettselskapet som er ansvarlig for sikkerhet i hele AMS-løsningen, også for de delene som eventuelt settes ut til tjenesteleverandør. Tjenesteutsetting endrer ikke på nettselskapet sitt ansvar for sikkerhet i AMS. Alle former for tjenesteutsetting må reguleres gjennom gode avtaler som inkluderer forhold som er relevante for sikkerhet. Med utgangspunkt i en kost-/nyttevurdering, skal det velges løsninger som gir høyeste praktisk mulig sikkerhetsnivå i AMS. Dette betyr at dersom den beste sikkerhetsløsningen medfører kostnader som ikke er økonomisk forsvarlige, må en annen løsning velges. Etter den store utrullingen av AMS rundt 2019, har AMS gått over i driftsfasen for nettselskapene, men det vil bli utskiftninger av målere i årene framover. Det forventes derfor at kost/nytte vurderinger knyttet til sikkerhetsnivå må utføres på nytt.

Sikkerhet i AMS omfatter beskyttelse mot alle typer uautorisert tilgang for å hindre misbruk, tyveri av data, spredning av ondsinnet programvare, utførelse av uautoriserte kommandoer og liknende.

Kravet presiserer også at de sikkerhetsløsningene som velges i AMS skal oppfylle krav til digitale informasjonssystemer i kraftberedskapsforskriften, gitt gjennom § 6 Informasjonssikkerhet og § 7 Beskyttelse av driftskontrollsystem.

**Ordforklaring**

| | |
|---|---|
| Vurdere sikkerhet | Gjennomføre risiko- og sårbarhetsanalyse (ROS) eller på annen hensiktsmessig måte vurdere sikkerhet for AMS |
| Oppstart | Igangsettelse av AMS |
| Endringsprosesser | Betydelige endringer i en eller flere deler av AMS-systemet (fra måler hos kunde, via kommunikasjonssystemet og inn til innsamlingssystemet. For AMS-struktur, se figur 1) |
| Sikkerhetsnivå | En indikasjon på grad av motstandsdyktighet mot angrep. Høyere sikkerhetsnivå medfører vanligvis flere eller mer omfattende sikkerhetstiltak, f.eks.: Krav til autentisering: Fra enkelt passord (lavt nivå) til to eller flere faktorer (høyt nivå) |

**Standarder**
ISO/IEC 27002:2017
**Veileder**
Veiledning til kraftberedskapsforskriften Kapittel 6: Informasjonssikkerhet
Veiledning til kraftberedskapsforskriften Kapittel 7: Beskyttelse av driftskontrollsystem
NSMs Grunnprinsipper for IKT-sikkerhet
Informasjonssikkerhet og personvern: Støtte til risikoanalyse av AMS og tilgrensende systemer
**Krysskobling til andre paragrafer og regelverk**
Kraftberedskapsforskriften § 6 Informasjonssikkerhet
Kraftberedskapsforskriften § 7 Beskyttelse av driftskontrollsystem

**Hvordan oppfylle kravet?**

Bestemmelsen plasserer ansvaret for å sikre AMS, hos nettselskapet. I tillegg til krav til sikkerhet gitt gjennom avregningsforskriften § 4-6, bør sikkerhetsløsninger som velges for AMS, også tilfredsstille kravene gitt gjennom følgende sikkerhetsområder:

1. Etablering og oppfølging av sikkerhetskrav (3.1.1)
2. Risiko- og sårbarhetsanalyse (3.1.2)
3. Sikkerhetsavtaler (3.1.3)
4. Utsetting av utrulling og/eller drift av AMS-løsningen til tredjepart (3.1.4)
5. Elektronisk beskyttelse mot ondsinnet programvare og inntrengning (3.1.5)
6. Beskyttelse mot uautorisert fysisk tilgang til AMS-utstyr (3.1.6)

Hvert sikkerhetsområde er forklart med kontrollmål, hensikt, evt. supplerende veiledning, med påfølgende eksempler.

### 3.1.1 Etablering og oppfølging av sikkerhetskrav

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Nettselskapets ledelse skal utarbeide og godkjenne interne krav for det overordnede sikkerhetsnivået til AMS-løsningen. Disse skal dekke alle prosesser og systemer relevant for AMS. Kravene skal være målbare og dokumenteres. | SKAL |
| b. Nettselskapets ledelse bør etablere et system for å følge opp og forbedre sikkerhetskravene for AMS. | BØR |

**Hensikt**

Hensikten med kravet er at ledelsen i nettselskapet skal gi retning og støtte for sikkerhetsarbeidet, samt sørge for at man gjennom organiseringen av nettselskapet følger opp arbeid med sikkerhet i AMS. Oppfølgingen er ment å skulle bidra til utvikling og forbedring av de interne sikkerhetskravene.

**Supplerende veiledning**

Disse kontrollmålene ligger tett opptil kravet om overordnede sikkerhetskrav i henhold til kraftberedskapsforskriften og organiseringen knyttet til beskyttelse av driftskontrollsystem.

I mindre virksomheter kan det være fornuftig å samle flere utøvende sikkerhetsoppgaver hos én person, f.eks. å vurdere om ledelse av sikkerhetsarbeidet i AMS også skal ligge under funksjonen til IKT- sikkerhetsleder/-koordinator, som er en funksjon det er krav om i henhold til kraftberedskapsforskriften. I tillegg kan det være nødvendig å gi utøvende ansvar for sikkerhetsoppgaver til personell som hovedsakelig har andre gjøremål. I slike situasjoner er det særlig viktig å påse at dette personellet gis nok tid og kompetanse til å utføre sikkerhetsoppgavene, og at ingen settes til å kontrollere eget arbeid.

**Eksempel: Etablering og oppfølging av sikkerhetskrav**

Nettselskapet skal utarbeide og godkjenne overordnede nivå til sikkerhet i sin AMS-løsning. For å få til dette, peker ledelsen ut en person som er ansvarlig for sikkerhet i AMS. Denne personen må ha/få tilstrekkelig kompetanse for å ivareta denne oppgaven, samtidig som det er viktig at personen gis nødvendig myndighet og ansvar, samt får avsatt tilstrekkelig med tid og ressurser slik at funksjonen kan ivaretas på en tilfredsstillende måte. Nettselskapet er lite, så dette ansvaret er allokert til en person. For å ivareta sikkerhet i AMS, er det viktig at alle Nettselskapets egne og innleide ressurser får tilstrekkelig opplæring på informasjonssikkerhet.

Når nettselskapet har ervervet seg tilstrekkelig kompetanse knyttet til informasjonssikkerhet, gjennomføres det en risiko- og sårbarhetsanalyse for å sette sikkerhetskravene på et akseptabelt nivå. Minst en gang i året gjennomgås sikkerhetskravene, for å sikre at Nettselskapet har hensiktsmessige sikkerhetskrav i

forhold til nettselskapets behov, etterlevelse av forskriftskrav og om kravene er tilstrekkelige.

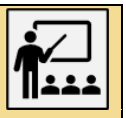
### 3.1.2 Risiko- og sårbarhetsanalyse

| **Kontrollmål:** | **Vurdering av krav** |
|---|---|
| a. Det skal gjennomføres risiko- og sårbarhetsanalyse eller annen hensiktsmessig sikkerhetsvurdering av AMS med den hensikt å identifisere risiko forbundet med drift og sikkerhet av AMS. Vurderingen skal gjentas med jevne mellomrom, og i hvert fall når det skjer vesentlige endringer i AMS-systemet og/eller omgivelser. | SKAL |
| b. Konfigurasjon og oppsett for kritiske kommandoer, målerdata og annen informasjon i AMS løsningen bør være basert på risiko. | BØR |

**Hensikt**

Sikkerhetsvurderingene skal gi nettselskapet styringsgrunnlag for å etablere hensiktsmessige sikkerhetstiltak og for å verifisere at risikoen er akseptabel. Dette gjennomføres gjerne som en risiko- og sårbarhetsanalyse (ROS-analyse).

ROS-analysen har som hensikt å identifisere årsaker til uønskede hendelser i AMS-løsningen, samt sannsynligheten for at de ulike hendelsene inntreffer og hvilke konsekvenser hendelsene kan utløse. Videre vil en slik analyse vurdere sannsynlighets- og /eller konsekvensreduserende tiltak. Avhengigheter mellom ulike deler av systemet bør også inkluderes i ROS-analyser.



**Eksempel: Gjennomføring av risiko- og sårbarhetsanalyse**
Nettselskapet gjennomfører sin årlige risiko- og sårbarhetsanalyse (ROS-analyse) for å identifisere risiko forbundet med drift av AMS. I denne analysen vurderer de alle forhold som for eksempel kan hindre korrekt avregning, hindre tilfredsstillende funksjonalitet, sette informasjonssikkerheten i fare eller hindre funksjonalitet i kraftforsyningen. Når alle forhold er vurdert, fastsettes det hva som er akseptabelt risikonivå som de ulike risikoene i ROS-analysen vurderes opp mot. Avhengigheter mellom ulike deler av systemet er med i ROS-analysen. Et eksempel på avhengighet kan være at selv om nettselskapet har sitt eget maskenettverk, er de likevel avhengig av Telenors 4G-nettverk.

Hvis nettselskaper finner tilfeller hvor risikonivå er høyere enn hva som er akseptabel risiko, etablerer de tiltak slik at de kan oppnå akseptabelt risikonivå. Til enhver tid skal nivå på sikkerhetstiltak være tilpasset risiko. Hvis Nettselskapet må gjøre større tiltak for å oppnå akseptabelt risikonivå, iverksettes tilstrekkelige midlertidige kompenserende tiltak inntil permanente tiltak er på plass.

I tillegg til å gjøre en slik ROS-analyse årlig, gjennomfører nettselskapet også ROS-analyser hvis det gjøres noen endringer i løsninger eller hvis en trusselsituasjon påvirker drift og sikkerhet i AMS.

**Maler**
Mal for risikovurdering av IKT-systemer – Nasjonal Sikkerhetsmyndighet
**Veileder**
Risikovurdering av IKT-systemer – Nasjonal Sikkerhetsmyndighet
Risikovurdering - Datatilsynet
Om risiko og risikovurdering - Digdir
Informasjonssikkerhet og personvern: Støtte til risikoanalyse av AMS og tilgrensende systemer

### 3.1.3 Sikkerhetsavtaler

| **Kontrollmål:** | **Vurdering av krav** |
|---|---|
| a. Nettselskapet skal inngå sikkerhetsavtaler med alle leverandører eller enkeltpersoner som ikke er ansatt i nettselskapet dersom de skal utføre arbeid på sentrale løsninger eller komponenter i AMS-løsningen. | SKAL |

**Hensikt**

Hensikten er å sørge for at leverandørene og enkeltpersonene gjennom avtalen behandler informasjonen og kunnskapen de får om nettselskapets AMS-løsning i henhold til nettselskapets egen policy på området.

**Eksempel: Etablering av sikkerhetsavtaler med ekstern leverandør**
Nettselskapet planlegger å gjennomføre en endring på AMS-løsningen, dvs. at de skal bytte kommunikasjonsløsning for målerne fra mobilt bredbånd til egen fiberløsning. De har bestemt seg for å sette ut deler av dette arbeidet til en ekstern leverandør. Før den eksterne leverandøren kan starte på jobben, inngår Nettselskapet en egen sikkerhetsavtale med leverandøren og de personene som skal utføre arbeidet.

