Årsberetning vedrørende program for intern overvågning Sydfyns Elforsyning Net A/S (SEN) – 2016

1 Indledning

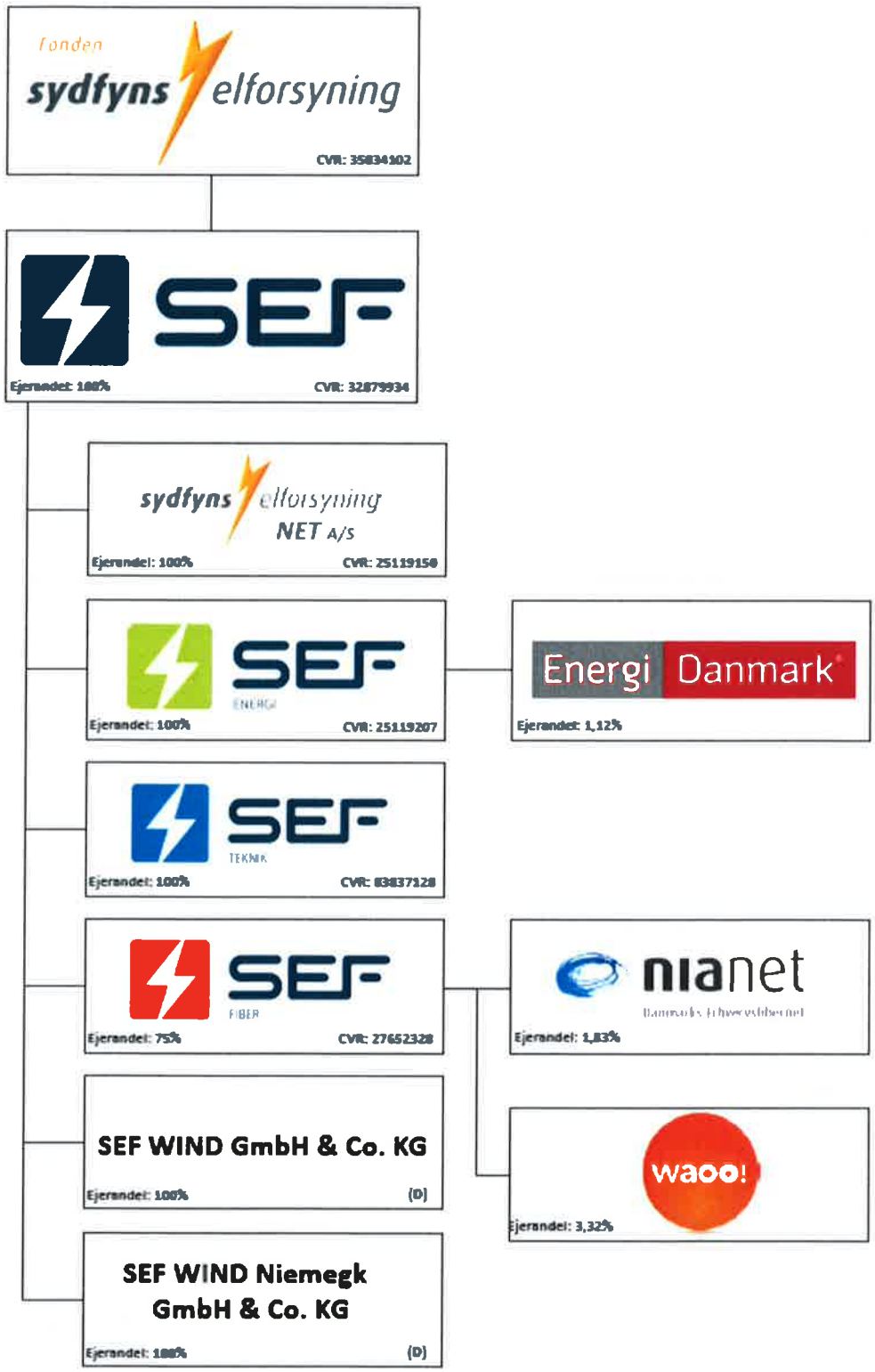
Sydfyns Elforsyning Net A/S (SEN) er underlagt reglerne for etablering af et program for intern overvågning i henhold til BEK nr. 980 af 06.10.2011 om program for intern overvågning for net- og transmissionsvirksomheder og Energinet.dk i henhold til lov om elforsyning.

Nærværende årsberetning om intern overvågning hos SEN for kalenderåret 2016 anmeldes til Energitilsynet inden den 1. juni 2017 i henhold til bekendtgørelsens §5.

