Politik for Coop Danmarks informations- og it-sikkerhed

Ansvarlig	Information Security
Udarbejdet af	Henriette Rolskov
Kontaktinformation:	information.security@coop.dk
Omfattede virksomheder:	• Coop Danmark A/S og datterselskaber, hvor Coop Danmark har bestemmende indflydelse
Berørte afdelinger	Alle afdelinger under ovennævnte virksomheder.
Regler	Reference til Coops koncern informations- og it-sikkerheds politik Relevant lovgivning • Persondataforordning • Regnskabsloven • Network and Information Security (NIS2) Directive
Reference ISO	• ISO 27001, ISO27002 og ISO27005

1. Formål og baggrund

Denne politik sætter rammen for det ansvar og de opgaver ledelsen i forretningen pålægges for implementering af informationssikkerhed, herunder it-sikkerhed i Coop. Hvis et forretningsområde varetager et af de fremhævede stabsområder, påhviler der ledelsen herfor et særligt ansvar.

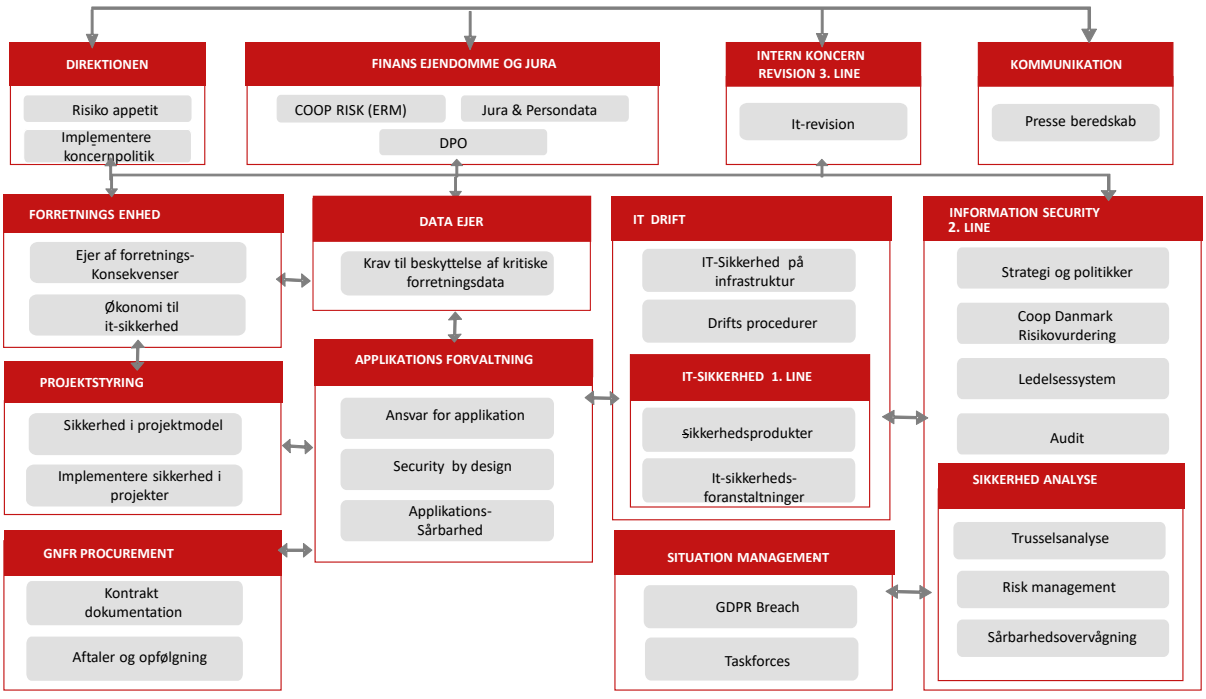
Politikken implementerer Coops Koncern informations- og it-sikkerhedspolitik, som delegerer ansvaret for informations- og it-sikkerhed til de enkelte koncernselskabers direktioner.

Med afsæt i denne rammesættende mandatpolitik vedtager Coop Danmark politikker, der tillige gælder i datterselskaber, hvor Coop Danmark har bestemmende indflydelse.

Politikken beskriver forankringen af ansvaret og opgaverne på ledelsesniveau. Alle medarbejdere er omfattet politikken, men budskaberne heri kommunikeres med målgruppen for øje. Hvorfor politikken ikke direkte forventes læst af alle medarbejdere, men budskaberne formidlet på passende vis, f.eks. i butik og på lager.