**Maler**

Driftsavtale (SSA-D) – Direktoratet for forvaltning og økonomistyring

NVEs sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen

**Veileder**

Avtale om håndtering og beskyttelse av kraftsensitiv informasjon

### 3.1.4 Tjenesteutsetting av utrulling og/ eller drift av AMS-løsningen til tredjepart

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Sikkerheten i AMS skal ikke påvirkes ved at utrulling eller drift av AMS settes ut til ekstern tjenesteleverandør. | SKAL |

**Hensikt**

Utsettelse av utrulling eller drift av AMS til en ekstern tjenesteleverandør skal ikke påvirke sikkerheten i AMS.

**Supplerende veiledning**

Hvis enkelte deler av løsningen driftes eller på annen måte håndteres av en tjenesteleverandør, bør nettselskapet avtalefeste krav om rett til revisjon av leverandøren.

Nettselskapet bør også kunne gis mulighet til, i sin avtale med leverandøren, å angi at den overnevnte retten til revisjon skal kunne benyttes av RME. Revisjon av leverandøren bør kunne gjennomføres uten hinder.

**Eksempel: Tjenesteutsetting av utrulling og/eller drift av AMS-løsningen til tredjepart**

Nettselskapet har bestemt seg for å sette ut utrulling og drift av AMS-løsningen til en tredjepart. For å kunne gjøre dette, og samtidig ivareta sitt ansvar for sikkerhet i AMS, må Nettselskapet ha tilstrekkelig kompetanse til at de kan lage en kravspesifikasjon hvor krav til sikkerhet i AMS er beskrevet. Nettselskapet må også kunne kontrollere at tredjepart klarer å etterleve disse kravene i en driftssituasjon. For å kunne gjennomføre slike kontroller, har Nettselskapet satt målbare krav til leverandøren sin, som Nettselskapet følger opp regelmessig.

For at Nettselskapet skal kunne følge opp dette regelmessig, må de få innsyn i og ha en forståelse av de sikkerhetstiltakene som etableres og risikoen en slik tjenesteutsetting medfører. Hvis Nettselskapet ser at tredjepart ikke overholder avtalen, må de ha en realistisk mulighet til å trekke tilbake avtalen ved et slikt avtalebrudd, uakseptabel risiko eller endringer i regulering.

Gjennom utarbeidelse av en god kravspesifikasjon som følges opp regelmessig, sikrer nettselskapet at tjenesteutsettingen ikke påvirker risiko for kraftforsyningen negativt.

Nettselskapet inngår Databehandleravtale med leverandøren.

**Veileder**

Nasjonal sikkerhetsmyndighet - Sikkerhetsfaglige anbefalinger ved tjenesteutsetting

Datatilsynet – Databehandleravtale

**Krysskobling til andre paragrafer og regelverk**

Energilovforskriften § 3-6 Tilgang til personell

Avregningsforskriftens § 4-6 Krav til sikkerhet for AMS første ledd første setning og fjerde ledd

### 3.1.5 Elektronisk beskyttelse mot ondsinnet programvare og inntrengning

| **Kontrollmål:** | **Vurdering av krav** |
|---|---|
| a. Det skal etableres et system for overvåking og beskyttelse av programvaren i AMS med hensikten å oppdage og stanse ondsinnet programvare. | SKAL |

**Hensikt**

Forhindre at ondsinnet programvare eller inntrengning forstyrrer eller ødelegger AMS i den grad at informasjonssikkerheten blir kompromittert.

**Eksempel: Elektronisk beskyttelse mot ondsinnet programvare og inntrengning**

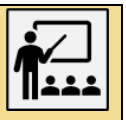
For å oppdage og stanse ondsinnet programvare, har Nettselskapet etablert et eget system for overvåking og beskyttelse av programvaren i AMS. I sentralsystemet har de et anti-skadevare og intrengningsdeteksjonssystem for å oppdage skadevare og andre angrep. Firmware i den enkelte AMS-måler er signert av leverandør, og ved oppstart vil AMS-måleren verifisere signaturen samt at firmwaren ikke har blitt endret.

### 3.1.6 Beskyttelse mot uautorisert fysisk tilgang til AMS-utstyr

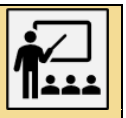
| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Alle rom som inneholder utstyr som er kritisk for AMS skal være i en egen adgangskontrollert sone. | SKAL |
| b. Komponenter i AMS utenfor adgangskontrollerte soner skal beskyttes mot uautorisert fysisk tilgang. | SKAL |
| c. Alle forsøk på å få uautorisert tilgang til utstyr i AMS-løsningen eller rom med kritisk AMS-utstyr skal registreres og varsles så snart som mulig. | SKAL |

**Hensikt**

Forhindre fysisk tilgang til komponentene i AMS, spesielt de som er plassert utenfor nettselskapets kontrollerte område. Slik tilgang kan gi elektronisk tilgang til AMS og systemene som inngår i AMS-infrastruktur.



**Eksempel:**
Nettselskapet bruker AMS-målere som er plombert i tillegg til elektronisk pirkesikring. Dersom noen del av måleren forsøkes åpnet, genereres det et alarmsignal som medfører en alarm til nettselskapet/leverandør i sentralsystemet.



**Eksempel:**
Nettselskapet har plassert sentralsystemet i tilknytning til driftssentralen. Lokalene er fysisk sikret, og adgang forutsetter bruk av adgangskort og kode. Lokalene er ytterligere beskyttet av alarmsystem knyttet til vekterselskap med utrykning.

**Eksempel:**
Med utgangspunkt i kravet om at sikkerhetsløsninger i AMS skal oppfylle kravene til digitale informasjonssystemer i kraftberedskapsforskriften, utfører nettselskapet i utgangspunktet alle sikkerhetskritiske oppgaver fra adgangskontrollert sone. I de tilfeller det er nødvendig med fjerntilgang til AMS-systemet fra hjemmekontor eller lignende, skal dette godkjennes i hvert enkelt tilfelle, og det skal dokumenteres at løsningene som brukes er

sikkerhetsmessig tilfredsstillende, f.eks. at det brukes en VPN-løsning med tilstrekkelig sikkerhet, at det kun er datautstyr administrert av Nettselskapet som tillates brukt, og at brukergrensesnittet låses med passord når det ikke er i bruk.

**Bruk av hjemmekontor**

Husk at kraftberedskapsforskriften § 6-10 fortsatt krever at bryterfunksjonen utføres fra adgangskontrollert sone.

## 3.2 Godkjenning av enheter og brukere som skal kommunisere til eller i AMS (§ 4-6 a)

§

a. Enheter og brukere som skal kommunisere til eller i AMS, må godkjennes i AMS av nettselskapet eller nettselskapets leverandør før de får tilgang.

**Beskrivelse av kravet**

Dette kravet omfatter godkjennelse av enheter og brukere som skal kommunisere til eller i AMS. Godkjennelsen gjøres innen AMS, og det er nettselskapet eller nettselskapets leverandør som gjør dette før den enkelte enhet og/eller bruker gis tilgang.

**Ordforklaring**

| | |
|---|---|
| Enheter | Elektronisk utstyr som skal kobles til AMS |
| Brukere | Kunde (åpning av HAN-port)<br>Ansatte i nettselskap<br>Ansatte hos tredjepart |

**Hvordan oppfylle kravet?**

Godkjenning av enheter og brukere som skal kommunisere til eller i AMS (§ 4-6 a) inkluderer følgende sikkerhetsområder:

- Tilgangskontroll for system (3.2.1)
- Identifisering og autorisasjon av enheter (3.2.2)
- Identifisering og autorisering av eksternt utstyr (3.2.3)
- Fjerntilgang til AMS fra tredjepart eller leverandør (3.2.4)

Hvert sikkerhetsområde er forklart med kontrollmål og hensikt, med påfølgende eksempler.

### 3.2.1 Tilgangskontroll for system

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Nettselskapet skal ha prosedyrer og kriterier for tildeling, endring, sletting og verifikasjon av korrekt tilgang til kundedata samt AMS-funksjonalitet | SKAL |

**Hensikt**

Nettselskapet har kontroll på hvem som har tilgang til kundedata og AMS-funksjonalitet, og hva de har tilgang til. Dette gjør det lettere for nettselskapet å avdekke eventuell uautorisert tilgang.

**Eksempel: Etablering av rutine for tilgangskontroll til system**
Nettselskapet har laget en egen rutine som sikrer at det kun er personer med rett autorisasjon som kan få tilgang til, endre, slette eller utlevere måledata eller annen sensitiv kundeinformasjon. Prosedyrene som er utarbeidet gjelder både for intern og ekstern tilgang.

Prosedyren inneholder også krav om bakgrunnssjekk av personell som skal ha tilgang til å håndtere sensitive systemer og informasjon. Bakgrunnssjekken skal som et minimum være vandelsattest (hvis mulig) og referansesjekk.

Når personer er godkjent, skal tilgang administreres på basis av forhåndsdefinerte roller og tilgangsnivåer, og det skal være tjenstlig behov som gir grunnlag for at tilganger skal tildeles, endres, fjernes og revideres.

**Eksempel: Rutine for å avdekke endring i målerdata eller annen kundeinformasjon**
For å ivareta kontroll på tilgang til systemet og på data i systemet, har Nettselskapet laget tekniske løsninger for både å oppdage uautorisert endring i måler- eller kundedata og for å forhindre uautorisert utlevering av måler- eller kundedata. For å ha kontroll på datakvaliteten, har Nettselskapet også laget tekniske løsninger for å loggføre dersom det utføres endringer i allerede registrerte målerdata og dersom målerdata eller annen kundeinformasjon utleveres til autorisert tredjepart.

**Eksempel: Tilgang fra underleverandører**
Nettselskapet har bruk for assistanse fra en leverandør som ikke er involvert i daglig drift av AMS-løsningen. Leverandøren får tilgang via en VPN-forbindelse som åpnes via sentralsystemet for en tidsbegrenset periode.

**Krysskobling til andre paragrafer og regelverk**
Kraftberedskapsforskriften § 6-1 Rettmessig bruker
Kraftberedskapsforskriften § 6-7 Personkontroll

### 3.2.2 Identifisering og autorisasjon av enheter

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Det skal implementeres mekanismer for å autentisere og autorisere enheter i AMS før det opprettes forbindelse mellom enheten og resten av AMS. | SKAL |
| b. Ved bruk av nettverk som nettselskapet ikke kontrollerer, f.eks. Mobilt Bredbånd (MBB), bør ekstra sterk autentisering foretas. | BØR |

**Hensikt**

Implementere en mekanisme for sikker identifisering av hver enkelt enhet som tilkoples AMS. Svært mange av enhetene i AMS vil måtte fysisk plasseres på steder der nettselskapet har begrenset kontroll med utstyret.

Dette gjelder i særdeleshet måleren og annet utstyr som blir plassert nær kundene (f.eks. vannmålere). Derfor bør enhetene underlegges strenge sikkerhetskontroller før de kommer i kontakt med AMS-løsningen.

**Eksempel: Identifisering og autorisasjon av enheter**
Hver enhet i AMS er tildelt et unikt sikkerhetssertifikat som kontrolleres før det sendes/mottas data fra enheten. Hvis man ikke får til å kontrollere enheten, eller den ikke kan verifiseres, skal enheten nektes tilgang til nettverket. Sikkerhetssertifikatet skal benyttes for å autorisere enheter i AMS.

