COOPS IT-SIKKERHEDSPOLITIK

1. MÅLSÆTNING OG IT-SIKKERHEDSNIVEAU

It-sikkerhedspolitikken skal til enhver tid understøtte Coops værdigrundlag, vision og strategiske mål.

It-sikkerhedspolitikken og de understøttende regler skal fastlægge de grundlæggende rammer vi arbejder ud fra for at søge at undgå it-sikkerhedsbrud og for at kunne håndtere de hændelser, der sker på trods af vores indsats.

It-sikkerhedspolitikken gælder for alle afdelinger og ansatte i Coop AMBA, Herunder Coop Danmark, Coop Trading og Brugsforeningerne for Danmark, Færøerne og Grønland. It-sikkerhedspolitikken gælder ikke for Coop Bank, idet banken er underlagt en anden regulering end resten af Coop koncernen.

It-sikkerhedspolitikken gælder for alle der er tilknyttet Coop på en måde, hvor der gives adgang til it-ressourcer og der hermed kan ageres på Coops regning og risiko.

Ledere i Coop har et ansvar for at gældende it-sikkerhedsregler efterleves. Det betyder, at den enkelte leder er ansvarlig for at såvel egne medarbejdere, som eksterne konsulenter og vikarer kender Coops it-sikkerhedspolitik, og har en grundlæggende forståelse for hvordan og hvorfor den skal overholdes. Coops ledelse skal understøtte Coops it-sikkerhed ved at udstikke klare retningslinjer og udvise synligt engagement.

I it-sikkerhedspolitikken fastlægges det overordnede it-sikkerhedsniveau for Coops forretning.

It-sikkerhedsniveauet afspejler Coops ledelsesforankrede risikovillighed, som fastlægges ved gennemførelse af en it-risikovurdering i forhold til de risici, der er vurderet ved brud på:

- Fortrolighed
- Pålidelighed
- Tilgængelighed

Resultatet af it-risikovurderingen forelægges til Coop Danmarks direktionens godkendelse. For risici, der retter sig imod brud på EU's persondataforordning, henvises til "Persondatapolitikken for hele Coop koncernen".

Hvor et projekt eller en udviklingsopgave omfatter behandling af personoplysninger, skal Coop Teknologis projektstyringsmodels regler for compliance anvendes.

Når der drøftes mulige konsekvenser af risici sker dette ved en afdækning af, om brud på sikkerheden kan påvirke forretningen herunder i forhold til:

- Strategier, hvor Coop bliver ude af stand til at gennemføre vigtige aktiviteter
- Økonomi, hvor der er væsentlige økonomiske tab, tabt indtjening eller store bøder
- Organisatoriske udfordringer, hvor ressourcer må udvides urealistisk
- Omdømme, som lider alvorlig skade
- Lovgivning eks. brud på persondata regler, brud på straffeloven

Ambitionsniveau på it-sikkerhedsområdet

Coop er en af Danmarks største virksomheder. Derfor skal vi leve op til de forventninger omverdenen og vores medlemmer har til os, som en stor spiller i det danske samfund.

Coop er en købmandsvirksomhed og det er afgørende for Coop, at varen kommer fra "jord til bord". Oversat til it-sikkerhed betyder det, at pålidelighed og tilgængelighed i varesystemerne og betalingssystemerne har afgørende betydning. Hvis vores systemer ikke kan tale sammen eller der er fejl i data, så kan kunden ikke købe varen og de rette varer kan ikke komme frem til kunden.

Vores medlemmer er i centrum og vi skal bevare deres tillid. Det betyder, at medlemsdata skal behandles fortroligt og ifølge persondatalovgivningen. Vores omdømme hos vores medlemmer er et af de største aktiver, vi har i Coop.

Coop vil bruge teknologien til at give kunderne en god indkøbsoplevelse og til at etablere gode processer for forretningen. Derfor skal vores systemer være fremtidssikrede, og gøre hverdagen lettere. Det betyder, at vi skal sikre en god arkitektur, struktur og kvalitet på systemerne og data, og it-sikkerheden og privacy by design indbygges som en del af de innovative løsninger.

Coop er en stor virksomhed med mange ansatte, derfor skal vi sikre en betryggende styring af brugerroller og de rettigheder vi giver til vores it-ressourcer. Vi skal ligeledes sikre en god styring af udviklingsprocesserne uanset om det sker via interne kræfter eller om opgaverne outsources.

Endelig skal vi på det teknologiske område være en professionel og fremsynet virksomhed, der kan tiltrække de bedste tekniske medarbejdere, så vi sammen kan indfri Coops digitale potentiale.

2. METODE OG KRAV

Som baggrund for it-sikkerhedsarbejdet tager Coop udgangspunkt i ISO 27001 og 27002. Hvor det er relevant i forhold til modtagelse af betalingskortoplysninger i butikkerne arbejdes i overensstemmelse med Payment Card Industri Data Security Standard (PCI DSS).