Informationssikkerhedsarbejdet tager udgangspunkt i den almindeligt udbredte og anerkendte ISO-standard, ISO 27001.

Herunder ses oversigt over organisering af det overordnede ansvar og opgaver i Coop Danmark. Pilene viser den primære samarbejdsrelation og er derfor ikke udtømmende, for alle de relationer der er på tværs. Ved termen Forretningsenhed henvises til området, som drives under hvert direktørområde.



2. Fem grundlæggende principper

Direktionen har det overordnede ansvar for it- og informationssikkerheden i Coop Danmark og for at sikre realisering af de 5 principper som givet i Coops koncern informations- og it-sikkerhedspolitik.

Principper

1) Bestyrelserne i de enkelte Coop-selskaber har det overordnede ansvar for overholdelsen af Sikkerhedspolitikken. Direktionerne i de enkelte Coop-selskaber skal sikre, at der afsættes tilstrækkelig økonomi og bemanding til at efterleve indholdet af Sikkerhedspolitikken.

2) Beskyttelse af data skal ske baseret på en fælles model for dataklassifikation.

3) Der skal implementeres sikkerhedsforanstaltninger, der matcher det aktiv, som skal beskyttes.

4) Adgang til Coops informationsaktiver, it-systemer, tekniske anlæg og bygninger gives ud fra et arbejdsbetinget behov.

5) Vurderinger af risici skal ske ud fra et aktuelt trusselsbillede.

3. Coops direktion

Direktionen skal sikre, at Coop Ledelses Team efterlever de 5 principper, og Coop Ledelses Team skal forholde sig til Coop Danmarks overordnede IT-risikobillede samt prioritere indsatser og allokere ressourcer til håndtering af uacceptable risici.

Det daglige ansvar for informationssikkerheden er uddelegeret til Information Security, som er ledet af CISO (Informationssikkerhedschef i Coop Danmark).

Direktør for Supply Chain, Teknologi & OpEx (COO) og CISO afholder månedsmøder og drøfter aktuelle forhold.

4. Datterselskaber

Coop Danmarks direktion skal som en del af virksomhedsledelsen sikre, at datterselskaber, hvor der er bestemmende indflydelse, overholder de 5 grundlæggende principper. Indsatsen skal være proportional med de data datterselskabet behandler samt graden af forretningskritiske aktiviteter.
Direktionen skal udpege en ansvarlig fra Coop Ledelses Team som følger op på overholdelsen af principperne.

5. Forretningsenheder

Forankringen af informationssikkerhed afhænger af adfærden og implementeringen i de enkelte forretningsområder. Derfor er ansvaret for implementeringen i Coop Danmark tværgående forretningsområder en del af ledelsesansvaret.

Ledelsen i de i enkelte direktørområder skal afsætte den nødvendige økonomi og bemanding for at kunne implementere informationssikkerhed. Den forretning som drives i området kan påvirkes, hvis data mister fortrolighed, pålidelighed eller tilgængelighed. Derfor skal ledelsen tage stilling til de konsekvenser, dette kan have. Er konsekvenserne uacceptable, skal forretningsledelsen tage hånd om det.

Når understøttelsen af sikkerheden skal implementeres i systemer og teknik, skal forretningen udpege en ansvarlig, der i dialog med applikationsejer, finder en løsning. Dette gælder uanset om det er en ekstern leverandør eller Coop Teknologi.

6. Finans, Ejendomme og Jura

I Jura ligger Coop Risk som faciliterer Enterprise Risk Management Board (ERM). ERM har til opgave at skabe et samlet overblik over Coop Danmarks 10 største risici og arbejde med den risikoprofil, der gælder på tværs af alle forretningsrisici på tværs af de forskellige risikoområder (fysisk sikkerhed, forsikringssager, finans, lager osv.). Arbejdet sker med henblik på at skabe et sammenhængende beslutningsgrundlag for hvilke initiativer, der ud fra en helhedsvurdering, giver Coop Danmark mest risikoreduktion per krone. Coop Risk arbejder sammen med Information Security om et it-kriseberedskab i forbindelse med cyberangreb. Via ERM er Coop Risk kravstiller til den ledelsesrapportering, som Information Security skal levere.