**Eksempel: Identifisering av nye målere**
Nettselskapet har rullet ut smarte målere fra leverandøren. Målerne kommer ferdig konfigurert med en symmetrisk krypteringsnøkkel, og Nettselskapet har en database med krypteringsnøklene til de forskjellige målerne i sitt nett. Ved hver kommunikasjon mot måleren gjennomføres det autentisering mot måleren, og kommunikasjonen mellom måler og sentralsystem krypteres ende-til-ende.

### 3.2.3 Identifisering og autorisering av eksternt utstyr

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Håndholdte enheter (feltutstyr) må være autorisert og skal autentiseres av AMS-løsningen. Bruker skal være autorisert og autentisert. | SKAL |

**Hensikt**

Implementere streng autorisasjons- og brukskontroll for påkobling av eksternt utstyr til AMS-løsningen for å forhindre misbruk.

**Eksempel: Identifisering og autorisering av eksternt utstyr**
Nettselskapet har utarbeidet en prosedyre for autoriseringsprosessen av eksternt utstyr som tilkobles AMS. I forbindelse med at prosedyren ble laget, har de gått gjennom at det er ingen portal/grensesnitt hvor man kan koble til eksternt utstyr uten at disse er autoriserte og autentiserte. Sikkerhetssertifikatet skal benyttes for å autorisere enheter i AMS. Hver enhet i AMS er tildelt et unikt sikkerhetssertifikat som kontrolleres ved oppkobling mot enheter i AMS. Hvis det er enheter ute i nett som skal tilkobles, gjøres godkjennelsen ved at nummeret på enhet kontrolleres mot liste over godkjente enheter. Den eksterne enheten som kobles til, skal ikke benyttes til annet enn oppgave mot AMS.

Hvis man ikke får til å kontrollere enheten, eller den ikke kan verifiseres, skal enheten nektes tilgang til nettverket. Det skal være mulig å fjerne/endre autorisering av håndholdte enheter sentralt.

### 3.2.4 Fjerntilgang til AMS fra tredjepart eller leverandør

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Det skal etableres prosedyrer for godkjenning, administrering og overvåking av eksterne tilkoblinger for vedlikehold og diagnostiske aktiviteter på alle komponenter i AMS-systemet. | SKAL |

**Hensikt**

Beskytte komponenter i AMS-systemet mot uautorisert tilgang slik at AMS-løsningen ikke utsettes for store sårbarheter og trusler i de tilfeller nettselskap ønsker å benytte en tredjepart eller leverandør til å bistå med systemvedlikehold, oppgradering av programvare, feilretting eller liknende.

**Eksempel: Fjerntilgang til AMS fra tredjepart eller leverandør**

For å ivareta sikkerhet i AMS ved fjerntilgang til AMS fra tredjepart eller leverandør, har nettselskapet satt som krav at det ikke skal opprettes tilkobling til tredjepart eller leverandør uten eksplisitt avtale med selskapet. Gjennom denne avtalen må tredjepart forplikte seg til å etterleve relevante sikkerhetskrav, som bl.a. inkluderer krav om å benytte en sikker løsning for fjerntilgang. En slik fjerntilgang skal kun tillates fra sikre lokasjoner som ikke medfører økt risiko.

I kravspesifikasjonen fra Nettselskapet er det også tatt med at når eksternt vedlikehold er fullført, skal det fra Nettselskapet eller fra AMS-komponenten avslutte alle økter og eksterne tilkoblinger som er opprettet.

## 3.3 Sporbarhet av endringer av programvare og konfigurasjon av dataprogram (§ 4-6 b)

§

b. Enhver endring av programvare og konfigurasjon av dataprogram i AMS skal kunne spores tilbake til bruker, tidspunkt og endringen som ble gjort.

**Beskrivelse av kravet**

Dette kravet omfatter sporing av enhver endring av programvare og konfigurasjon av dataprogram i AMS: Det skal være mulig å spore tilbake til bruker, tidspunkt for endring og hvilken endring som ble utført.

**Hvordan oppfylle kravet?**

Sporbarhet av endringer av programvare og konfigurasjon av dataprogram omfatter følgende sikkerhetsområder:

- Kontroll med og sporing av endringer (3.3.1)
- Oppdatert dokumentasjon av AMS-løsningen (3.3.2)
- Kontroll med integriteten til programvare (3.3.3)

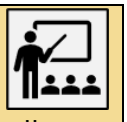
Hvert sikkerhetsområde er forklart med kontrollmål og hensikt, med påfølgende eksempler.

### 3.3.1 Kontroll med og sporing av endringer

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Nettselskapet skal dokumentere prosedyrer for å planlegge og utføre endringer i AMS-miljøet. | SKAL |
| b. Sentralsystemet skal logge alle endringer i programvare og konfigurasjon i AMS | SKAL |

**Hensikt**

Kontroll med endringer i AMS-løsningen er avgjørende for å ivareta krav om robust sikkerhetsfunksjonalitet og at AMS-løsningen fungerer etter sin hensikt også etter endringer.



**Eksempel:**
Nettselskapet har dokumentert en prosedyre for IT-avdelingen som angir at alle planlagte endringer i AMS-løsningen registreres i et eget

konfigurasjonsstyringsverktøy, og at både planlagte og ikke-planlagte endringer registreres her når de er utført. Prosedyren angir at IT-leder er ansvarlig for å overvåke når leverandør publiserer endringer i AMS-systemets programvare eller firmware, og sørge for at endringer blir risikovurdert og planlagt utført i konfigurasjonsstyringsverktøyet.

**Eksempel:**
Nettselskapet har et sentralsystem som krever innlogging med personlig brukernavn og tofaktor autentisering. Sentralsystemet logger automatisk alle endringer i konfigurasjon og programvareoppdateringer med brukernavn og tidspunkt, og i tillegg registreres endringene manuelt i konfigurasjonsstyringssystemet. Større endringer som medfører utskifting av hele sentralsystemet logges manuelt i konfigurasjonsstyringsverktøyet. Sentralsystemet vil også logge konfigurasjonsendringer og installasjon av oppdatert firmware på AMS-målere (måler-ID, brukernavn, tidspunkt, og endring).

### 3.3.2 Oppdatert dokumentasjon av AMS-løsningen

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Det skal til enhver tid foreligge fullstendig og oppdatert dokumentasjon av AMS-løsningens komponenter og konfigurasjoner. | SKAL |

**Hensikt**

Fullstendig og oppdatert dokumentasjon er viktig for å vurdere risiko, planlegge sikkerhetstiltak, planlegging av nye funksjoner, samt vedlikehold. Ved feil eller større hendelser hvor man må gjenoppbygge deler av systemet, vil dokumentasjonen være helt avgjørende i forhold til hvor lang tid gjenoppretting vil ta.

Oppdatert systembeskrivelse er også viktig for hvordan man vurderer for eksempel tilgang på reservemateriell, mulige reserveløsninger og andre beredskapstiltak. Det er derfor viktig at dokumentasjonen også utformes med tanke på slik bruk.

**Eksempel:**
Nettselskapet har implementert et konfigurasjonsstyringsverktøy som inneholder dokumentasjon av alle komponentene i AMS-systemet, samt kopi av alle konfigurasjonsfiler.

### 3.3.3 Kontroll med integriteten til programvare

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Det bør etableres et system for overvåking av endringer for å kunne oppdage uautoriserte endringer av programvare og informasjon. | BØR |

**Hensikt**

Systemkomponenter som har gjennomgått uventede eller uautoriserte endringer har trolig blitt kompromittert eller korrupte. Slike hendelser må oppdages, rapporteres, vurderes og eventuelt korrigeres av kompetent personell.

Man må påse at bruken av automatiske verktøy for integritetskontroll ikke har negativ innvirkning på AMS-løsningens operative funksjon, for eksempel ved å gi utilbørlig reduksjon av ytelse. Dette kontrollmålet kan ses i sammenheng med kontrollmål for sikker kommunikasjon (se 3.4).

**Eksempel: System for overvåking og avdekking av uautoriserte endringer**

Nettselskapet har etablert et system for å avdekke uautoriserte endringer av programvare og informasjon, og slik oppdage om noen systemkomponenter har blitt kompromitterte eller korrupte. Dette systemet utfører integritetsskanning av AMS-løsningen, og sjekker integriteten på programvare ved oppstart, oppdatering og eksekvering.

Dette systemet skal også sørge for at enheten i AMS er sikret fysisk og logisk mot uautorisert oppdatering og endring av programvare, og at endringer av programvare skal være testet og godkjent før de gjennomføres. I tillegg skal enhetene i AMS kunne verifisere at alle spørringer og kommandoer er gyldige, har rett format og er foretatt fra autentisert og autorisert kilde.

Nettselskapet har satt opp systemet slik at kun autoriserte og autentiserte brukere er i stand til å utføre kommandoer. Dette medfører at det ikke er mulig å utføre kommandoer i AMS med mindre man har tilgang til den rette symmetriske krypteringsnøkkelen. I tillegg har de implementert et automatisk verktøy som varsler ved integritetsavvik.

## 3.4 Beskyttelse av kommunikasjon mellom AMS-måler og sentralsystemet (§ 4-6 c)

§

c. Kommunikasjon i nettverket mellom AMS-måler og sentralsystem skal være beskyttet med ende-til-ende-kryptering. Ved bruk av et eget datanettverk, stengt for uvedkommende, kan kravet om ende-til-ende-kryptering fravikes.

**Beskrivelse av kravet**

Dette kravet gjelder for kommunikasjon i nettverket mellom AMS-måler og sentralsystemet, og at denne kommunikasjonen skal beskyttes med ende-til-endre-kryptering. Hvis det brukes eget datanettverk for denne kommunikasjonen, hvor ingen uvedkommende har adgang, er det ikke krav om ende-til-ende-kryptering. Det er også mulig å benytte en løsning hvor deler av kommunikasjonen er beskyttet med kryptering og deler er beskyttet med bruk av et eget datanettverk som er stengt for uvedkommende.

!

**Eget datanettverk for kommunikasjon mellom AMS-målere og sentralsystem**

Dette er normalt aktuelt for AMS tilknyttet høyspenningsanlegg eller konsentratorer i nettstasjoner, og ikke AMS tilknyttet målepunkt hos sluttbruker i lavspenningsanlegg.

**Ordforklaring**

| | |
|---|---|
| Sentralsystem | Se illustrasjon av AMS-system (Figur 1) |

**Hvordan oppfylle kravet?**

Beskyttelse av kommunikasjon mellom AMS-måler og sentralsystemet inkluderer følgende sikkerhetsområder:

- Sikkerhet i kommunikasjon i AMS-løsningen (3.4.1)
- Oppbevaring av sikkerhetssertifikater og krypteringsnøkler (3.4.2)

Sikkerhetsområdet er forklart med kontrollmål og hensikt, med påfølgende eksempler.

### 3.4.1 Sikkerhet i kommunikasjon i AMS-løsningen

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. All kommunikasjon mellom måler og sentralsystem og øvrig utstyr i AMS skal foregå på en sikker måte slik at innsyn, avlytting eller manipulering av signaler og informasjon ikke er mulig. | SKAL |
| b. Signalene og informasjonen bør krypteres ende-til-ende mellom måler og HES. | BØR |

**Hensikt**

Kommandoer, målerdata og annen sensitiv informasjon som overføres i AMS løsningen skal beskyttes mot uautorisert innsyn, avlytting eller endring.