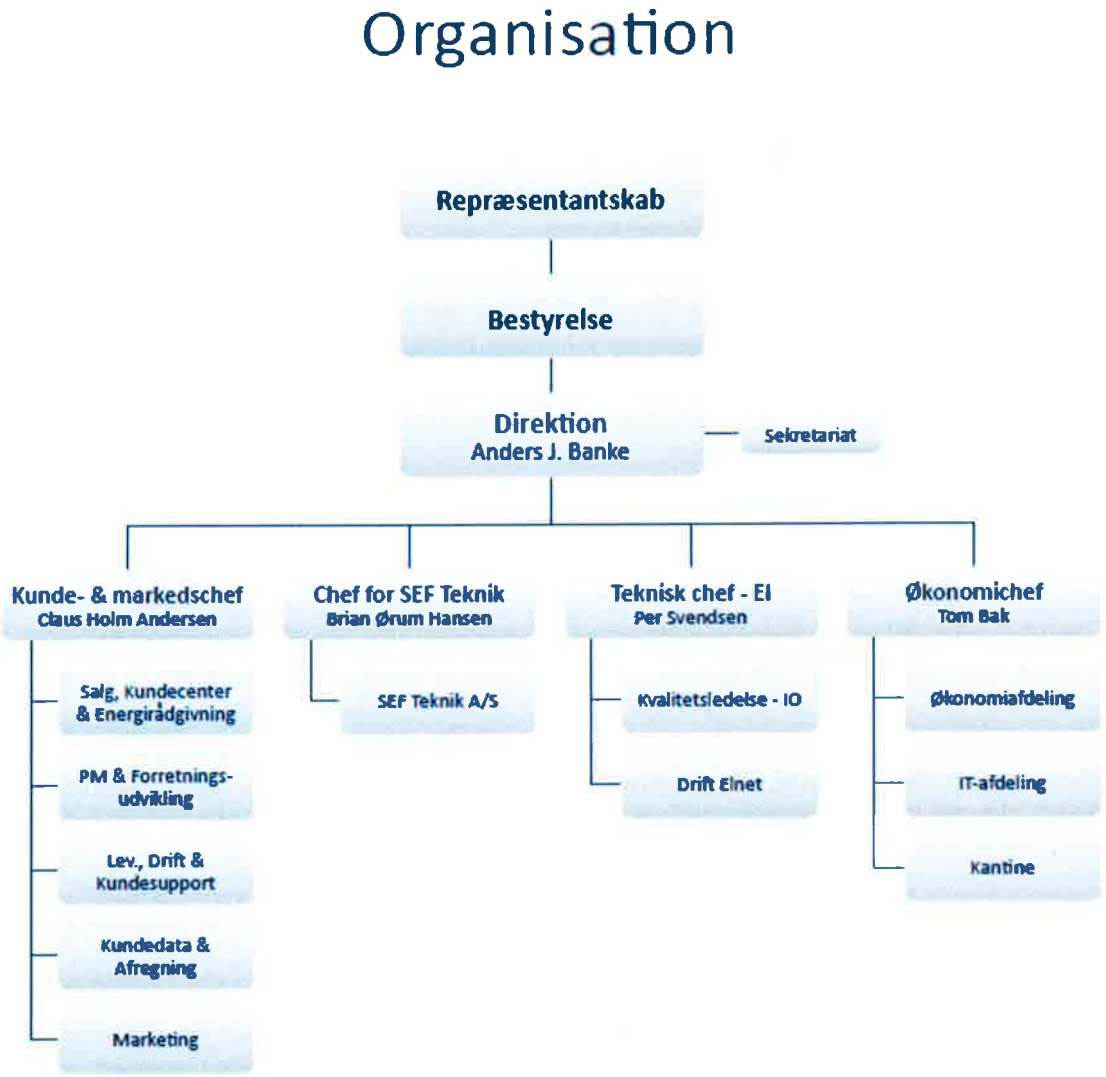
2 Koncernstruktur

SEN A/S indgår i koncernen SEF A/S:
Den erhvervsdrivende fond Sydfyns Elforsyning har i 2016 drevet hele sin virksomhed gennem de underliggende 100 % ejede selskaber. Aktieselskabet Sydfyns Elforsyning A/S har i koncernen samtlige rettigheder og forpligtelser, aktiver og passiver fra den erhvervsdrivende fond, og det er således dette selskab, der er ejer af og moderselskab for de underliggende selskaber i koncernen. Endvidere er samtlige medarbejdere i koncernen ansat i SEF A/S, der således leverer arbejdskraften til de forskellige selskaber i koncernen.
SEN A/S har derudover dog egen ansat ledelse, som forudsat i elforsyningsloven.

2 Koncernstruktur - fortsat



3 Organisation



Pr. 31.12.2016 var der 80 ansat

Der er ikke sket væsentlige ændringer i organisationen i 2016 ud over personaletilpasning. Alle nye medarbejdere gennemgår introduktionsforløb, hvor de bl.a. instrueres om Intern Overvågning.

4 Gennemførelse og kontrol af program for intern overvågning

SEF A/S har et kvalitetsledelsessystem – QMS (**Q**uality **M**anagement **S**ystems), der er certificeret i henhold til ISO 9001:2008. Program for intern overvågning er sammen med andre juridiske krav og myndighedskrav implementeret i QMS. Efterprøvning, dokumentstyring og kontrol foretages derfor systematisk og styres i kvalitetsledelsessystemet. QMS er udvidet med procedurer for informationssikkerhed.

Program for intern overvågning er beskrevet i proceduren "Intern Overvågning", som er vedlagt årsberetningen som bilag. Proceduren er under løbende revision i forhold til organisation m.m.

I henhold til program for Intern Overvågning rapporteres gennemførelsen af programmet iht. til de opstillede punkter:

1. Adgang til og drift af distributionsnettet skal ske på ikke-diskriminerende vis.
2. Netselskabet må ikke i sin kundekontakt favoriserer bestemte selskaber.
3. Krav til habilitet i ledelsen skal overholdes.
4. Netselskabet skal indgå alle aftaler på markedsmæssige vilkår.
5. Krav om regnskabsmæssig adskillelse skal overholdes.
6. Krav om selskabsmæssig udskillelse af aktiviteter, der ligger uden for netbevillingen.
7. Kommunikation med elhandlere om konkrete aftagenumre skal ske via datahubben.
8. Forretningsmæssige følsomme oplysninger skal behandles fortroligt, og hvis oplysninger kan videregives, skal det ske ikke-diskriminerende.
9. Oplysninger om netselskabets egne aktiviteter, som kan være forretningsmæssigt fordelagtige, må ikke videregives på diskriminerende måde.
10. Netselskabet skal sikre klarhed om sin særskilte identitet.
11. Netselskabet skal have faktisk og retlig råderet over egen hjemmeside.

Ad 1)
Ifølge bekendtgørelsen om etablering af program for intern overvågning skal netvirksomheden sikre adgang til nettet i forbindelse med tilslutning af nye kunder, vedligeholdelse af nettet samt udbygning af nettet.

Kunder på nettet behandles ensartet i henhold til selskabets betingelser for adgang til og brug af elnettet iht. "Standardaftale mellem Netselskab og Elleverandør om brug af Distributionsnettet – gældende pr. 01.04.2016", samt "Vilkår for Serviceniveauet mellem Netselskab og Elleverandør" der er i overensstemmelse med Dansk Energis branchestandard.

Udbygning af nettet sker ud fra objektive nettekniske betragtninger, hvorved det sikres, at favorisering eller diskrimination af kunder ikke finder sted.

Vedligeholdelse af nettet sker ud fra en målsætning om, at kunden altid er i centrum, uanset størrelse og gennem indberetning af afbrudsstatistik til Dansk Energi sikres, at der er fokus på kvalitet i levering.

Medarbejderne er således informeret om, at udbygnings- og vedligeholdelsesaktiviteter skal udføres på ikke diskriminerende måde.

Der er ikke modtaget klager i forbindelse med behandling af tilslutnings- eller vedligeholdelsesaktiviteter i netselskabet.

Ad 2)
Alle medarbejdere med kundekontakt er orienteret om formålet med etablering af det interne overvågningsprogram i SEN samt orienteret om, at de ikke i deres kundekontakt må favorisere bestemte selskaber, kunder, leverandører, konsulenter, håndværkere m.fl. Alle samarbejdspartnere behandles efter samme principper og ikke-diskriminerende. Der gennemføres intern audit og der henvises til procedure "IT Adfærdskodeks og telefonpolitik". Medarbejderne får bl.a. ved afdelingsmøder opfrisket og repeteret

reglerne omkring intern overvågning, ligesom nye medarbejdere introduceres til reglerne straks efter ansættelsen.

Ad 3)
SEN har ca. 32.000 tilsluttede målepunkter og er derfor ikke omfattet af de særlige regler om habilitet, som er fastsat i elforsyningslovens § 45 (< 100.000).

Ad 4)
Koncerninterne aftaler om omkostningsfordeling godkendes i bestyrelserne i forbindelse med bestyrelsesgodkendelse af de koncernforbundne selskabers budgetter.

Der er indgået følgende koncerninterne aftaler:
- Samarbejdsaftale mellem SEN A/S og SEF Energi A/S om køb af nettab.
- Samarbejdsaftale mellem SEN A/S og SEF A/S om køb af energirådgivning.
- Samarbejdsaftale mellem SEN A/S og SEF Teknik A/S om målerudskiftning.