Derudover er der love og regler på nogle områder der stiller særlige krav. Det drejer sig om:

- Behandling af personoplysninger, herunder medarbejderoplysninger, kundeoplysninger og medlemsoplysninger
- Håndtering af bonus og dividende, som skal behandles som et vederlagsfrit betalingssurrogat

Coops applikationer og data betragtes som en kritisk ressource for Coop. Der lægges derfor vægt på driftsikkerhed, kvalitet og veldokumenterede arbejdsprocesser. Coops samlede it-sikkerhedskoncept omfatter følgende:

- Coop it-sikkerhedspolitik, som fastlægger de overordnede ledelsesmæssige rammer. Denne godkendes på bestyrelsesniveau.
- Coops politik for behandling af personoplysninger
- It-risikovurderingen, som godkendes i Coop Danmark på direktionsniveau, og afrapporteres til bestyrelsen.
- It-beredskabet
- Øvrige interne regler og procedurer udstedt af Information Security

Alle it-sikkerhedsprocedurer og instrukser formuleres og vedligeholdes af de ansvarlige for den specifikke it-service. Forhold af principiel eller strategisk karakter løftes til Coop Technology Information Security.

3. IT SIKKERHEDSORGANISATIONEN OG ANSVAR

Coops bestyrelse har det overordnede ansvar for it-sikkerheden og har uddelegeret det daglige ansvar for it-sikkerheden til Coop Technology Information Security, der refererer til Coop Danmarks direktion. Mandatet til Information security går på at agere på koncernniveau.

Information Security driver Teknologi Risiko Komiteen (TRK), som er ansvarlig for, at det ønskede it-sikkerhedsniveau realiseres, og efterleves på tværs i organisationen. TRK er et specialudvalg i forhold til ERM board (Enterprise Risk Management), der har det brede perspektiv på tværs af alle typer risici. Teknologi Risiko Komitéen mødes en gang om måneden.

3.1 Medarbejdere

Det skal sikres, at den enkelte medarbejder modtager folderen "sikkerhedsselen" som giver en overordnet introduktion til de forventninger, der stilles i forhold til it-sikkerhed.

3.2 Samarbejdspartnere

Når Coop anvender eksterne konsulenter og samarbejdspartnere skal det sikres, at internt Coop ansatte varetager de ledelsesmæssige roller og står i spidsen for alle forretningsmæssige beslutninger.

De af Coops eksterne samarbejdspartnere, der vurderes at have behov for adgang til systemer på Coops netværk, kan få denne tildelt. Samarbejdspartneren må dog kun tildeles adgang til de systemer, hvor der er et arbejdsbetinget behov for adgang.

Inden adgang til Coops netværk gives, skal den eksterne konsulent underskrive fortrolighedsklausul (Coops Non Disclosure Agreement -NDA).

Hvis adgangen til systemerne sker under overvågning af en Coop ansat, er det tilstrækkeligt at samarbejdspartneren på vegne af den ansatte har underskrevet en aftale (NDA), hvor samarbejdspartneren sikrer at ovenstående forpligtelser overholdes.

4. IT-BEREDSKAB

Katastrofer forsøges undgået gennem en veltilrettelagt fysisk sikring og overvågning af bygninger, tekniske installationer og it-udstyr. Omfanget af disse foranstaltninger besluttes ud fra en afvejning af risici imod sikringsomkostninger og udmøntes i SLA´er.

Coops Teknologis beredskab skal omfatte:

- Hvordan beredskab håndteres og sammenhængen med eksisterende Task force håndtering via ServiceDesk.
- Genetablering af midlertidige /permanente løsninger.
- Beredskabsplanerne skal opdateres og testes løbende.

5. ADGANGE TIL SYSTEMER OG APPLIKATIONER

Der skal for driftssystemer findes konkrete retningslinjer og procedurer for administration af brugere og adgange.

- Coop beskytter data og it-systemer ud fra princippet "Need to Protect". Det vil sige, at en bruger, som har tilladelse til at tilgå et system som udgangspunkt får adgang til hele systemet. Hvis der skal ske yderligere begrænsning af brugernes adgang skal der være en forretningsmæssig begrundelse.
- Coop Teknologi skal være i kontrol med brugerstyringen på alle koncernens it-systemer. Dette betyder, at der skal være en autorisationsmodel, som sikrer at decentrale, og dermed uautoriserede, ændringer overskrives.
- Coop skal have en central og automatisk proces for brugeradministration.
- Coop skal holde adgange til Coops egne systemer og Coop bank A/S systemer skarpt adskilt.

- Personer, der gives adgang til et it-system, holdes ansvarlig for brug og misbrug af adgangen.
- Der skal være processer for manuel tildeling af ekstra adgange i de tilfælde, hvor de normale kriterier for tildeling af adgange viser sig ikke at være tilstrækkelige skal Coop følge de principper, der er beskrevet nedenfor.

6. ÆNDRINGSSTYRING

Coops procedurer for forandringer (Change Management) skal følges ved enhver ændring i applikationer, it-services og infrastruktur og tildeling af adgange hertil.

7. FYSISKE LOKATIONER

Der skal ved ibrugtagning af bygninger være udarbejdet og implementeret konkrete regler og procedurer for regulering af adgangsforholdene.

Hvis en aktivitet er omfattet af en outsourcingaftale, skal det i aftalegrundlaget med leverandøren tilsikres, at Coops NDA aftale og it-sikkerhedspolitik overholdes, f.eks. ved at pålægge leverandøren at foretage forskellige kontroller og rapportere effektiviteten af disse, eksempelvis i en passende revisionserklæring.

8. OPFØLGNING

It-sikkerhedspolitikken revideres hvert 3. år og ved større ændringer, og godkendes på Coop Amba bestyrelsesniveau.