Utstedelsen av offentlige nøkkel-sertifikater skal skje gjennom en sertifikat-policy eller fra en anerkjent tjenesteleverandør. Nøkkelgenerering og -håndtering skal gjøres på en sikker måte for å forhindre at løsningen blir sårbar. Kryptografimoduler, algoritmer og nøkler må være sikret.

**Eksempel:**
Nettselskapet har tatt i bruk en AMS-løsning der hver måler har en unik symmetrisk krypteringsnøkkel, og sentralsystemet har en beskyttet database med oversikt over hvilken nøkkel som hører til hvilken AMS-måler. Den symmetriske nøkkelen brukes til gjensidig utfordring-svar-autentisering mellom sentralsystem og måler, og til å etablere en sesjonsnøkkel som i sin tur brukes til å kryptere all data som sendes mellom måleren og sentralsystemet.

### 3.4.2 Oppbevaring av sikkerhetssertifikater og krypteringsnøkler

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Nettselskapet skal utarbeide retningslinjer for sikker oppbevaring av sikkerhetssertifikater og krypteringsnøkler som benyttes i AMS. | SKAL |
| b. Enheten skal lagre påloggingsinformasjon, sikkerhetssertifikater og annen sikkerhetsinformasjon sikkert. | SKAL |
| c. Autentisering bør gjøres ved bruk av flere faktorer | BØR |

**Hensikt**

Forhindre kompromittering av krypteringsnøkler og sikkerhetssertifikater for AMS-løsningen.

**Eksempel: Oppbevaring av sikkerhetssertifikater og krypteringsnøkler**

Nettselskapet har etablert et system for oppbevaring av krypteringsnøkler til hver enkelt måler. Krypteringsnøklene oppbevares kryptert, og kun navngitte medarbeidere har tilgang via sentralsystemet etter autentisering.

Private nøkler til digitale sertifikater oppbevares kryptert i en maskinvarebasert sikkerhetsmodul (HSM), og er beskyttet av egne passord og autentiseringkode (multi-faktor autentisering).

**Veileder**

TOTP: Time-Based One-Time Password Algorithm

## 3.5 Oppdatering av programvare (§ 4-6 d)

§

d. Programvare i AMS skal være oppdatert. Før ny programvare installeres i AMS, skal nettselskapet eller nettselskapets leverandør kontrollere at programvaren er autentisk.

**Beskrivelse av kravet**

Dette kravet gjelder for oppdatering av programvare i AMS. Programvaren skal til enhver tid være oppdatert. Før en ny oppdatering gjennomføres, ved at ny programvare installeres i AMS, skal nettselskapet eller nettselskapet sin leverandør kontrollere at ny programvare er autentisk.

**Hvordan oppfylle kravet?**

Oppdatering av programvare inkluderer følgende sikkerhetsområder:

- Oversikt over versjoner i program- og maskinvare (3.5.1)
- Kontroll av ekthet av programvare (3.5.2)
- Kontroll med sårbarheter i programvare (3.5.3)

Hvert sikkerhetsområde er forklart med kontrollmål og hensikt, med påfølgende eksempler.

### 3.5.1 Oversikt over versjoner i program- og maskinvare

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Nettselskapet skal ha en oppdatert oversikt over versjoner av all maskinvare, firmware, oppdateringer og programvare som benyttes i AMS løsningen. Oversikten skal oppdateres ved endringer og ved regelmessige gjennomganger. | SKAL |

**Hensikt**

Forhindre at kjente sårbarheter finnes i nettselskapets systemer, ved kontinuerlig ha god oversikt over programvare og maskinvare. AMS vil for mange selskaper være en stor og kompleks løsning med mange komponenter. Må ses i sammenheng med 3.3.3)

**Eksempel:**
Nettselskapet har en database med oversikt over alle måler-ID-er, som inneholder type og modell/versjon av måler, versjon av firmware, når den ble installert, og

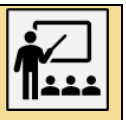
eventuelle tidligere versjoner av firmware som er tilgjengelig på måleren. Databasen omfatter også eventuelle konsentratorer og annet nettverksutstyr mellom måleren og sentralsystemet. Dessuten finnes det en database med oversikt over maskinvare som brukes i sentralsystemet, versjon av operativsystem, installerte oppdateringer med dato, og versjon av HES programvare samt oppdateringer med dato.

### 3.5.2 Kontroll av ekthet i programvare

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Nettselskapet skal verifisere at programvare, firmware og tilhørende oppdateringer er ekte | SKAL |

**Hensikt**

Forhindre at en angriper kan introdusere manipulert programvare eller firmware på endesystem eller måler. Dette kontrollmålet gjelder kun oppdateringer fra leverandør, ikke programvare etc. som allerede er installert (dette dekkes av 3.3.3).



**Eksempel:**
Nettselskapet har valgt en leverandør av AMS-system som sørger for at all programvare, firmware og oppdatering er signert med en digital signatur. Leverandørens offentlige nøkkel er signert av en anerkjent Certification Authority (CA), og nettselskapet har lastet ned det offentlige sertifikatet til leverandøren og verifisert ektheten til det. Før ny programvare installeres på endesystemet, verifiseres det at den digitale signaturen på programvaren fra leverandøren er korrekt. Det samme gjøres ved nedlasting av oppdatert firmware til AMS-måler. I tillegg vil også AMS-måleren verifisere at signaturen er korrekt før ny firmware tas i bruk på AMS-måleren.

### 3.5.3 Kontroll med sårbarheter i programvare

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Nettselskapet skal ha prosesser for å fange opp eventuelle kjente programvaremessige sårbarheter i sitt AMS-miljø. | SKAL |
| b. Dersom man blir kjent eller varslet om sårbarheter, skal disse evalueres og eventuelt håndteres umiddelbart. | SKAL |

**Hensikt**

Forhindre at kjente sårbarheter ikke blir vurdert eller håndtert.

Det kan være nødvendig at man vurderer om sikkerhetsoppdateringene kan utgjøre en trussel mot funksjonaliteten til AMS. Derfor bør man ha tett dialog med leverandøren omkring sikkerhetsoppdateringer.

Det er viktig at lukking av sårbarheter ikke gjøres på en måte som medfører for stor risiko for nettselskapet eller kraftsystemet.

**Eksempel:**
Nettselskapet abonnerer på varsler fra KraftCERT, og har laget en prosess som automatisk filtrerer ut varsler som er relevant for deres AMS-miljø. Sårbarheter i sentralsystemet oppdateres i samråd med leverandør så snart dette er praktisk mulig. Sårbarheter i firmware for AMS-målere håndteres så snart firmwareoppdatering fra leverandør er tilgjengelig og testet hos nettselskapet.

**Veileder**
Grunnprinsipper for IKT-sikkerhet 2.0 – Ivareta en sikker konfigurasjon
Grunnprinsipper for IKT-sikkerhet 2.0 – Oppdag og fjern kjente sårbarheter og trusler

## 3.6 Sikkerhetsavtaler (§ 4-6 e)

§

e. Hendelser som kompromitterer sikkerheten i en AMS-måler, eller dens kommunikasjon med sentralsystemet, skal ikke kompromittere sikkerheten i andre AMS-målere, deres kommunikasjon med sentralsystemet, eller sentralsystemet i seg selv.

**Beskrivelse av kravet**

Dette kravet omhandler å hindre eskalering av sikkerhetshendelser. Det betyr at hvis en hendelse kompromitterer sikkerheten i en AMS-måler, eller i kommunikasjonen mellom AMS-måler og sentralsystemet, skal ikke sikkerheten i andre AMS-målere kompromitteres. Tilsvarende skal ikke sikkerheten i kommunikasjonen fra andre AMS-målere til sentralsystemet, eller selve sentralsystemet kompromitteres.

**Ordforklaring**

| | |
|---|---|
| Kompromittere | Kompromittere betyr at noen har kommet seg forbi sikkerhetsløsningene på en eller flere enheter i AMS-systemer. |

**Hvordan oppfylle kravet?**

Sikkerhetshendelser inkluderer følgende sikkerhetsområder:

- Logging og overvåking (3.6.1)
- Uavhengighet (3.6.2)

Hvert sikkerhetsområde er forklart med kontrollmål og hensikt, med påfølgende eksempler.

### 3.6.1 Logging og overvåking

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Nettselskapet skal ha satt opp løsning og rutiner for sikkerhetslogging i den totale AMS-løsningen. | SKAL |

**Hensikt**

Logger er et svært viktig verktøy for å kunne påvise unormal aktivitet i systemet. Som et supplement bør nettselskapet vurdere å etablere et automatisk analyseverktøy for logger, slik at man raskt får et varsel dersom man får unormal trafikk.

**Eksempel:**

Nettselskapet har installert et inntrengningsdeteksjonssystem (IDS) som en del av sentralsystemet, og IDS overvåker både lokale logger og nettverkstrafikk til/fra HES.

**Veileder**

Grunnprinsipper for IKT-sikkerhet 2.0 – Etabler sikkerhetsovervåking

### 3.6.2 Uavhengighet

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Sikkerhetsfunksjonalitet i AMS-løsningen skal ikke påvirkes ved feil i AMS eller feil konfigurasjon av annen funksjonalitet. | SKAL |
| b. Hvis man kompromitterer en måler, skal ikke dette ha noen konsekvenser for andre målere eller sentralsystemet. | SKAL |

**Hensikt**

Dersom det oppstår en feil i et system eller i kommunikasjonsløsningen til AMS, så skal dette ikke påvirke informasjonssikkerheten ved at for eksempel kundedata eller annen informasjon blottlegges. Dersom noen får fysisk tilgang til en måler, og mulighet til å hente ut informasjon fra denne (som f.eks. krypteringsnøkler), skal ikke dette kunne brukes til å få tilgang til informasjon fra (eller påvirke) andre målere eller hente ut informasjon fra sentralsystemet.

**Eksempel:**

Nettselskapet har sørget for at alle AMS-målere har en unik symmetrisk nøkkel som brukes for å autentisere måleren mot HES (og omvendt) samt for å etablere sesjonsnøkler for ende-til-ende-kryptering. Nettselskapet overvåker at det kun er en måler som kommuniserer med en gitt måler-ID/nøkkel-kombinasjon, og dersom det oppdages at flere enheter bruker samme ID/nøkkel, blir den angjeldende nøkkel gjort ugyldig, og måleren må byttes.

## 3.7 Tilgjengelig funksjonalitet (§ 4-6 f)

§

f. AMS skal til enhver tid kunne utføre de oppgaver systemet er designet for. Nettselskapet eller nettselskapets leverandør skal deaktivere funksjonalitet i AMS som ikke skal benyttes.

**Beskrivelse av kravet**

Dette kravet omfatter oppgavene som AMS-systemet skal utføre. Det er kun funksjonalitet som er i bruk til ett eller flere formål, som skal være aktiverte. Funksjonalitet som ikke benyttes, skal deaktiveres.