Ingen af de koncerninterne aftaler har været i udbud, men de aftalte priser observeres og kontrolleres op mod gennemsnitlige markedspriser inden for de respektive samarbejdsområder og – brancher.

Ad 5)
SEN udfører kun aktiviteter i henhold til netbevillingen i SEN og er ikke involveret i transmission.
Der opretholdes selskabsmæssig adskillelse mellem SEN og de øvrige selskaber i koncernen ved så direkte omkostningskontering som muligt og regnskaberne bliver revideret af statsautoriseret revisor.

SEF A/S' fordelingsnøgler vedr. koncernens fællesfunktioner er udarbejdet, så det sikres, at alle posteringer vedr. fællesfunktioner så vidt muligt fordeles efter omkostningsbyrde og føres direkte på afdelinger via projektstyring. Alle medarbejdere fører timeregnskab over de daglige arbejdsopgaver. Desuden bliver SEN Benchmarket mod øvrige netselskaber i Danmark.

Ad 6)
Koncernens aktiviteter vedrørende elinstallation (SEF Teknik A/S), bredbånd (SEF Fiber A/S) og øvrige kommercielle aktiviteter (SEF Energi A/S) herunder elhandel og salg af naturgas, er selskabsmæssigt og juridisk udskilt fra netselskabet i særskilte aktieselskaber.

Denne udskillelse er omfattet af den ordinære revision af koncernen, og der vurderes ikke at være behov for yderligere tiltag på dette område.

SEN varetager kun aktiviteter som vedrører netbevillingen. Aktiviteter som eks.: "drift og vedligeholdelse af vejbelysning" samt "driftsledelse af private 10 kV anlæg" varetages i koncernens kommercielle selskaber.

Det bemærkes, at SEN med sine ca. 32.000 målepunkter godt kunne drive sideordnede aktiviteter i SEN, såfremt de samlede indtægter herfra udgør mindre end 5% af omsætningen i netselskabet.

Ad 7)
Kommunikation mellem elhandlere, SEN og EnergiNet.dk om konkrete aftagenumre sker via datahubben i henhold til forskrifter udstedt af EnergiNet.dk. Herved sikres formålet om at der skabes vandtætte skodder og stille alle elhandlere ens.

Der gennemføres introduktion for alle nyansatte hvor der informeres om koncernens mange funktioner. Her informeres der særligt om det forhold, at koncernen består af både en kommerciel del og en monopol del og de særlige spilleregler som gælder her.

Ad 8)
Oplysninger i koncernens kundedatabase betragtes og behandles alle som følsomme oplysninger.

Der oplyses alene om forbrug, bl.a. i relation til leverandørskifte, kun skriftligt til kunden, eller til el-leverandøren, såfremt leverandøren har fuldmagt fra kunden. Selskabets ansatte, samt de medarbejdere i koncernen, der har adgang til kundedatabasen, er alle instrueret i at behandle oplysninger fortroligt, idet disse oplysninger således alene anvendes til at gennemføre selskabets elforsyningsaktiviteter i overensstemmelse med elforsyningsloven.

Alle oplysninger i databasen over el-kunder samt SEN´s tekniske data betragtes som forretningsmæssigt følsomme, med mindre det udtrykkeligt er angivet i lov eller bekendtgørelse, at de skal udleveres på anfordring til rette vedkommende.

Dokumentationen er lagt ind i et elektronisk system, hvor der bl.a. er registreret alle informationsaktiver og – ejere. Informationsaktiverne er klassificeret efter følsomhed. Alle medarbejdere registreres i koncernens HR-system, hvor kompetencer og adgangsrettigheder administreres og opsættes via intern kommunikation mellem HR-systemet og IT- / Økonomiafdelingen.

Databasen med kundeoplysninger er derfor adgangsbegrænset til det personale, som har et arbejdsbetinget behov for at have adgang hertil. Adgangen er sikret ved passwords iht. QMS proces "16 – IT Adgangsstyring for interne og eksterne medarbejdere". Denne er vedlagt årsberetningen som bilag.

Der har ikke – siden sidste år – været modtaget klager i forbindelse med behandling af forretningsmæssige følsomme oplysninger.

Ad 9)
Koncernens ansatte instrueres løbende i og bekræfter deres kendskab til, bl.a. i forbindelse med intern audit i ISO 9001, at oplysninger om selskabets egne aktiviteter, der kan være fordelagtige for andre at have kendskab til, ikke på diskriminerende måde må videregives til andre. Dette drøftes også på afdelingsmøder i de enkelte afdelinger. Oplysningerne betragtes som fortrolige og behandles i henhold til procedurer for informationssikkerhed, bl.a. "IT Adfærdskodeks og telefonpolitik", som er vedlagt årsberetningen som bilag.

Alle medarbejdere bekræfter ovennævnte ved deres underskrivelse af ansættelseskontrakten.

Der er ikke – siden sidst år – modtaget klager i forbindelse med behandling af forretningsmæssige fordelagtige oplysninger.

Ad 10)
Der fokuseres på områder, hvor der kan være risiko for diskriminerende adfærd, fælles markedsføring og henvisning til egen elinstallationsforretning. Disse aktiviteter holdes adskilte og medarbejderne får bl.a. ved afdelingsmøder opfrisket og repeteret reglerne omkring intern overvågning, ligesom nye medarbejdere introduceres til reglerne straks efter ansættelsen.

Den 01.04.2016 blev Engrosmodellen idriftsat. Dette afstedkom flere tiltag som skal sikre, at SEN i sit kommunikationsarbejde og sine identitetsstrategi ikke skaber uklarhed om virksomhedens særskilte identitet.

Det øgede kommunikationskrav har bl.a. betydet, at SEN kun kommunikerer med elleverandørerne om konkrete aftagenumre via Datahubben for at sikre anonymitet og mindske risikoen for diskrimination.

Ligeledes er der gjort tiltag til sikring og tydeliggørelse af SEN´s særlige identitet. Dette er bl.a. sket i form af SEN´s egen hjemmeside (www.SEN-NET.dk), SEN´s egen mail (kontakt@SEN-NET.dk), SEN´s eget brevpapir, SEN´s eget telefonnummer, nye SEN visitkort og SEN´s logo og navn er valgt forskelligt fra de øvrige koncernforbundne selskaber.

Ad 11)
Netselskabet skal have faktisk og retlig råderet over egen hjemmeside
Hjemmesiden www.SEN-NET.dk er helt adskilt fra den kommercielle hjemmeside, således at SEN´s hjemmeside kun omfatter information og bestemmelser vedr. netselskabet.