Coop Risks konkrete opgaver i forbindelse med informations- og it-sikkerhedsarbejdet omfatter:

- At stille krav til den risikobaserede ledelsesinformation om it-sikkerhed, så ERM board kan anvende og bearbejde informationen til egne formål, herunder vurdere om der er forhold, der skal løftes til en af de 10 største risici
- Samarbejde med Information Security om Kriseberedskab, hvor it er involveret
- Deltagelse i fraud-samarbejdet og sikre koordinering imellem fysiske tyverier og anvendelse af it-løsninger i den forbindelse

Persondatajura og DPO'en ligger i Finans, Ejendomme og Jura. Der er et nært samarbejde imellem Information Security, Persondatajura og DPO'en i forhold til snitfladerne mellem persondatajuraen og it-sikkerhed. Persondatakontoret driver Persondatakomitéen, som er ansvarlig for at påse overholdelsen af persondataforordningen. CISO deltager i Persondatakomitéen.

7. Coops Intern Koncern Revision

Intern Koncernrevision er den øverste ledelses uafhængige kontrolinstans.

Intern Koncernrevision kan ikke indgå som en del af kontrolmiljøet, men deltager som observatør i en række fora med det formål at overvåge og bistå i drøftelserne omkring it-sikkerhed. Intern Koncern Revision håndterer undersøgelser, hvor medarbejdere er involveret i besvigelser eller andre uregelmæssigheder.

Intern Koncernrevision er sammen med de eksterne revisorer medkravstiller i forhold til den finansielle revision af it-området.

Bestyrelsen kan igangsætte opgaver/undersøgelser til udførelse af Intern Koncernrevision.

8. Kommunikationsafdelingen

Større brud på informations- og it-sikkerheden kan få betydelige negative konsekvenser for Coop og/eller for Coops kunder, medarbejdere og samarbejdspartnere. Det er afgørende, at Coop i forbindelse med nedbrudssituationer er i stand til at kommunikere kontrolleret og retvisende om bruddet, herunder om årsager, konsekvenser, forebyggende indsatser mv. Professionel kommunikation kan i sig selv medvirke til at afbøde visse negative konsekvenser, fx i forhold til Coops omdømme.

Effektiv krisekommunikation forudsætter, at der er etableret et kommunikationsberedskab, som kan aktiveres, når et sikkerhedsbrud indtræffer. Kommunikationsafdelingen kan derfor understøtte it-sikkerhedsarbejdet proaktivt gennem forberedelse og afprøvning af beredskab, og reaktivt i forbindelse med håndteringen af brud på it-sikkerheden. Kommunikationsafdelingen kan også bruges til mere ”offensive”/positive budskaber i forbindelse med it-sikkerhedsarbejdet, fx om effekten af implementerede kontroller, om awareness tiltag osv.

Kommunikationsafdelingens konkrete opgaver i forbindelse med informations- og it-sikkerhedsarbejdet omfatter:

- At samarbejde med Information Security for kommunikationsberedskab- og strategi, der kan aktiveres i forbindelse med brud på it-sikkerheden
- At fungere som kommunikationsmæssigt knudepunkt i forbindelse med konkrete brud på it-sikkerheden, herunder varetage ansvaret for den interne koordination og godkendelse af kommunikationsaktiviteter, og for dialogen med eksterne interessenter, herunder pressen

9. Information Security

Coop Danmarks Chief Information Security Officer (CISO) driver afdelingen Information Security. Afdelingens overordnede rolle er at sikre etablering af de nødvendige rammer for arbejdet med informationssikkerhed. Dette omfatter et ledelsessystem, der understøtter de opgaver, der drives i det daglige arbejde. Information Security rapporterer til Coop Danmarks øverste ledelse om Coop Danmarks aktuelle informationssikkerhedsmæssige risikoprofil, samt udarbejder oplæg til at imødegå uacceptable generelle samt tværgående risici.

Information Security er Coop koncernens centrale rådgivningsfunktion om informationssikkerhed og it-sikkerhedsforanstaltninger.

Information Security driver Teknologi Risiko Komiteen (TRK), som er ansvarlig for, at det ønskede informationssikkerhedsniveau realiseres, og efterleves på tværs i Coop Danmarks organisation.