**Ordforklaring**

| | |
|---|---|
| Deaktivere | Gjøres utilgjengelig for bruk/Settes ut av drift |

**Hvordan oppfylle kravet?**

Kontroll på sikkerhet i AMS med tilgjengelig og deaktivert funksjonalitet inkluderer følgende sikkerhetsområde:

- Kontroll på sikkerhet med deaktivert eller ikke brukt funksjonalitet (3.7.1)
- Avviks- og hendelseshåndtering (3.7.2)
- Katastrofehåndtering og -øvelser (3.7.3)
- Sikkerhetskopier og gjenoppretting (3.7.4)

Sikkerhetsområdet er forklart med kontrollmål og hensikt, med påfølgende eksempler.

### 3.7.1 Kontroll på sikkerhet med deaktivert eller ikke brukt funksjonalitet

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Funksjonalitet i AMS som ikke er i bruk skal deaktiveres | SKAL |
| b. Funksjonalitet som er deaktivert eller ikke tilgjengelig for bruk skal ikke påvirke sikkerheten i løsningen. | SKAL |

**Hensikt**

Forhindre at funksjonalitet som ikke er i bruk er aktivert og kan utnyttes av en angriper. Ideelt sett burde all kode som ikke er i bruk fjernes, da dette vil redusere kompleksiteten, og gjøre analyser lettere. Utover dette vil all kode potensielt kunne

representere et angrepspunkt for en inntrenger, og ved å deaktivere kode som ikke brukes vil man minimalisere angrepsflaten til AMS.

**Eksempel:**
Nettselskapet har ikke tatt i bruk muligheten for struping i deres AMS-løsning. De gjennomfører egne tester for å verifisere at det ikke er mulig å strupe strømmen hos sluttbrukere fra sentralsystemet.

**Eksempel:**
Nettselskapet har ikke åpnet for bruk av serviceport (optisk kommunikasjonsport) i deres AMS-løsning. De gjennomfører egne tester for å verifisere at det ikke er mulig å koble til serviceporten eller på noe vis å påvirke AMS-løsningen via den deaktiverte serviceporten.

### 3.7.2 Avviks- og hendelseshåndtering

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Nettselskapet skal etablere en dokumentert prosess for avviks- og hendelsesregistrering. | SKAL |
| b. Nettselskapet skal etablere en dokumentert prosess for hendelseshåndtering. | SKAL |

**Hensikt**

Å registrere og håndtere avvik er en svært viktig funksjon for å kontrollere at sikkerheten er tilstrekkelig ivaretatt, samtidig som man raskt kan se trender som forteller om det er uvanlig aktivitet rundt AMS.

Ved en konkret hendelse er det viktig at nettselskapet har klare rutiner og prosedyrer for hvordan hendelsen skal håndteres, slik at man unngår misforståelser, uklare ansvarsforhold og at man på en mest mulig effektiv måte får normalisert situasjonen.

**Eksempel:**
Nettselskapet har etablert en prosess for registrering og håndtering av avvik og hendelser hvor forskjellige hendelser er klassifisert i følgende kategorier:

1. Uautorisert tilgang til informasjon
2. Kompromittering
3. Forsøk på kompromittering
4. Tjenestenekt

5. Rekognosering/informasjonsinnsamling
6. Annet

Nettselskapet har dokumentert roller og ansvar, og har en plan for håndtering og avklaring av hendelser, og rutiner for eskalering. Alle hendelser i kategori 1-5 over rapporteres til KraftCERT via MIPS-plattformen, andre hendelser vurderes individuelt om de skal rapporteres. Avvik som det ikke gjøres noe med, skal godkjennes av nettselskapets sikkerhetsansvarlig. Alle avvik fra egne og eksterne krav dokumenteres, og alle avvik som ikke er lukket følges opp til de lukkes.

**Veileder**

Grunnprinsipper for IKT-sikkerhet 2.0 – Forbered virksomheten på håndtering av hendelser

Grunnprinsipper for IKT-sikkerhet 2.0 – Vurder og klassifiser hendelser

Grunnprinsipper for IKT-sikkerhet 2.0 – Kontroller og håndter hendelser

### 3.7.3 Katastrofehåndtering og -øvelser

| **Kontrollmål:** | **Vurdering av krav** |
|---|---|
| a. Nettselskapet skal ha beredskapsplaner og forberedte løsninger for å sikre beredskap, kontinuitet og evne til å håndtere katastrofer knyttet til informasjonssikkerhet og AMS. | SKAL |
| b. Det skal jevnlig gjennomføres øvelser for å håndtere omfattende sikkerhetshendelser og -katastrofer. | SKAL |

**Hensikt**

Beredskapsplaner og øvelser er helt nødvendig for at nettselskapet effektivt kan håndtere en katastrofe, og raskt kan gjenopprette AMS-løsningen ved en større hendelse. For mer informasjon om beredskapsplaner og øvelser, se eksempler i ”Veiledning til forskrift om beredskap i kraftforsyningen”.

**Eksempel:**

Nettselskapet har en beredskapsplan som også omfatter sikkerhetshendelser i AMS. Nettselskapet gjennomfører årlig en beredskapsøvelse som tester de vesentlige momentene i beredskapsplanen. Alle tjenesteleverandører som er involvert i AMS hos Nettselskapet deltar i øvelsen.

**Veileder**
Veiledning til forskrift om beredskap i kraftforsyningen

### 3.7.4 Sikkerhetskopier og gjenoppretting

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Det skal foreligge sikkerhetskopier av all kritisk programvare, konfigurasjoner og dokumentasjon av alle relevante komponenter i AMS-løsningen. | SKAL |
| b. Det skal foretas jevnlig sikkerhetskopiering av måledatabasen. | SKAL |
| c. Sikkerhetskopiene bør lagres på et sikkert sted, et annet fysisk sted enn der originalene befinner seg. | BØR |
| d. Sikkerhetskopiene bør umiddelbart gjenopprettes på et test/skyggesystem for å verifisere at de er korrekt generert. | BØR |

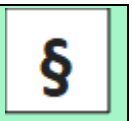
**Hensikt**

Ved katastrofale feil i systemet, er det svært viktig at nettselskapet har rask tilgang på sikkerhetskopier for å unngå unødig lang nedetid og eksponering av AMS-løsningen for mulige sårbarheter.

**Eksempel:**
Nettselskapet har sikkerhetskopi av HES programvare og alle HES konfigurasjonsfiler samt de tre siste versjoner av firmware for alle AMS-målertyper i sitt nett. Sikkerhetskopiene oppbevares off-line hos nettselskapets leverandør av IT-tjenester. Hver gang det tas sikkerhetskopi av HES og tilhørende konfigurasjon verifiseres det at dette kan gjenopprettes korrekt på et test/skyggesystem.

**Veileder**
Grunnprinsipper for IKT-sikkerhet 2.0 – Etabler evne til gjenoppretting av data

## 3.8 Tilgangsbegrensning i målepunkt (§ 4-6 g)



g. I målepunkt for sluttbrukere i lavspenningsanlegg skal tilgang til AMS-målerens grensesnitt begrenses for andre enn sluttbruker, nettselskapet og andre aktører med legitimt behov. I øvrige målepunkt skal kun nettselskapet og andre aktører med legitimt behov ha tilgang til AMS-måleren.

**Beskrivelse av kravet**

Dette kravet omfatter tilgang til målepunkt hvor AMS-måler er installert. For målere tilknyttet lavspenningsanlegg og tilknyttet en sluttbruker, er det kun sluttbruker, nettselskapet og andre aktører med legitimt behov som skal ha tilgang til grensesnittet på AMS-måler. I øvrige målepunkt er det kun nettselskap og andre aktører med legitimt behov som skal ha tilgang.

**Ordforklaring**

| | |
|---|---|
| Sluttbruker i lavspenningsanlegg | Strømkunde (f.eks. husholdningskunde, hyttekunde, næringskunde, …) |

**Veileder**
AMS + HAN - om å gjøre sanntids måledata tilgjengelig for forbruker. Vedlegg 1 - HAN personvern
**Krysskobling til andre paragrafer og regelverk**
Lov om behandling av personopplysninger (personopplysningsloven)

**Hvordan oppfylle kravet?**

Tilgangsbegrensning i målepunkt inkluderer følgende sikkerhetsområde:

- Beskyttelse mot uautorisert fysisk tilgang til AMS-utstyr (3.8.1)

Sikkerhetsområdet er forklart med kontrollmål og hensikt, med påfølgende eksempler.

### 3.8.1 Beskyttelse mot uautorisert fysisk tilgang til AMS-utstyr

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Det skal være tiltak for å forhindre misbruk av HAN-port, port for andre målere og serviceport, samt eventuelle andre fysiske grensesnitt | SKAL |

**Hensikt**

AMS-måler er utstyrt med flere porter som gir fysisk tilgang. Det gjelder HAN-port, port for andre målere og serviceport samt eventuelle andre fysiske grensesnitt. Det skal være implementert tiltak som forhindrer at disse portene kan misbrukes av uautoriserte som kan få tilgang til lokalene hvor AMS-måler er montert.

**Eksempel: HAN-port**
Nettselskapet har i utgangspunktet deaktivert HAN-porten i alle AMS-målere. Kunder kan aktivere HAN-porten slik at den begynner å sende ut forbruksdata ved å gå inn på "min side" i Nettselskapets kundeportal. Når kunder flytter eller sier opp leveransen av strøm fra nettselskapet, blir HAN-porten automatisk deaktivert. Kunden må evt. manuelt åpne HAN-port igjen på den nye adressen.

## 3.9 Opprettholdelse/ forbedring av sikkerhetsnivå i AMS ved tilkobling av andre enheter eller systemer (§ 4-6 fjerde ledd)

§

Dersom nettselskapet eller nettselskapets leverandør kobler andre enheter eller systemer til AMS, skal sikkerhetsnivået i AMS opprettholdes eller forbedres. Tilsvarende gjelder dersom sluttbruker eller tredjepart kobler seg til AMS.

**Beskrivelse av kravet**

Dette kravet omfatter tilkobling av andre enheter eller systemer til AMS, og at dette kun kan gjøres hvis sikkerhetsnivået i AMS kan opprettholdes eller forbedres. Dette gjelder både for nettselskap, nettselskapets leverandør, sluttbruker eller tredjepart.

**Hvordan oppfylle kravet?**

Opprettholdelse/forbedring av sikkerhetsnivå i AMS ved tilkobling av andre enheter eller systemer inkluderer følgende sikkerhetsområder:

- Tilkobling av eksternt utstyr (3.9.1)
- Tilkobling av utstyr i AMS lokalisert hos sluttbruker (3.9.2)

Sikkerhetsområdene er forklart med kontrollmål og hensikt, med påfølgende eksempler.

**Veileder**
HAN+AMS – om å gjøre sanntid måledata tilgjengelig for forbruker - NEK

### 3.9.1 Tilkobling av eksternt utstyr

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Nettselskapet skal eksplitt godkjenne alle enheter som kobles til AMS | SKAL |
| b. Enheter som kobles til AMS skal ikke påvirke sikkerheten negativt | SKAL |

**Hensikt**

Kun utstyr som er eksplisitt godkjent av nettselskap skal kobles til andre deler av AMS enn HAN-porten. Nettselskapet skal også eksplisitt godkjenne evt. utstyr som kobles til slike "andre enheter eller utstyr".