Direktøren har udpeget QMS-koordinatoren og teknisk chef for SEN som den IO-ansvarlige.
Til begrundelse for QMS-koordinatorens uafhængighed kan følgende oplistes:

- QMS-koordinatoren er ansvarlig for funktioner, som yder service til den øvrige virksomhed og er som sådan uafhængig og neutral i forhold til den øvrige forretning.
- Samtidig har QMS-koordinatoren stort indblik i og kan få adgang til diverse oplysninger i de forskellige forretningsområder – samtidig med, at han som QMS-koordinator er neutral i forhold til de forskellige forretningsområder.
- SEF-koncernen er certificeret efter standarden ISO 9001 – kvalitetsledelse, hvor SEF bliver eksternt auditeret en gang om året.
- Det er indføjet i QMS-koordinatorens Funktions- og jobbeskrivelse, under særligt ansvar, at han uden ophold og indblanding fra direktøren kan orientere Energitilsynet i tilfælde af observationer, der strider imod Bekendtgørelsen om Intern Overvågning.

Intern Overvågning indgår som et fast punkt på de kvartalsmæssige ledelsesevalueringsmøder, hvor der følges op på status for information om IO. Her vurderes evt. registreringer af hændelser om brud på retningslinjer. Der har været gennemført 4 møder i 2016 og 1 i 2017 der kan bl.a. fremhæves flg. konklusioner fra møderne vedr. I/O-punkter:

- **08.03.2016 – nr. 87** Der er ikke registreret diskriminerende hændelser i Q3 og Q4 i 2015. AJB har den 15.02.2016 modtaget rapport om IO forhold ved SEF for 2015, denne skal forelægges bestyrelsen.
- **23.05.2016 – nr. 88** Der er ikke registreret diskriminerende hændelser i Q1 i 2016. AJB har den 15.02.2016 modtaget rapport om IO forhold ved SEF for 2015, denne skal forelægges bestyrelsen. Der indsendes IO årsrapport vedr. program for Intern Overvågning – SEN A/S inden den 31.05.2016. PS er ansvarlig for dette.

- **30.08.2016 – nr. 89** Der er ikke registreret diskriminerende hændelser i Q2 i 2016.

- **15.11.2016 – nr. 90** Der er ikke registreret diskriminerende hændelser i Q3 i 2016.

- **22.02.2017 – nr. 91** Der er ikke registreret diskriminerende hændelser i Q4 i 2016. Den 01.04.2016 blev Engrosmodellen idriftsat. Dette afstedkom flere tiltag som skal sikre, at SEN i sit kommunikationsarbejde og sine identitetsstrategi ikke skaber uklarhed om virksomhedens særskilte identitet. Det øgede kommunikationskrav har bl.a. betydet, at SEN kun kommunikerer med el-leverandørerne om konkrete aftagenumre via Datahubben for at sikre anonymitet og mindske risikoen for diskrimination. Ligeledes er der gjort tiltag til sikring og tydeliggørelse af SEN´s særlige identitet. Dette er bl.a. sket i form af SEN´s egen hjemmeside (www.SEN-NET.dk), SEN´s egen mail (kontakt@SEN-NET.dk), SEN´s eget brevpapir, SEN´s eget telefonnummer, nye SEN visitkort og SEN´s logo og navn er valgt forskelligt fra de øvrige koncernforbundne selskaber.

Der er løbende over året gennemført interne audits i hele koncernen og herunder gennemgås og drøftes IO-retningslinjer for de enkelte afdelinger. Det er blevet kontrolleret, at funktionerne bliver udført neutralt ligesom eventuelle hændelser eller tvivlsspørgsmål bliver rapporteret og belyst.
De medarbejdere, der deltager i auditeringen, underskriver en medarbejdererklæring, Bekræftelse af intern audit i Intern Overvågning. Der er ikke sket ændringer i brugen af medarbejdererklæringer.

Den IO-ansvarlige tilsendes hvert kvartal information fra hvert chefområde vedrørende registrerede hændelser, der ikke har været i overensstemmelse med fortroligheds- og ikke-diskriminationsreglerne. Rapporteringerne behandles således, at direktøren senest 1. april kan orientere bestyrelsen om status på program for intern overvågning. Den IO-ansvarlige har den 15.02.2017 rapporteret til direktøren om intern overvågning hos SEF i 2016. Dette er forelagt bestyrelsen på bestyrelsesmøde den 30 marts 2017.

5 Tiltag i det forløbne år

Den IO-ansvarlige holder sig løbende orienteret på området gennem samarbejde og dialog med Dansk Energi og Energitilsynet. Der er igennem hele året taget tiltag til at informere om Intern Overvågning gennem deltagelse i afdelingsmøder og ved intern audit.

Svendborg, den 24. maj 2017

Sydfyns Elforsyning Net A/S

Anders J. Banke
Direktør

Per Svendsen
IO-ansvarlig

Fåborgvej 44 • 5700 Svendborg
CVR: 25119150 • Tlf.: 62 21 27 71

Bilag:
- Årsrapport 2016 for SEF Net A/S
- QMS Procedurerne
    - QMS kopi 14.05.2017 – Intern Overvågning
    - QMS kopi 14.05.2017 – IT-Adgangsstyring for interne og eksterne medarbejdere
    - QMS kopi 14.05.2017 – IT Adfærdskodeks
    - QMS kopi 14.05.2017 – Risikovurdering og - håndtering

Intern Overvågning.

1 Formål

SEF-koncernens interne overvågningsprogram er foranlediget af bekendtgørelse nr. 980 af 6. oktober 2011, Bek. om program for intern overvågning for net - og transmissionsvirksomheder og Energinet.dk i henhold til lov om elforsyning

Det interne overvågningsprogram justeres efter behov, herunder foretages hvert år audit for koncernens medarbejdere, således at selskabet kan vurdere konsekvensen af eventuelle klager eller hændelser samt foretage generel opdatering af de berørte medarbejdere og ændre procedurer i nødvendigt omfang.

2 Anvendelsesområde

2.1 Krav om intern overvågning

Kravet om intern overvågning gælder net selskabet Sydfyns Elforsyning Net A/S. Bestemmelserne vedrørende habilitet er ikke gældende for SEF-koncernen, da antal tilsluttede kunder i Sydfyns Elforsyning Net A/S er under 100.000.

Samtlige medarbejdere i SEF-koncernen er ansat i moderselskabet SEF A/S. Sydfyns Elforsyning Net A/S har dog selvstændig ledelse. Medarbejderne i moderselskabet udfører arbejder for alle selskaber i koncernen. Det interne overvågningsprogram omfatter de arbejdsopgaver, der af moderselskabets medarbejdere udføres for Sydfyns Elforsyning Net A/S. Programmet omfatter endvidere de arbejdsopgaver, som medarbejderne udfører for andre selskaber i koncernen, når medarbejdernes viden fra arbejdet for Sydfyns Elforsyning Net A/S kan give mulighed for misbrug. I det omfang arbejdsopgaver udføres af selskaber uden for koncernen, udarbejdes særskilte procedurer for dette arbejde, f.s.v. arbejdet er omfattet af bekendtgørelsen om intern overvågning.