Information Security har følgende hovedopgaver:

- Etablere og vedligeholde et ledelsessystem i overensstemmelse med Coops behov og risikoappetit
- Sikring af de overordnede styringsmæssige rammer for informations- og it-sikkerhedsarbejdet i form af politikker, modeller og skabeloner
- Implementering og vedligehold af it-platform, der anvendes til styringen af informationssikkerheden samt til dokumentation af it-sikkerhedsmæssige forhold
- Løbende ledelsesrapportering om det overordnede sikkerhedsmæssige risikobillede
- Rådgive organisationen om informationssikkerhed, samt belyse behovet for it-sikkerhedsforanstaltninger
- Gennemførelsen af audit og opfølgning på it-revisionsanmærkninger samt findings i andre gennemførte audits
- Generelle oplysningskampagner og uddannelsestiltag indenfor it-sikkerhedsområdet tilrettelægges og gennemføres i samarbejde med Coops uddannelsesfunktioner
- Overvåge trusselsbilledet samt kritiske sårbarheder for Coop (fx via trusselsefterretninger, scanninger og penetrationstests)
- I sikkerhedstaskforces udarbejder funktionen cyber security-analyser og påser bevissikring

10. GNFR procurement

Ved indgåelse af kontrakter sikrer GNFR (Goods Not for Resale), at it-sikkerhed inddrages som en del af kontraktgrundlaget. I forhold til databehandleraftaler, der opstår i forbindelse med anskaffelser (køb eller egenudvikling) af nye persondatabehandlende applikationer, sikrer GNFR, at der indgås databehandleraftaler og følger op på disse.

GNFR-procurements konkrete opgaver i forbindelse med informations- og it-sikkerhedsarbejdet omfatter:

- Opdateringer og tilretninger af aftaleskabeloner, som udarbejdes af Jura, Persondatakontoret og Information Security.
- Fastlæggelse og facilitering af løbende opfølgningsmodeller, herunder indhentelse af revisionserklæringer, opfølgning på eksisterende databehandleraftaler, genforhandlinger af kontrakter
- GNFR har ansvaret for indgåelse af aftaler, med involvering fra bl.a. Information Security og andre specialister fra Coop Teknologi
- GNFR er ansvarlige for indgåelse af databehandleraftaler i overensstemmelse med Coops procedure givet af persondatajura

- Registrering af indgåede databehandleraftaler
- Løbende vedligehold af "stamoplysningerne" om den enkelte databehandleraftale

11. Projektstyring

God informations og it-sikkerhed skal tænkes ind i alle Coops digitale løsninger, inden de går i drift. Det er derfor helt afgørende, at de udviklingsforløb, der introducerer nye løsninger, indrettes så behovene for information og it-sikkerhed analyseres systematisk i designfasen, samt at der stilles krav både til styringen af udviklingsforløbene og leverance- og udviklingsmodellen.

Styringen af udviklingsforløbene sker i henhold til projekt- og opgavestyringsmodeller, er ejet af Project Management Office (PMO). PMO'et skal sikre, at der i projektstyringen og udviklingsmodellerne er indbygget ledelseskontroller, der understøtter, at styregrupper/opgaveansvarlige på passende tidspunkter undervejs i udviklingsforløbet kan vurdere, om løsningens it-sikkerhedsmæssige egenskaber og elementer er arkitektonisk sammenhængende med Coops øvrige løsninger. Derudover skal løsningen være designet med security-by-design som testes inden idriftsættelse

PMO'et skal sørge for, i samarbejde med Information Security, at uddanne de projektledere mv., der arbejder professionelt med styring af it-udviklingsforløb, i håndteringen af den it-sikkerhedsmæssige dimension af udviklingsarbejdet.

De konkrete valg af tekniske og organisatoriske kontroller skal bygge på de krav, som Information Security har fastlagt.

PMO skal sikre, at leverance- og udviklingsmodellen beskriver, hvilke konkrete it-sikkerhedsmæssige leverancer, der skal indgå i alle udviklingsforløb, og henvise til relevante retningslinjer for, hvordan disse leverancer i praksis skal produceres.