**Eksempel:**
Nettselskapet inngår avtale med kommunens vann- og avløpsverk om å koble automatiske vannmålere til AMS-målere i kommunen. Nettselskapet påser at datamengden fra vannmåleren ikke kan overstige en nærmere angitt maksimumsgrense, slik at vannmåleren ikke kan utgjøre en risiko for tilsiktet eller utilsiktet tjenestenekt. Data som overstiger denne grensen, skal avvises i AMS-måleren. Vannmåleren skal ha tilsvarende adgangsbegrensninger som AMS-måleren, dvs. at sluttbrukere kun får koble til enveis (kun lese) grensesnitt, og ingen ytterligere enheter kan kobles til vannmåleren uten at dette er eksplisitt godkjent av nettselskapet. Vannmåleren får kun kommunisere måleverdier via AMS-måleren, og vannmåleren får ikke anledning til å sende kommandoer eller på annet vis påvirke AMS-måleren.

### 3.9.2 Tilkobling av utstyr i AMS lokalisert hos sluttbruker

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Enheter som sluttbrukere kobler til AMS skal kun kunne lese fra, ikke skrive til AMS | SKAL |

**Hensikt**

Sluttbrukere skal kun ha mulighet til å koble seg til HAN-porten, og hvis HAN-porten er ukryptert kun dersom de eksplisitt har bedt om at den skal åpnes. HAN-porten skal være enveis, dvs. det skal kun være mulig å lese ut av porten, ikke sende data til den. Sluttbrukere kan koble til utstyr fra tredjeparter til HAN-porten, men ettersom HAN-porten er enveis, vil ikke dette kunne påvirke AMS.

**Eksempel:**
Sluttbrukeren har kontaktet Nettselskapet for å få åpnet HAN-porten, og har koblet den til en tredjeparts enhet for å administrere strømsparing i boenheten. HAN-porten sender ut forbruksdata i henhold til fastlagt skjema, men det er ikke mulig å skrive data til HAN-porten.

**Tilkobling av utstyr til AMS lokalisert hos sluttbruker**

Dette gjelder kun tilkobling av utstyr til HAN-port på AMS-måler tilknyttet sluttbrukere i lavspenningsanlegg, eller tilsvarende port for AMS-måler tilknyttet sluttbrukere i høyspenningsanlegg.

## 3.10 Internkontrollsystem (§ 4-6 femte ledd)

§

Nettselskapet skal dokumentere oppfyllelse av krav i første til fjerde ledd i et internkontrollsystem.

**Beskrivelse av kravet**

Dette kravet innebærer at nettselskapet skal etablere et internkontrollsystem, for å kunne dokumentere hvordan krav i § 4-6 første til fjerde ledd er oppfylt. Systemet skal være et oversikts- og styringsverktøy for virksomheten. Systemet skal kunne gi en rask og korrekt dokumentasjon over status i forhold til alle relevante bestemmelser etter denne forskriftsparagraf.

**Ordforklaring**

| | |
|---|---|
| Internkontroll | Bedriftens egenkontroll. |
| Internkontrollsystem | Et kvalitetssystem, styringssystem eller ledelsessystem for etterlevelse av regelverk. |

**Hvordan oppfylle kravet?**

Internkontrollsystem inkluderer følgende sikkerhetsområde:

- Internkontrollsystem for sikkerhet (3.10.1)

### 3.10.1 Internkontrollsystem for sikkerhet

| Kontrollmål: | Vurdering av krav |
|---|---|
| a. Nettselskapet skal ha et dokumentert internkontrollsystem for sikkerhet som omfatter AMS. | SKAL |

**Hensikt**

Sikre at nettselskapet etablerer et system som legger til rette for at personvern, konfidensialitet, integritet og tilgjengelighet ivaretas for alle aspekter av driften.

Den enkelte virksomhet må selv bestemme hvor omfattende systemet skal være. Bestemmelsen gir ingen avgrensning med hensyn til å bruke eller tilpasse allerede etablerte internkontrollsystemer, så lenge bestemmelsens vilkår er oppfylt gjennom å dokumentere at alle krav til sikkerhet i lov og forskrift er oppfylt.

**Eksempel: Etablering av internkontrollsystem**

For å være sikre på å kunne dokumentere hvordan krav i §4-6 første til fjerde ledd er oppfylt, har nettselskapet valgt å etablere et eget internkontrollsystem i henhold til anbefalinger fra Datatilsynet. Nettselskapet skaffer seg tilstrekkelig kunnskap om personvern og informasjonssikkerhet gjennom å engasjere en ekstern konsulent for å gjennomføre et opplæringsopplegg, og ledelsen tar ansvar for at det utarbeides retningslinjer/rutiner og at internkontrollaktiviteter gjennomføres. Formålet med internkontrollen dokumenteres, sammen med vurdering av lovlighet, nødvendighet og proporsjonalitet av tiltak. Nettselskapet beskriver de overordnede rammer for internkontrollen, og tilhørende plikter. Nettselskapet bruker malene til Datatilsynet for å lage styrende, gjennomførende, og kontrollerende dokumentasjon, og sørger for at malene tilpasses nettselskapets lokale forhold.

**Maler**

Datatilsynet Maler og støtteverktøy for etablering av internkontroll

**Standarder**

ISO/IEC 27001 – Beskrivelse (Digitaliseringsdirektoratet)

**Veileder**

Veiledning til kraftberedskapsforskriften Kapittel 2

Datatilsynet – Hvordan gjennomføre internkontroll i praksis

**Krysskobling til andre paragrafer og regelverk**

Kraftberedskapsforskriften § 2-10 Internkontrollsystem

Internkontrollforskriften

Elmålerforskriften § 55 Krav til internt kontrollsystem

# 4 Vedlegg - Sjekklister

## 4.1 **Tabell 1 Krav til nettselskap i henhold til avregningsforskriften § 4-6 første og andre ledd** (SKAL-krav er beskrevet i vanlig font, *BØR-krav* er beskrevet i kursiv)

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| **Sikkerhetsområde: Etablering og oppfølging av sikkerhetskrav** | | |
| a. Nettselskapets ledelse skal utarbeide og godkjenne overordnede sikkerhetskrav til AMS-løsningen. Disse skal dekke alle prosesser og systemer som påvirker AMS og eventuelt kraftforsyningen. Kravene skal være målbare og dokumenteres.<br>*b. Nettselskapet ledelse bør etablere et system for å følge opp og forbedre sikkerhetskravene for AMS.* | • Nettselskapets ledelse dokumenterer sitt engasjement for å få utarbeidet sikkerhetskravene og oppfølgingen av dem.<br>• Nettselskapet sørger for å ha nødvendig tilgang på kompetanse på eget sikkerhetsarbeid knyttet til AMS.<br>• Nettselskapet har utpekt en informasjonssikkerhetsansvarlig for AMS. Denne personen gis nødvendig myndighet, ansvar og opplæring samt få avsatt tilstrekkelig tid og ressurser slik at funksjonen kan ivaretas på en tilfredsstillende måte.<br>• Det gjennomføres tilstrekkelig opplæring på informasjonssikkerhet for alle nettselskapets egne og innleide ressurser.<br>• Kravene baseres på risiko- og sårbarhetsanalyse, og er tilstrekkelige for å oppnå et akseptabelt risikonivå.<br>• Sikkerhetskravene gjennomgås minimum årlig for å klarlegge om kravene er hensiktsmessige i forhold til nettselskapets behov, og kontrollere etterlevelse av forskriftskrav.<br>• Konkretiser sikkerhetskrav i konkurransegrunnlag og kontrakt med leverandør. | |

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| | | |
| **Sikkerhetsområde: Risiko- og sårbarhetsanalyse** | | |
| a. Det skal gjennomføres risiko- og sårbarhetsanalyse eller annen hensiktsmessig sikkerhetsvurdering av AMS med den hensikt å identifisere risiko forbundet med drift og sikkerhet av AMS.<br>*b. Konfigurasjon og oppsett for kritiske kommandoer, målerdata og annen informasjon i AMS løsningen bør være basert på risiko.* | • I analysen vurderes alle forhold som for eksempel kan hindre korrekt avregning, hindre tilfredsstillende funksjonalitet, sette informasjonssikkerheten i fare eller hindre kraftforsyning til sluttbrukere.<br>• Det fastsettes akseptabelt risikonivå som risikoene i risiko- og sårbarhetsanalysen skal vurderes mot. Der hvor risikonivå er høyere enn akseptabel risiko etableres tiltak slik at akseptabelt risikonivå oppnås. Omfang av og type sikkerhetstiltak er tilpasset risiko.<br>• Dersom større tiltak er nødvendig for å oppnå akseptabelt risikonivå, iverksettes tilstrekkelige midlertidige kompenserende tiltak inntil permanente tiltak er på plass.<br>• Risiko- og sårbarhetsanalysene utføres og gjennomgås årlig og ved endringer i løsninger eller i trusselsituasjon som påvirker drift og sikkerhet i AMS. | |
| **Sikkerhetsområde: Sikkerhetsavtaler** | | |
| a. Nettselskapet skal inngå sikkerhetsavtaler med alle leverandører eller enkeltpersoner som ikke er ansatt i nettselskapet dersom de skal utføre enhver form for arbeid på sentrale løsninger eller komponenter i AMS-løsningen. | • Underskrevne avtaler. | |
| **Sikkerhetsområde: Tjenesteutsetting av utrulling og/eller drift av AMS-løsningen til tredjepart** | | |

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| a. Sikkerheten i AMS skal ikke påvirkes ved at utrulling eller drift av AMS settes ut til ekstern tjenesteleverandør. | • Nettselskapet påser at de selv har tilstrekkelig kompetanse til å sette krav til sikkerhet i AMS gjennom kravspesifikasjonen, og også kunne kontrollere at kravene blir etterlevd i driftssituasjonen.<br>• Nettselskapet setter målbare krav til leverandørene.<br>• Kravene følges opp regelmessig.<br>• Nettselskapet har innsyn og forståelse av sikkerhetstiltakene som etableres og risikoen tjenesteutsettingen medfører.<br>• Nettselskapet har realistisk mulighet til å trekke tilbake avtalen ved avtalebrudd, uakseptabel risiko eller endringer i regulering.<br>• Tjenesteutsettingen påvirker ikke risiko for kraftforsyningen negativt. | |
| **Sikkerhetsområde: Elektronisk beskyttelse mot ondsinnet programvare og inntrengning** | | |
| a. Det skal etableres et system for overvåking og beskyttelse av programvaren i AMS med hensikten å oppdage og stanse ondsinnet programvare. | • Virusbeskyttelse eller tilsvarende.<br>• Beskyttelse mot målrettede og tilfeldige angrep.<br>• Implementering av ”Intrusion detection system” eller ”Intrusion prevention system”.<br>• Brannmurbeskyttelse.<br>• Logisk eller fysisk segmentering/soneinndeling av ulike deler av nettverk etc. | |
| **Sikkerhetsområde: Beskyttelse mot uautorisert fysisk tilgang til AMS-utstyr** | | |
| a. Alle rom som inneholder utstyr som er kritisk for AMS skal være i egen adgangskontrollert sone.<br>b. Komponenter i AMS utenfor adgangskontrollerte soner skal beskyttes mot uautorisert fysisk tilgang. | • Ved forsøk på uautorisert fysisk adgang sendes det et varsel til nettselskapet. Varselet logges og inneholder tidspunkt for utløsning av varselet.<br>• Det kan bevises dersom det har blitt utført uautorisert tilgang, for eksempel ved at det etterlates fysiske merker eller andre typer spor dersom noen bryter opp enheten.<br>• Kommunikasjonsinstallasjoner og - skap beskyttes mot uautorisert fysisk adgang. Ved forsøk på og uautorisert adgang sendes varsel til nettselskapet. Nettselskapet undersøker og iverksetter aktiviteter tidsriktig. | |