2.2 Ledelse, opgaver og organisation

Fonden Sydfyns Elforsyning er en erhvervsdrivende fond, hvorunder de øvrige selskaber er placeret.

SEF A/S er moderselskab for Sydfyns Elforsyning Net A/S, SEF Energi A/S, SEF Fiber A/S og SEF Teknik A/S.

SEF A/S øverste myndighed er repræsentantskabet. Repræsentantskabet vælger selskabets bestyrelse, der ansætter selskabets direktør.

Sydfyns Elforsyning Net A/S har ca. 32.000 netkunder og har kun aktiviteter i henhold til net bevillingen i Sydfyns Elforsyning Net A/S og har ikke bevilling til transmissionsvirksomhed. Elforsyningslovens § 45 vedrørende habilitetskrav for selskabets bestyrelsesmedlemmer, direktør og øverste daglige ledelse (ledelsesmæssig "unbundling") er ikke gældende. Selskabet er således alene omfattet af almindeligt gældende habilitetsregler.

SEF A/S' arbejdsopgaver.
SEF A/S er moderselskab for såvel selskaberne med bevillingsopgaver (Sydfyns Elforsyning Net A/S) som for de kommercielle selskaber, SEF Energi A/S, SEF Fiber A/S og SEF Teknik A/S– vist på koncernoversigt på SEF's hjemmeside - klik her.

Samtlige medarbejdere i koncernen er ansat i SEF A/S som illustreret på Organisationen - Startside
SEF er organisatorisk opdelt i følgende områder:

Direktion
Sekretariat
Kunde/Marked
Økonomi / IT / Kantine
Drift El
SEF Teknik

Opgaver i koncernen.
De øvrige selskaber i koncernen har således ikke egne ansatte bortset fra net selskabet, der jf. elforsyningsloven har en ansvarlig ledelse. Alene net selskabet er omfattet af bestemmelserne om intern overvågning.

Opgaver, der udføres af selskaber uden for koncernen.
Netselskabet bestiller i visse situationer arbejdsopgaver udført af eksterne samarbejdspartnere, fx leverandører. I det omfang eksterne leverandører kommer i berøring med fortroligt materiale, får adgang til informationer, eller får adgang til at henvende sig til omverdenen på vegne af SEF, vil der blive udarbejdet særlige procedurer, der sikrer, at bestemmelserne vedr. intern overvågning bliver overholdt også i disses arbejde.

Det samme gælder i det omfang, eksterne samarbejdspartnere kommer i berøring med information hos andre selskaber i koncernen, hvor dette materiale hidrører fra netvirksomheden og er underlagt begrænsninger i anvendelsen. Se også Adgangsstyring for interne og eksterne medarbejdere.

Det arbejde, moderselskabet udfører for netselskabet, er fuldt ud omfattet af den interne overvågning, medens det arbejde, som moderselskabet udfører for andre selskaber i koncernen, alene er omfattet af de dele af reglerne om intern overvågning, der indeholder risiko for misbrug af informationer, som er opnået i kraft af arbejdet for net virksomheden.

3 Ansvar og myndighed

3.1 Overordnet ansvar

Direktøren for SEF A/S er ansvarlig for, at der findes et program for intern overvågning i Sydfyns Elforsyning Net A/S og at det er implementeret således at alle medarbejdere er bekendt med reglerne i programmet.

Direktøren sikrer sig hvert år senest 15. februar via den udpegede IO-ansvarlige at modtage rapport fra chefgruppens medlemmer vedrørende overholdelse af reglerne for intern overvågning. Direktøren orienterer senest 1. april hvert år bestyrelsen om status for selskabets interne overvågningsprogram, herunder om hændelser og forslag til ændringer i programmet.

Direktøren tager initiativ til at sikre, at selskabet senest den 1. juni hvert år kan offentliggøre og indsende beretning til Energitilsynet om selskabets interne overvågning.

Direktøren er ansvarlig for Sydfyns Elforsyning Net A/S' interne overvågning samt for delegering af arbejdsopgaver vedr. intern overvågning til afdelingslederne, herunder:

- Sikring af gennemførelse af de enkelte afdelingers overvågningsprogram
- Sikring af kontrol af de enkelte afdelingers interne overvågningsprogram
- Udarbejdelse af endelig årsrapport.

3.2 IO ansvarlig koordinator

Direktøren har udpeget en IO ansvarlig koordinator, der tager initiativ til at sikre udarbejdelse af rapporter. QMS-koordinatoren er udpeget som den IO-ansvarlige, som er placeret i Drift El. Til begrundelse for QMS-koordinatorens uafhængighed kan følgende oplistes:

- QMS-koordinatoren er placeret i Drift El med reference til den Tekniske chef for elnet-aktiviteter.
- Han har som QMS-koordinator stort indblik i og kan få adgang til diverse oplysninger i de forskellige forretningsområder – samtidig med, at han som QMS-koordinator er neutral i forhold til de forskellige forretningsområder.
- SEF er certificeret efter standarden ISO 9001, hvor SEF bliver eksternt auditeret en gang om året.
- Det er indføjet i QMS-koordinatorens Job- og Funktionsbeskrivelse under særligt ansvar, at han uden ophold og indblanding fra direktøren kan orientere Energitilsynet i tilfælde af observationer, der strider imod Bekendtgørelsen om Intern Overvågning.

IO-koordinatoren er i øvrigt ansvarlig for følgende:

- Igangsætning og udarbejdelse af afdelingernes IO-program.
- Information til afdelingerne og deres medarbejdere.

- Opstilling af kontrolsystem for sikring af, at IO-program kendes og overholdes af de relevante ledere og medarbejdere samt at rapportering finder sted til IO-koordinator.
- Gennemførelse af audit (gennemførelse af opfriskningskursus for de involverede medarbejdere efter foretagen revision af det interne overvågningsprogram).

Ansvaret for udarbejdelse og vedligeholdelse af denne procedure påhviler således den IO-ansvarlige koordinator.

4 Fremgangsmåde

4.1 Kontrol

De punkter, der skal fokuseres på i de enkelte afdelinger i forhold til Sydfyns Elforsyning Net A/S er følgende:

1. Adgang til og drift af distributionsnettet skal ske på ikke-diskriminerende vis.
2. Netselskabet må ikke i sin kundekontakt favoriserer bestemte selskaber.
3. Krav til habilitet i ledelsen skal overholdes.
4. Netselskabet skal indgå alle aftaler på markedsmæssige vilkår.
5. Krav om regnskabsmæssig adskillelse skal overholdes.
6. Krav om selskabsmæssig udskillelse af aktiviteter, der ligger uden for netbevillingen.
7. Kommunikation med elhandlere om konkrete aftagenumre skal ske via datahubben.
8. forretningsmæssige følsomme oplysninger skal behandles fortroligt og hvis oplysninger kan videregives, skal det ske ikke-diskriminerende.
9. Oplysninger om netselskabets egne aktiviteter, som kan være forretningsmæssige fordelagtige, må ikke videregives på diskriminerende måde.
10. Netselskabet skal sikre klarhed om sin særskilte identitet.
11. Netselskabet skal have faktisk og retlig råderet over egen hjemmeside.