PMO's konkrete opgaver i forbindelse med informations- og it-sikkerhedsarbejdet omfatter:

- At indarbejde ledelseskontroller i Coops projekt- og opgavestyringsmodeller, som skal understøtte, at der arbejdes systematisk med it-sikkerhed i udviklingsforløbene
- At uddanne ledere, projektledere mv. i de informations- og it-sikkerhedsmæssige aspekter af udviklingsarbejdet

IT Developments konkrete opgaver i forbindelse med informations- og it-sikkerhedsarbejdet omfatter:

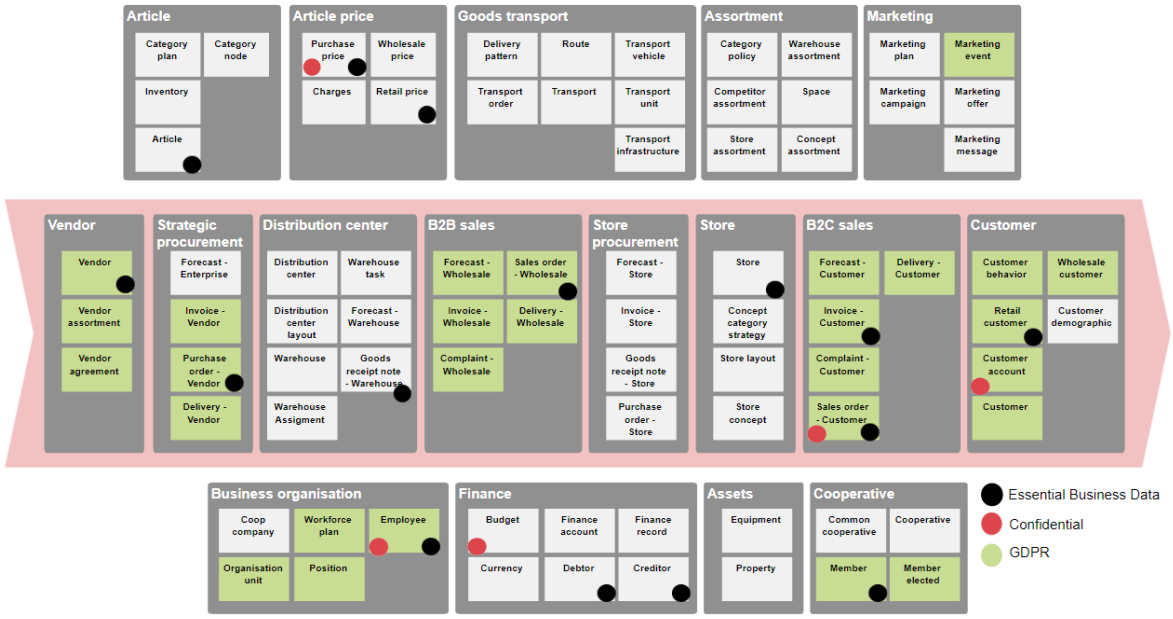
- At dokumentere (i samarbejde med Information Security) de konkrete informations og it-sikkerhedsmæssige leverancer, der skal produceres i udviklingsforløbene, herunder referere til relevante politikker og retningslinjer (udarbejdet af Information Security)
    - Leverancerne der i udviklingen skal tages stilling til omfatter: Risiko- og trusselsvurderinger
    - Dokumentation af konkrete tekniske- og organisatoriske kontroller, der er relevante for projektet
    - Organisatorisk forankring ved overgang til drift.

12. Data ejerskab

Der udpeges en ejer for Coops overordnede dataområder ud fra "Coop Conceptual Information Model", som ses herunder.

Dataejere agerer på tværs af applikationer og forretningsejere og skal kunne stille krav til beskyttelsen af datas integritet, tilgængelighed og fortrolighed.

De 17 overordnede dataområder på figuren omfatter bl.a. de særligt kritiske områder som vareflow, medlemsdata og HR-data. Figuren angiver tillige områder med operationelt essentielle data med en sort prik. Tilsvarende angiver figuren områder, der som udgangspunkt indeholder fortrolige data, med en rød prik (business high og business very high jf. klassifikationsmodellen). Figuren angiver tillige med grønne prikker, de oplagt GDPR-omfattede områder.



13. Forvaltning af applikationer

Forvaltningsorganisationen (Application management) tager sig af den løbende vedligeholdelse af de løsninger, som Teknologi har ansvaret for.

Application Managements væsentligste rolle i forhold til informations og it-sikkerhed er at vedligeholde den centrale informations og it-sikkerhedsmæssige dokumentation, herunder særligt trusselsvurderingerne. I takt med, at der opstår ny viden om trusler og sårbarheder, og når der gennemføres løbende, mindre ændringer af løsningen.