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| c. Alle forsøk på å få uautorisert tilgang til utstyr i AMS-løsningen eller rom med kritisk AMS-utstyr skal oppdages, straks registreres og varsles så snart som mulig. | • Varsel om uautorisert fysisk adgang følges opp av nettselskapet. | |

## 4.2 Tabell 2 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 a

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| **Sikkerhetsområde: Tilgangskontroll for system** | | |
| a. Nettselskapet skal ha prosedyrer og kriterier for tildeling, endring, sletting og verifikasjon av korrekt tilgang til kundedata samt AMS-funksjonalitet. | • Ha prosedyrer som sikrer at kun autoriserte personer kan få tilgang til, endre, slette eller utlevere målerdata eller annen sensitiv kundeinformasjon. Prosedyrene inkluderer både intern og ekstern tilgang.<br>• Nettselskapet foretar tilstrekkelig bakgrunnssjekk av personell som skal ha tilgang til å håndtere sensitive systemer og informasjon. Med tilstrekkelig menes for eksempel som minimum vandelsattest (hvis mulig), kredittsjekk og referansesjekk.<br>• Tilgang administreres på basis av forhåndsdefinerte roller og tilgangsnivåer.<br>• Tilganger tildeles, endres, fjernes og revideres basert på tjenstlig behov.<br>• Ha prosedyrer og tekniske løsninger som sikrer at kritiske operasjoner ikke kan kunne utføres av én person alene. Den som gir tilgang til funksjonen, skal ikke kunne utføre tilsvarende funksjon.<br>• Ha prosedyrer som sikrer at maskinvare som inneholder sensitiv informasjon avhendes på en sikker måte. | |

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| | • Ha tekniske løsninger for å oppdage uautorisert endring i målerdata eller personopplysninger.<br>• Ha tekniske løsninger for å forhindre uautorisert utlevering av målerdata eller personopplysninger.<br>• Ha tekniske løsninger for å loggføre dersom det utføres endringer i allerede registrerte målerdata.<br>• Ha tekniske løsninger for å loggføre dersom målerdata eller annen kundeinformasjon utleveres til autorisert tredjepart. | |
| **Sikkerhetsområde: Identifisering og autorisasjon av enheter** | | |
| a. Det skal implementeres mekanismer for å autentisere og autorisere enheter i AMS før det opprettes forbindelse mellom enheten og resten av AMS.<br>*b. Ved bruk av nettverk som nettselskapet ikke kontrollerer, f.eks. Mobilt Bredbånd (MBB), bør ekstra sterk autentisering foretas.* | • Det tillates ikke tilkobling av enheter uten at disse er autorisert og autentisert.<br>• *Hver enhet i AMS tildeles et unikt sikkerhetssertifikat som kontrolleres før det sendes/mottas data fra enheten.*<br>• Der man ikke får kontrollert eller verifisert enheten, nektes enheten tilgang til nettverket.<br>• *Sikkerhetssertifikat benyttes for å autorisere enheter i AMS.* | |
| **Sikkerhetsområde: Identifisering og autorisering av eksternt utstyr** | | |
| a. Håndholdte enheter (feltutstyr) må være autorisert og skal autentiseres av AMS - løsningen. Bruker skal være autorisert og autentisert. | • Det tillates ikke tilkobling av eksternt utstyr uten at disse er autorisert og autentisert.<br>• Hver enkelt enhet utstyres med et sikkerhetssertifikat som kontrolleres ved oppkobling mot enheter i AMS.<br>• *Det sperres for at eksternt utstyr benyttes til annet enn oppgave mot AMS.* | |

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| | • Autoriseringsprosessene er formaliserte i form av instrukser/ prosedyrer.<br>• Det er mulig å fjerne/endre autorisering av håndholdte enheter sentralt. | |
| **Sikkerhetsområde: Fjerntilgang til AMS fra tredjepart eller leverandør** | | |
| a. Det skal etableres prosedyrer for godkjenning, administrering og overvåking av eksterne tilkoblinger for vedlikehold og diagnostiske aktiviteter på alle komponenter i AMS-systemet. | • Det opprettes ikke tilkobling til tredjepart eller leverandør uten eksplisitt avtale med selskapet.<br>• Tredjepart forpliktes til å etterleve relevante sikkerhetskrav.<br>• Tredjepart benytter en sikker løsning for fjerntilgang.<br>• *Fjerntilgang tillates kun fra sikre lokasjoner som ikke medfører økt risiko.*<br>• Når eksternt vedlikehold er fullført, avslutter nettselskapet eller AMS-komponenten alle økter og eksterne tilkoblinger som er opprettet. | |

## 4.3 Tabell 3 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 b

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| **Sikkerhetsområde: Sporing av endringer** | | |
| a. Nettselskapet skal dokumentere prosedyrer for å planlegge og utføre endringer i AMS-miljøet.<br>b. Sentralsystemet skal logge alle endringer i programvare og konfigurasjon i AMS. | • Alle endringer i AMS-løsningen dokumenteres.<br>• Alle endringer testes og godkjennes før de rulles ut.<br>• Alle endringer vurderes i forkant om endringen kan medføre risiko for kritiske AMS-funksjoner eller medføre konsekvenser for kraftforsyningen.<br>• All ny programvare som innføres i AMS løsningen sikres slik at integritet ivaretas.<br>• Enheter kan verifisere at oppdatering av firmware er autorisert og at firmwaren er umodifisert og godkjent før den oppdateres.<br>• Sentralsystem med personlig innlogging og tofaktor autentisering. | |
| **Sikkerhetsområde: Oppdatert dokumentasjon av AMS-løsningen** | | |
| a. Det skal til enhver tid foreligge fullstendig og oppdatert dokumentasjon av AMS-løsningens komponenter og konfigurasjoner. | • Alle sikkerhetsrutiner og sikkerhetstiltak er dokumentert.<br>• *Dokumentasjonen er systematisert og sporbar*.<br>• Det fremkommer tydelig gyldighet, eierskap og endringshistorikk.<br>• Dokumentasjonen er beskrevet og komplett på en slik måte at enhver (både internt og evt leverandør) effektivt kan utføre vedlikehold eller feilretting.<br>• Dokumentasjonen oppbevares separat fra AMS-løsningen.<br>• Utførte kontrolltiltak er dokumenterte og etterprøvbare. | |

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| **Sikkerhetsområde: Kontroll med integriteten til programvare** | | |
| *a. Det bør etableres et system for overvåking og avdekking av uautoriserte endringer av programvare og informasjon.* | • *Utføre integritetsskanning av AMS-løsningen.*<br>• *Integriteten på programvare sjekkes ved oppstart, oppdatering og eksekvering.*<br>• *Enheten er sikret fysisk og logisk mot uautorisert oppdatering og endring av programvare.*<br>• *Endringer av programvare er testet og godkjent.*<br>• *Implementering av automatiske verktøy som varsler ved integritetsavvik.*<br>• *Enhetene i AMS verifiserer at alle spørringer og kommandoer er gyldige, har rett format og er foretatt fra autentisert og autorisert kilde.*<br>• *Sikkerhetssertifikatet benyttes for verifikasjon av kommandoeksekvering.* | |

## 4.4 Tabell 4 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 b

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| **Sikkerhetsområde: Sikkerhet i kommunikasjon i AMS-løsningen** | | |
| a. All kommunikasjon mellom måler og sentralsystem og øvrig utstyr i AMS skal foregå på en sikker måte slik at innsyn, avlytting eller manipulering av signaler og informasjon ikke er mulig.<br>*b. Signalene og informasjonen bør krypteres ende-til-ende mellom måler og HES.* | • *Krypteringsalgoritmer som benyttes for sikker kommunikasjon er som minimum FIPS-godkjent (eller ekvivalent).*<br>• *Krypteringsløsningen støtter PKI (Public Key Infrastructure) nøkkelkryptografi.*<br>• Påloggingsinformasjon som krypteringsnøkler, sikkerhetssertifikat etc kan oppdateres sentralt.<br>• *Sertifikatnøkler lagres kryptert.*<br>• Det ansees ikke tilstrekkelig å benytte den innebygde krypteringsløsningen i MBB. | |

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| | | |
| **Sikkerhetsområde: Oppbevaring av sikkerhetssertifikater og krypteringsnøkler** | | |
| a. Nettselskapet skal utarbeide retningslinjer for sikker oppbevaring av sikkerhetssertifikater og krypteringsnøkler som benyttes i AMS.<br>b. Enheten skal lagre påloggingsinformasjon, sikkerhetssertifikater og annen sikkerhetsinformasjon sikkert.<br>*c. Autentisering bør gjøres ved bruk av flere faktorer.* | • Dokumentasjon av retningslinjer.<br>• *Ved tilgang til private nøkler til sertifikater benyttes både passord og TOTP-basert sikkerhetskode.* | |

## 4.5 Tabell 5 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 d

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| **Sikkerhetsområde: Oversikt over versjoner i program- og maskinvare** | | |
| a. Nettselskapet skal ha en oppdatert oversikt over versjoner av all maskinvare, firmware, oppdateringer og programvare som benyttes i AMS løsningen. Oversikten skal oppdateres ved | • Etablere en form for sentral liste med oversikt over maskinvare, versjoner av programvare som disse benyttes etc.<br>• Alle endringer i konfigurasjoner og programvare logges.<br>• Fast prosedyre og klare ansvarsforhold for oppdatering av listen ved endringer.<br>• Automatiske systemer som gir oversikt over programvareversjoner og som kan rulle ut oppdateringer. | |

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| endringer og ved regelmessige gjennomganger. | | |
| **Sikkerhetsområde: Kontroll av ekthet av programvare** | | |
| a. Nettselskapet skal verifisere at programvare, firmware og tilhørende oppdateringer er ekte. | • Programvareoppdateringer er signert av leverandøren, og verifiseres av leverandørens offentlige nøkkel. | |
| **Sikkerhetsområde: Kontroll med sårbarheter i programvare** | | |
| a. Nettselskapet skal ha prosesser for å fange opp eventuelle kjente programvaremessige sårbarheter i sitt AMS-miljø.<br>b. Dersom man blir kjent eller varslet om sårbarheter, skal disse evalueres og eventuelt håndteres umiddelbart. | • Avtaler om varsling fra leverandør(ene) eller andre relevante samarbeidspartnere dersom det oppdages sårbarheter i sine system.<br>• Regelmessig sårbarhetsscanning av enheter og infrastruktur.<br>• Interne prosedyrer for hvordan slik informasjon skal behandles og sårbarheter håndteres.<br>• Prosedyrer som sørger for at sikkerhetsoppdateringer blir utført så raskt som praktisk mulig på en sikker måte. | |

## 4.6 Tabell 6 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 e

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| **Sikkerhetsområde: Logging og overvåking** | | |