Hver afdeling er forpligtet til at registrere henvendelser, der giver anledning til tvivl om rækkevidden af forholdsregler og instruks for den pågældende afdeling samt klager vedr. misbrug af følsomme oplysninger eller diskriminerende adfærd m.m. i forhold til ovenstående punkter.
Den enkelte chef indberetter hvert kvartal registreringerne til den IO-ansvarlige.
Den IO-ansvarlige vurderer indberetningerne og tager skridt til evt. ændringer i de interne procedurer og instruktioner.
Den IO-ansvarlige sikrer, at afdelingslederne løbende implementerer ændringer i procedurer og instruktioner.

4.2 Audit

Der foretages i alle afdelinger årlig kontrol af, om internt overvågningsprogram er effektivt implementeret i organisationen. Kontrollen dokumenteres ved underskrift af QMS-formular 11-Bekræftelse af intern audit i Intern Overvågning.docx .
Kontrollen foretages ved intern audit i afdelingerne sammen med audit iht. ISO 9001.

Intern audit er fordelt over kalenderåret, men hver afdeling auditeres mindst en gang årligt som beskrevet i Intern audit.

16 – IT adgangsstyring for interne og eksterne medarbejdere.

1. Formål

Formålet er at beskrive retningslinjer for styring af adgangen til af SEFs IT informationsaktiver med udgangspunkt i de forretnings- og sikkerhedsmæssige krav.

2. Roller og ansvar

Alle medarbejdere der foretager IT adgangsstyring er ansvarlige for at overholde denne proces. IT-afdelingens afdelingsleder er ansvarlig for denne proces.

Det er System-og/eller Forretningsapplikationsejerens ansvar til enhver tid at sikre, at kun relevante brugere har adgang til SEFs informationsaktiver. Tildeling af adgange dokumenteres og kontrolleres jævnligt, så det sikres, at kun autoriserede brugere har adgang.

3. Input

Input er mail fra den ansvarlige chef / afdelingsleder om IT brugerrettigheder jf. processen "11-HR Første oprettelse af medarbejder i SEF".

4. Fremgangsmåde

4.1 Principper for medarbejderes adgang til SEF's IT-systemer.

- Alle brugere, som skal have fast adgang, oprettes med personlige brugerkonti.
- Alle brugere anvender komplekse passwords, som skiftes regelmæssigt.
- Alle nye brugere oprettes med et førstegangs password, som skal skiftes ved første pålogning.
- Medarbejdere har ved pålogning uden for SEF mulighed for at logge på med Direct Access eller VPN. Ved Direct Access logges på fra egen PC med installeret certifikat. Ved brug af VPN sker pålogning med 2 faktor log-on. Ud over almindelig bruger-id+ password angives et engangspassword genereret via en SMS til mobiltelefon.
- Medarbejdere skal anvende udstyr udleveret af SEF, når de logger på SEFs netværk uden for SEFs lokationer.

4.2 Brugeradgang for eksterne konsulenter.

- Der skal være underskrevet en samarbejdsaftale og tilhørende tavshedserklæring med den pågældendes arbejdsgiver, inden der gives IT-adgang.
- Der gives tidsbegrænset adgang på enten 5 dage eller 1 års gyldighed.
- Det er System- og/eller Forretningsapplikations-ejeren, der bestiller IT brugeradgangen.

- Alle eksterne brugere logger på via en sikker VPN forbindelse undtagen når SEF stiller en PC til rådighed på SEFs lokation.

4.3 Kontrol af IT brugeradgange.

- En gang årligt gennemgås Brugerarkivet med henblik på at verificere, at der findes godkendte brugerbestillinger for alle brugere i brugerdatabasen, samt vurdering af, om brugerne er aktive. Endvidere laves stikprøvekontrol på ca. 10 % af brugerne (interne såvel som eksterne), hvor det for kritiske systemer verificeres, at brugeren har adgange svarende til det, der er givet tilladelse til.

4.4 Anvendelse af administratorkonti.

- Anvendelse af Administratorkonti på servere og andet hardware skal begrænses mest muligt ved at tildele Driftspersonalet særlige administratorrettigheder til deres personlige adgang.

5. Output

Betryggende og sikker gennemførelse af IT adgangsstyring for interne og eksterne medarbejdere.

IT Adfærdskodeks og telefonpolitik

1 Formål

Formålet med denne retningslinie er dels at fastlægge retningslinier for medarbejderes anvendelse af SEFs informationsaktiver og dels at beskrive den IT-overvågning der finder sted hos SEF.
Formålet er endvidere at beskytte medarbejdere i tilfælde af sikkerhedsbrud, idet der her gælder fælles "spilleregler" samt at sikre, at lovgivningen på området overholdes.

2 Gyldighedsområde

Denne retningslinie er gældende for alle SEFs medarbejdere og for eksterne konsulenter, der gives adgang til SEFs netværk.

3 Ansvar og myndighed

Ansvaret for udarbejdelsen og vedligeholdelsen af denne retningslinie er pålagt direktionen.
Ansvaret for overholdelsen er pålagt alle SEFs medarbejdere og eksterne konsulenter, der gives adgang til SEFs netværk.

4 Fremgangsmåde

4.1 Overvågning af IT-brug

Af informationssikkerhedsmæssige grunde foretages registrering af enhver form for aktivitet på SEFs netværk.
Registreringen (logning) tillader, hvis det er nødvendigt, at spore enhver aktivitet til enhver specifik computer i netværket. Detaljeringsniveauet tillader for eksempel at aflæse, hvilke web-sider der besøges fra en given computer. Endvidere sker logning af alle e-mailaktiviteter.
Logningerne gemmes i mindst seks måneder.
Logningerne læses ikke systematisk, men der er lagt en række filtre ind i systemet, som vil gøre systemadministratoren opmærksom på, om der foregår specifikke typer af aktiviteter, som vurderes at indebære en informationssikkerhedsmæssig risiko. Logningerne anvendes alene i forbindelse med fejlsøgning, udredning af driftsforstyrrelser og til informationssikkerhedsmæssige formål. Dog overvåges e-mail logningerne som led i den daglige drift (tidligt varsel om driftsproblemer).
Logningerne er kun tilgængelige for Systemadministratorer, der er underlagt tavshedspligt med hensyn til alle typer af logning.

4.2 Styring via IT systemer

Følgende adgangsforhold, tilladelser, administration mv. styres automatisk via IT systemerne:

- Anvendelse af komplekse passwords
- Tvunget password-skift

- Styring af administratorrettigheder på egen computer og på servere
- Antivirus og antispyware
- Medarbejdercomputere låses med pauseskærm efter ubenyttet i max. 15 minutter
- Styring af brugerrettigheder for digitale data

4.3 Adfærdskodeks – hvad skal medarbejderen selv gøre

Nedenfor er listet en række retningslinier for anvendelse af SEFs informationsaktiver. Retningslinierne skal følges og eventuelt brud på disse, vil blive behandlet efter pkt. 4.6 – Sanktionering.