Application Management skal bistå forretningen med at vedligeholde gældende forretningsprocesser, som de forvaltede løsninger understøtter. Kerne forretningsprocesser der gælder alle løsninger er brugerstyring, rettighedsstyring, ændringsstyring og sikkerhedsopdateringer.

Application Management skal sikre, at ændringer til løsningen implementeres sikkerhedsmæssigt forsvarligt, dvs. i henhold til Information Securitys retningslinjer for security-by-design og privacy-by-design.

Application Management i forhold til informations- og it-sikkerhedsarbejdet omfatter i hver af de organisatoriske enheder:

- At gennemføre løbende vurderinger af sårbarheder i forhold til det forretningsmæssige risikobillede
- At stille krav til it-sikkerheden på den platform applikationen understøttes af
- At opdatere trusselsvurderingerne for området, når der sker ændringer af løsningen
- At sikre, at ændringer af løsningen håndteres i henhold til retningslinjerne for security-by-design
- At deltage i håndteringen af evt. sikkerhedshændelser

14. Situation Management

Situation Management udgør den yderste forsvarslinje i forhold til det daglige it-sikkerhedsarbejde. Situation Management har 24/7-vagt og arbejder reaktivt med den løbende overvågning af Coops driftsmiljøer, modtager driftsinformation fra eksterne databehandler, håndterer sikkerhedshændelser (herunder brud på persondatasikkerheden) i 1. line, og eskalerer øvrige hændelser i henhold til Coops eskalationsmodel.

Situation Managements konkrete opgaver i forbindelse med informations- og it-sikkerhedsarbejdet omfatter:

- At reagere på it-sikkerhedsrelaterede alarmer og hændelser fra overvågningen eller personhenvendelser
- At håndtere kendte it-sikkerhedsmæssige hændelser i henhold til standardinstrukser herfor
- At eskalere it-sikkerhedshændelser i henhold til Teknologis procedurer for incidents og taskforces samt håndtering af sikkerhedshændelser
- At registrere problems der afdækkes i forbindelse med taskforce eller sikkerhedshændelser

15. IT Drift

Alle it-sikkerhedsprocedurer og instrukser formuleres og vedligeholdes af de produktansvarlige for den specifikke it-service. Produktansvarlige holder øje med opdateringer på egne produkter. Forhold af principiel eller strategisk karakter løftes efter behov til Information Security.

IT Operations vedligeholder it-beredskabet og sikrer operationel overvågning af kritiske systemer.

IT-Sikkerhedsdrift

I IT-driften ligger it-sikkerhedsfunktionen, Security Operations Center (SOC), som arbejder både proaktivt og reaktivt. Her varetages den daglige it-sikkerhedsmæssige overvågning af Coops it-driftsmiljøer, som ligger i den enkelte driftsorganisation.

IT Operations har ansvaret for at vurdere den it-sikkerhedsmæssige information, der løbende indsamles fra diverse logs og sikkerhedssystemer (fx Firewalls, IDS'er, IPS'er og antivirus systemer). Operational Security skal sikre at kendte trusler håndteres hurtigt og som en del af den daglige drift. Operational Security er udførende for mitigering af de it-sikkerhedshændelser, der kommer ind via Situation Management.

Operational Securitys konkrete opgaver i forbindelse med it-sikkerhedsarbejdet omfatter:

- At varetage den løbende daglige it-sikkerhedsmæssige overvågning af Coops driftsmiljøer
- At varetage sagsbehandlingen i forbindelse med it-sikkerhedshændelser
- At etablere og vedligeholde den it-platform, der gør det muligt at indsamle, konsolidere og analysere data fra mange forskellige it-sikkerhedssystemer
- At levere information til Information Security (Security Analytics Center - SAC) om mere strukturelle problemstillinger i forhold løsningernes it-sikkerhedsmæssige robusthed
- At fungere som fagspecialister og første instans der rådføres med ved it-sikkerhedshændelser
- At vedligeholde procedurer for operationel sikkerhed (ex. firewall, netværk, applikationssikkerhed)
- At levere rapportering om it-sikkerhedshændelser til Information Security

16. Opfølgning

Behovet for ændringer i sikkerhedspolitikken vurderes årligt af Information Security. Forelæggelse for Direktionen sker, hvis der er forslag til indholdsmæssige ændringer.

Opdatering af årstal ved revurdering sker uden forelæggelse.