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| a. Nettselskapet skal ha satt opp løsning og rutiner for sikkerhetslogging i den totale AMS-løsningen. | • Alle nettverkskomponenter, AMS enheter, operativsystemer, databaser, applikasjoner med videre settes opp med rett loggnivå for sikkerhet.<br>• Endringer, feil, normal og unormal aktivitet og sikkerhetshendelser logges.<br>• Loggene sikres og overvåkes sentralt for å fange opp eventuelle uønskede sikkerhetshendelser.<br>• Logger kan lagres lokalt dersom kommunikasjon mot sentralsystem ikke er tilgjengelig. Lokal logg er av tilstrekkelig omfang for å kunne håndtere forventet maksimal nedetid på kommunikasjonsløsning.<br>• Lokale og sentrale logger sikres mot uautoriserte endringer. | |
| **Sikkerhetsområde: Uavhengighet** | | |
| a. Sikkerhetsfunksjonalitet i AMS-løsningen skal ikke påvirkes ved feil i AMS eller feil konfigurasjon av annen funksjonalitet. | • Utstrakt testing av funksjonalitet i et begrenset testmiljø.<br>• Foreta regelmessig sikkerhetstesting.<br>• Ha prosess og prosedyrer for regelmessig identifikasjon og feilretting av sikkerhetssvakheter.<br>• Overvåking og varsling av unormal bruk eller trafikk. | |
| b. Hvis man kompromitterer en måler, skal ikke dette ha noen konsekvenser for andre målere eller sentralsystemet. | • Alle AMS-målere bruker unike symmetriske nøkler. | |

## 4.7 Tabell 7 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 f

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| **Sikkerhetsområde: Kontroll på sikkerhet med deaktivert eller ikke brukt funksjonalitet** | | |
| a. Funksjonalitet som er deaktivert eller ikke tilgjengelig for bruk skal ikke påvirke sikkerheten i løsningen. | • Utstrakt testing av funksjonalitet i et begrenset testmiljø.<br>• Foreta regelmessig sikkerhetstesting.<br>• Ha prosess og prosedyrer for regelmessig identifikasjon og feilretting av sikkerhetssvakheter.<br>• Overvåking og varsling av unormal bruk eller trafikk. | |
| **Sikkerhetsområde: Avviks- og hendelseshåndtering** | | |
| a. Nettselskapet skal etablere en dokumentert prosess for avviks- og hendelsesregistrering og -håndtering. | • Alle avvik følges opp.<br>• Prosessen inneholder retningslinjer for hvordan avvik skal behandles. De kan for eksempel være;<br>  ○ klassifisering av hendelser,<br>  ○ roller og ansvar<br>  ○ plan for håndtering og avklaring<br>  ○ eskalering<br>  ○ terskel for varsling til NVE<br>• Avvik som det ikke gjøres noe med, er godkjente.<br>• Alle avvik fra egne og eksterne krav dokumenteres.<br>• Alle avvik som ikke er lukket følges opp til de lukkes.<br>• Utstrakt testing av funksjonalitet i et begrenset testmiljø.<br>• Foreta regelmessig sikkerhetstesting.<br>• Ha prosess og prosedyrer for regelmessig identifikasjon og feilretting av sikkerhetssvakheter.<br>• Overvåking og varsling av unormal bruk eller trafikk. | |

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| **Sikkerhetsområde: Katastrofehåndtering og –øvelser** | | |
| a. Nettselskapet skal ha beredskapsplaner og forberedte løsninger for å sikre beredskap, kontinuitet og evne til å håndtere katastrofer knyttet til informasjonssikkerhet og AMS.<br>b. Det skal jevnlig gjennomføres øvelser for å håndtere omfattende sikkerhetshendelser og -katastrofer. | • Beredskapsplaner og løsninger evalueres regelmessig og i forbindelse med evaluering av øvelser.<br>• Planene for og resultatene fra øvelsene dokumenteres. Avdekkes gap eller mangler etter øvelsene, tas det hensyn til dette i evalueringen eller oppdateringen av beredskapsplaner.<br>• *Øvelser inkluderer feilsituasjoner, sikkerhetshendelser i kombinasjon med ekstremvær eller andre relevante hendelser.*<br>• *Øvelsene inneholder elementer av gjenoppretting etter katastrofer.*<br>• Det gjennomføres øvelser minimum årlig. | |
| **Sikkerhetsområde: Sikkerhetskopier og gjenoppretting** | | |
| a. Det skal foreligge sikkerhetskopier av all kritisk programvare, konfigurasjoner, dokumentasjon av alle relevante komponenter i AMS-løsningen.<br>b. Det skal foretas jevnlig sikkerhetskopiering av måledatabasen.<br>*c. Sikkerhetskopiene bør lagres på et sikkert sted et annet fysisk sted enn der originalene befinner seg.*<br>d. *Sikkerhetskopiene bør umiddelbart gjenopprettes på et* | • Dokumentasjon av sikkerhetskopieringsrutiner.<br>• *Nettselskapet tester med jevne mellomrom at gjenoppretting av sikkerhetskopiene fungerer etter hensikten.* | |

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| *test/skyggesystem for å verifisere at de er korrekt generert.* | | |

## 4.8 Tabell 8 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 g

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| a. Det skal være tiltak for å forhindre misbruk av HAN-port, port for andre målere og serviceport. | • HAN-port er stengt i utgangspunktet, åpnes kun ved anmodning, og stenges automatisk ved flytting. | |

## 4.9 Tabell 9 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 fjerde ledd

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| **Sikkerhetsområde: Tilkobling av andre enheter eller systemer til AMS** | | |
| a. Nettselskapet skal eksplitt godkjenne alle enheter som kobles til AMS.<br>b. Enheter som kobles til AMS skal ikke påvirke sikkerheten negativt. | • Alle enheter autentiserer seg mot sentralsystemet.<br>• Kommunikasjon fra enheter som ikke er autentisert ignoreres. | |
| **Sikkerhetsområde: Tilkobling av andre enheter eller systemer til AMS** | | |
| a. Enheter som sluttbrukere kobler til AMS skal kun kunne lese fra, ikke skrive til AMS. | • Dokumentasjon av funksjonalitet av HAN-port.<br>• Testing av HAN-port i et begrenset testmiljø. | |

## 4.10 Tabell 10 Krav til nettselskapet i henhold til avregningsforskriften § 4-6 femte ledd

| Sikkerhetsområde/Kontrollmål | Eksempler for å oppnå kontrollmål | Status/evaluering |
|---|---|---|
| **Sikkerhetsområde: Internkontrollsystem for sikkerhet** | | |
| Nettselskapet skal ha et dokumentert internkontrollsystem for sikkerhet som omfatter AMS. | • Dokumentasjon. | |

# 5 Vedlegg – Kobling mellom sikkerhetskrav i avregningsforskriften og tiltak i NSM sine grunnprinsipper

NSMs grunnprinsipper for IKT-sikkerhet anbefales for alle norske virksomheter, og bl.a. kraftberedskapsforskriftens krav til informasjonssikkerhet er i stor grad basert på grunnprinsippene. Grunnprinsippene er i stor grad anvendbare på industrielle systemer som smart grid.

### 5.1.1 Tabell 11 NSMs grunnprinsipper for IKT-sikkerhet

| Identifisere og kartlegge | | Beskytte og opprettholde | | Oppdage | | Håndtere og gjenopprette | |
|---|---|---|---|---|---|---|---|
| 1.1 | Kartlegg styrings-strukturer, leveranser og understøttende systemer | 2.1 | Ivareta sikkerhet i anskaffelses- og utviklings-prosesser | 3.1 | Oppdag og fjern kjente sårbarheter og trusler | 4.1 | Forbered virksomheten på håndtering av hendelser |
| 1.2 | Kartlegg enheter og programvare | 2.2 | Etabler en sikker IKT-arkitektur | 3.2 | Etabler sikkerhetsover-våkning | 4.2 | Vurder og klassifiser hendelser |
| 1.3 | Kartlegg brukere og behov for tilgang | 2.3 | Ivareta en sikker konfigurasjon | 3.3 | Analyser data fra sikkerhetsovervåkning | 4.3 | Kontroller og håndter hendelser |
| | | 2.4 | Beskytt virksomhetens nettverk | 3.4 | Gjennomfør inntrengnings-tester | 4.4 | Evaluer og lær av hendelser |
| | | 2.5 | Kontroller dataflyt | | | | |
| | | 2.6 | Ha kontroll på identiteter og tilganger | | | | |
| | | 2.7 | Beskytt data i ro og i transitt | | | | |
| | | 2.8 | Beskytt e-post og nettleser | | | | |
| | | 2.9 | Etabler evne til gjenoppretting av data | | | | |
| | | 2.10 | Integrer sikkerhet i prosess for endringshåndtering | | | | |

Grunnprinsippene er delt i 4 kategorier (Identifisere og kartlegge; Beskytte og opprettholde; Oppdage; Håndtere og gjenopprette), og hvert prinsipp er detaljert i et antall tiltak. Tabell 12 viser kobling mellom sikkerhetskrav i avregningsforskriften og relevante tiltak fra NSMs grunnprinsipper.

### 5.1.2 Tabell 12 Kobling mellom sikkerhetskrav i avregningsforskriften og tiltak i NSMs grunnprinsipper

| Forskriftskrav | Kort beskrivelse | Tiltak i NSMs grunnprinsipper | I hvilken grad dekker tiltakene forskriftskravet? |
|---|---|---|---|
| § 4-6 a) | Godkjennelse av enheter og brukere som skal kommunisere til eller i AMS | 1.2.1<br>1.2.2<br>1.2.3<br>1.3.1<br>1.3.2<br>2.6.2<br>2.6.3<br>2.6.6 | Dekkes fullt ut |
| § 4-6 b) | Loggføring av endringer av programvare og konfigurasjon av dataprogram i AMS | 1.2.4<br>2.2.1 d)<br>2.10.1 | Dekkes i stor grad, men sier ikke eksplisitt at endringer skal spores tilbake til enkeltbruker |
| § 4-6 c) | Ende-til-ende kryptering i kommunikasjonen mellom AMS-måler og sentralsystem | 2.4.2<br>2.7.1<br>2.7.2<br>2.7.4 | Dekkes i stor grad, selv om ende-til-ende-kryptering ikke angis eksplisitt. Imidlertid vil ikke ende-til-ende-kryptering være et krav dersom nett-selskapet kontrollerer (og kan forhindre uvedkommendes tilgang til) alle steder informasjonen er ukryptert |
| § 4-6 d) | Oppdatering av programvare i AMS | 2.1.2<br>2.10.4<br>3.1.3<br>2.3.1 | Dekkes fullt ut |
| § 4-6 e) | Sikkerhet i AMS-målere skal ikke påvirkes av hverandre | 2.2.5<br>2.3.4<br>2.5.3<br>2.7.1 | Dekkes i stor grad, men sier ikke eksplisitt at alle målerne skal ha forskjellige symetriske nøkler |
| § 4-6 f) | Funksjonalitet i AMS skal fungere til enhver tid. Funksjoner som ikke brukes, skal deaktiveres | 2.3.3<br>2.9.1 | Andre del av kravet dekkes fullt ut |
| § 4-6 g) | Kontroll på tilgang til AMS-målerens grensesnitt | | Dekkes ikke (for spesifikt til å dekkes av grunnprinsipper) |

NVE

Reguleringsmyndigheten
for energi – RME


Reguleringsmyndigheten for energi

MIDDELTHUNS GATE 29

POSTBOKS 5091 MAJORSTUEN

0301 OSLO

TELEFON: (+47) 22 95 95 95

www.reguleringsmyndigheten.no