Adgang/password

1. Enhver forespørgsel udefra om SEFs netværk, om styresystemer, procedurer vedr. passwords henvises til IT-afdelingen.
2. Du skal holde dit password privat.
3. Du må ikke udlevere til eller opbevare password tilgængeligt for tredjemand.
4. Din computer skal låses med password når lokalet forlades, så den ikke kan anvendes af andre.

Elektronisk kommunikation

Ved kommunikation via e-mail eller sociale medier er det vigtigt at huske, at indhold og form af kommunikationen har juridisk forpligtende karakter for SEF, og at kommunikationen kan læses af andre end modtagere.

5. Brug kun e-mail og sociale medier til korte beskeder.
6. Hvis du modtager en underlig og uvedkommende e-mail, så undlad at svare og undlad at klikke på vedhæftede dokumenter, filer eller links. Er du i tvivl, så slet mailen uden at åbne den.
7. Husk at gøre en mødeindkaldelse i Outlook privat, hvis den indeholder fortrolig information.(Tekst eller vedhæftet fil)
8. Ved fremsendelse af elektroniske dokumenter som vedhæftede filer er det vigtigt at huske, at dokumenterne vil kunne læses af andre end modtageren. Fremsendelse af fortroligt materiale skal som et minimum ske i form af et passwordbeskyttet dokument, men egentlig kryptering er at foretrække.
   F.eks. må user-ID og password aldrig følges ad i samme kommunikationsmedie.
9. Modtagne og afsendte E-mails som har forretningsmæssig betydning for Sydfyns Elforsyning må ikke slettes, før der er foretaget nødvendig arkivering, jf. processen 11- Ind- og udgående korrespondance.

Brug af Internet

10. Det er ikke tilladt at surfe på hjemmesider med ulovligt indhold, sider med pornografisk, politisk ekstremistisk eller diskriminerende indhold eller andet indhold, der kan skade SEFs omdømme, og som strider mod almindelige etiske standarder.
11. Det er tilladt at benytte homebanking, e-boks, offentlige websteder og lignende.

12. Det er kun tilladt at downloade arbejdsrelateret materiale.
13. Det er ikke tilladt at downloade spil, film, musik mm.

Brug af arbejdsstation, mobiltelefon og mobilt udstyr

14. Det er dit ansvar, at virksomhedens data forvaltes på forsvarlig vis. Alle filer skal opbevares på netværket, hvor der automatisk tages backup, og ikke på lokal harddisk.
15. Installation af nye programmer foregår altid via IT-afdelingen, og det er ikke tilladt at installere downloadede programmer.
16. USB tilslutning af eksternt udstyr er kun tilladt efter aftale med IT-afdelingen.
17. Du må ikke give uvedkommende adgang til SEFs udstyr. Dette gælder alle steder, også på hjemmearbejdspladser.
18. Ved tab, tyveri eller anden bortkomst af SEFs udstyr (fx mobiltelefon, bærbar computer, PDA) eller fortroligt materiale, skal det straks anmeldes til den IT sikkerhedsansvarlige.
19. Informationsbehandlingsudstyr som f.eks. fysiske servere, stationære PC'er o.l. må ikke fjernes fra SEFs lokationer uden tilladelse fra systemejeren.

Andet

Alt materiale vedr. SEF og SEFs kunder, leverandører, medarbejdere systemer, Netværk data m.v. er som udgangspunkt fortroligt. Materiale som indeholder personhenførbare data (f.eks. kunders forbrugstal, private oplysninger om medarbejdere) er følsomt. Oplysninger om kunders og medarbejderes mail, internetforbrug og opkaldslister er særlig følsomme.

20. Der henstilles til, at samtale om forretningsfortrolige oplysninger vedrørende SEF i det offentlige rum (f.eks. samtale i mobiltelefon, i bus, tog, restaurant og lignende) sker med omtanke.
21. Forretningsfortroligt og følsomt materiale må ikke ligge frit tilgængeligt for uvedkommende hos SEF (f.eks. flyde på skriveborde).
22. Fortroligt materiale skal makuleres iht. reglerne beskrevet i "Bortskaffelse af affald".
23. Følsomt materiale uanset medie skal beskyttes yderligere, idet der ikke må udveksles følsomme oplysninger om kunder, medarbejdere m.v., hverken internt eller eksternt til andre, som ikke har de samme rettigheder, eller for eksterne uden at der er underskrevet en særlig tavshedserklæring.
24. Følsomt materiale uanset medie må ikke kopieres uden tilladelse fra dataejeren.
25. Særligt følsomt materiale uanset medie må kun håndteres af internt "clearede" personer i IT Drift og SI Drift.

4.4 Telefonpolitik

1. Generelt

Vores telefonsystem supporteres af en ekstern leverandør. Kontakt til denne leverandør varetages af vores superbruger (person i IT-afdelingen). Information om rigtig brug af systemtelefoner, mobiltelefoner m.m. samt evt. behov for nye / ændring af telefonsvarer i forbindelse med ændrede åbningstider, skal ligeledes rettes til IT-afdelingen.

Det tilstræbes at der under normale omstændigheder er en maksimal ventetid på 30 sekunder før telefonen svares eller viderestilles til telefonsvarer eller omstilling.

2. Forholdsregler for intern telefonbetjening

Brug telefonen med omtanke.
- Har du behov for at bruge mobiltelefon i udlandet, vælges den billigste udbyder, som oplyses via sms til din mobiltelefon første gang du tænder mobiltelefonen i udlandet.
- Sørg altid for at din fastnettelefon er kodet korrekt; møde, ferie eller pause m.m. Hvis du har en mobiltelefon stillet til rådighed, bør du så vidt muligt sørge for at viderestille din fastnettelefon til mobilen, når du ikke er til stede.
- Indtal korrekt telefonbesked
    - Indtal tydelig navn, firma og evt. stillingsbetegnelse på din mobilsvarer så der ikke opstår tvivl hos dine kunder/ kolleger om nummeret de har ringet til.
- Hold din kalender opdateret
    - Sørg for at din kalender altid er opdateret og med korrekt og forståelig information, så dine kolleger / omstillingen har mulighed for at give dine kunder / samarbejdspartnere den bedst mulige service.

3. Telefonåbningstider, telefonvelkomst for hovednummer, helligdage m.m.
Telefonomstillingen er personligt bemandet i SEF´s åbningstid:

mandag, tirsdag , onsdag kl. 08.30 – 15.30
torsdag kl. 08.30 – 18.00
fredag kl. 08.30 – 12.00

Ved opkald til hovednummeret oplyses automatisk, at man har ringet til Sydfyns Elforsyning. Der oplyses om mulighed for omstilling til support eller at vente på personlig betjening. Derefter besvares personligt med "omstillingen" og der spørges ind til kundens behov for hjælp og omstilles til den medarbejder, der forventes at kunne besvare forespørgslen. Hvis der ikke kan omstilles til den ønskede person lægges på opfordring besked for opringning til kunden.

Telefonopkald udenfor åbningstid

Udenfor den nævnte åbningstid går telefonopkald til hovednummeret til en automatisk telefonsvarer. Se i øvrigt Vagtordninger EL og Support SI.

Såfremt der i enkeltstående tilfælde er behov for at ændre på ovennævnte åbningstider, er det meget vigtigt at IT-afdelingen bliver orienteret mindst 7 dage før, ændringen træder i kraft. Der skal i så fald tages kontakt til vores leverandør, som har mulighed for at ændre tidspunktet for omstilling til vagttelefon m.m.

4.5 Gæster, kunder, leverandører og eksterne konsulenter

Det er SEFs medarbejderes ansvar, at gæster, kunder, leverandører og eksterne konsulenter føler sig velkommen, men kun har relevant adgang ved at:

1. Der findes en kontaktperson hos SEF.

2. De kun færdes på relevante lokationer/områder.

Gæster

3. Må kun færdes uledsaget i Butik og atrium
4. Må kun anvende SEF's trådløse gæstenetværk. Adgangskode til gæstenetværket kan ses på SEF Info

Kunder

5. Må kun færdes uledsaget i Butik og Atrium

Leverandører og eksterne konsulenter

7. Må kun færdes uledsaget i arbejds-/kontor-områder, lagerrum og teknikrum, hvis der er givet særlig tilladelse.
8. Arbejde udført af eksterne konsulenter i sikre områder er så vidt muligt overvåget af en SEF medarbejder.
9. Må kun få adgang til relevante systemer og udstyr i SEF's netværk og kun i en tidsbegrænset periode.
10. Kan som udgangspunkt kun få adgang til SEFs netværk og systemer via autoriseret VPN-forbindelse. Direkte adgang uden VPN kan kun gives i særlige tilfælde.
11. Alle leverandører og eksterne konsulenter som har behov for adgang til SEF's netværk skal underskrive en tavshedserklæring, før arbejde for SEF påbegyndes.
12. Det er ikke tilladt at medbringe forretningsfortroligt materiale udenfor SEF.
13. Mobilt udstyr, som ikke er SEFs ejendom, må kun tilsluttes SEFs gæstenetværk og efter aftale med IT afdelingen.

4.6 Sanktionering

Tilsidesættelse af gældende Informationssikkerhedspolitik betragtes som en grov misligholdelse af ansættelsesforholdet. Ikke-tilfældig, gentagen overtrædelse af gældende regler for informationssikkerhed hos SEF kan derfor, afhængig af overtrædelsens karakter, medføre afskedigelse eller bortvisning.
Informationssikkerhedshændelsen behandles iht. procedure Styring af informationssikkerhedshændelser og rapporteres til ledelsen, som tager stilling til yderligere handling.
Ved mistanke om ikke-tilfældig, gentagen overtrædelse af gældende regler for informationssikkerhed hos SEF, foretages gennemgang af den enkelte medarbejders aktiviteter og lagrede data på IT-systemerne. Gennemgang af loggen foretages af en systemadministrator sammen med en repræsentant fra ledelsen.

Risikovurdering og -håndtering.

1 Formål

Formålet med denne retningslinje er at fastlægge ansvar for gennemførelse af risikovurdering og – analyse af SEFs informationsaktiver. Resultatet af risikoanalysen bruges til at fastsætte informationssikkerhedsniveauet for SEF.

2 Gyldighedsområde

Denne retningslinje er gældende for alle SEFs medarbejdere samt eksterne samarbejdspartnere, der gives adgang til SEFs informationsaktiver.

3 Ansvar og myndighed

Ansvaret for udarbejdelsen og vedligeholdelsen af denne retningslinie er pålagt Informationssikkerhedsorganisationen.
Ansvaret for overholdelsen af denne retningsline er pålagt alle SEF's medarbejdere.

4 Fremgangsmåde

4.1 Sårbarheds- og trusselsvurdering

Informationssikkerhedsorganisationen mødes en gang i kvartalet og vurderer her, om der er ændringer i trusselsbilledet eller der er sårbarheder, der ikke er håndteret i risikovurderingen af informationsaktiver. I dette forum opsamles således alle potentielle sårbarheder og trusler, der måtte opstå imellem den egentlige risikovurdering af informationsaktiver. Det påhviler hvert medlem af informationssikkerheds-organisationen at melde ind til de øvrige ved mistanke om potentielle trusler eller sårbarheder. Der udarbejdes referat fra møderne og der igangsættes straks tiltag til forebyggelse af evt. trusler og sårbarheder.

4.2 Risikovurdering af informationsaktiver

Der gennemføres en risikovurdering af SEF's kritiske informationsaktiver to gange om året. Risikovurderingen skal identificere og prioritere risici med udgangspunkt i SEF's forretningsmæssige forhold. Resultatet skal bidrage til fastlæggelse og prioritering af de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.
Det er applikationsejernes ansvar, at der gennemføres risikovurderinger regelmæssigt og ved væsentlige ændringer i risikobilledet, herunder organisatoriske og teknologiske ændringer.
Risikovurderingen gennemføres metodisk og systematisk, så resultaterne er sammenlignelige.
Analysen af de identificerede risici vil resultere i et trusselsbillede hvor konsekvenser og sandsynlighed for skadevoldende hændelser vurderes i forhold til aktuelle sikringsforanstaltninger.

Risikovurderingen skal resultere i konkrete beslutninger og handlinger vedrørende:

- Behov for forbedringer i SEFs informationssikkerhedsstyring
- Ændringer i Chefgruppens overordnede informationssikkerhedskrav
- Ændringer i ressourceallokering og/eller ansvarsplaceringer

Resultatet af risikovurderingen danner grundlag for formulering af SEFs Informationssikkerhedspolitik.
Risikovurderingen følges løbende op på kvartårlige møder i informationssikkerhedsorganisationen.

4.2 Risikohåndtering

Såfremt en risikovurdering afdækker et relevant informationssikkerhedsbehov, skal de nødvendige sikringsforanstaltninger og styringsmål udvælges og implementeres for at reducere risikoen til et acceptabelt niveau under hensyntagen til:

- SEFs forretningsmæssige forhold
- Nationale og internationale love og forordninger
- Operationelle krav og begrænsninger
- Omkostningerne ved implementering og drift af sikringsforanstaltningerne i forhold til den reducerede risiko
- En afvejning af de forretningsmæssige konsekvenser af et informationssikkerhedsbrud i forhold til de samlede omkostninger ved sikringsforanstaltningen.

Resultatet af risikovurderingen for et bestemt informationssikkerhedsbehov eller ændrede risici kan danne grundlag for igangsættelse af en forebyggende handling.