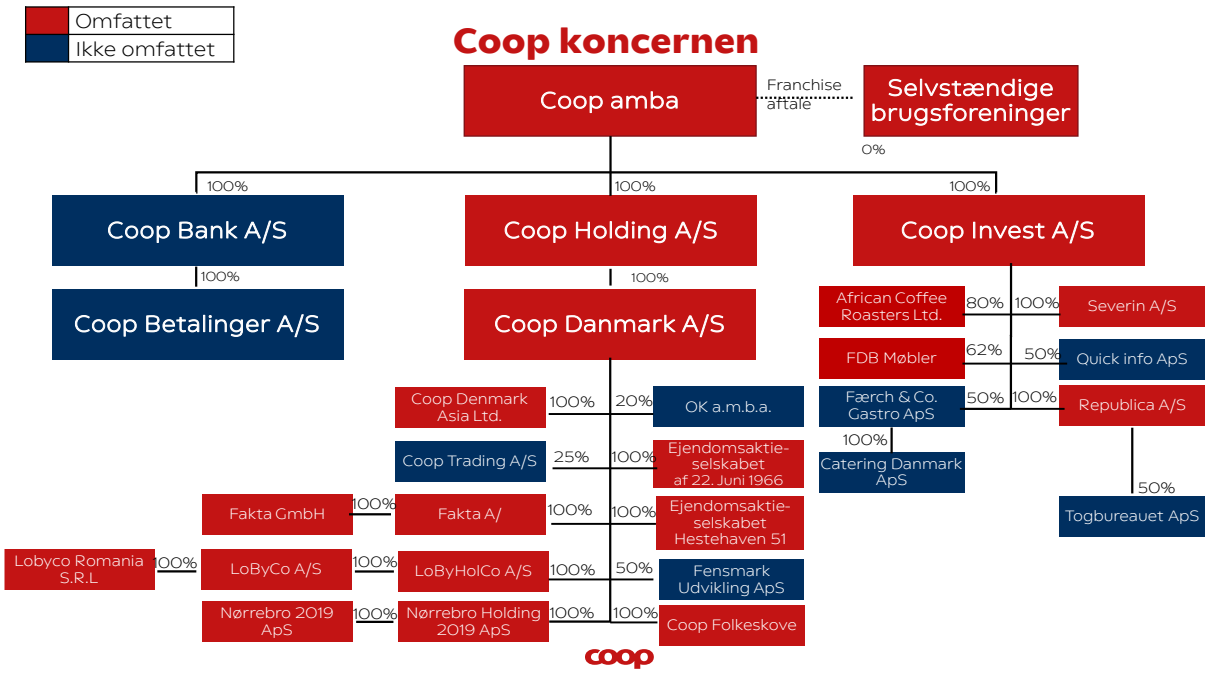
Koncern informations- og it-sikkerhedspolitik

Ansvarlig	Information Security
Kontaktinformation:	information.security@coop.dk
Omfattede virksomheder:	• Coop amba • Coop Danmark og datterselskaber, hvor Coop Danmark har bestemmende indflydelse • Coop Invest og datterselskaber, hvor Coop Invest har bestemmende indflydelse Ovennævnte virksomheder betegnes herefter samlet som Coop. Politikken omfatter ikke Coop Bank, der er underlagt selvstændig regulering.
Regler	• Databeskyttelsesforordningen • Finansiel revision (generelle it-kontroller) • Network and Information Security directive (NIS2)

Oversigt over omfang ses herunder:



1. Baggrund og formål

Informations- og it-sikkerhedspolitikken, herefter benævnt "Sikkerhedspolitikken", skal understøtte Coops værdigrundlag og vision.

Sikkerhedspolitikken fastlægger de grundlæggende rammer, vi arbejder ud fra, for at sikre en styret indsats. Coop Danmark og Coop Invest skal vedtage og implementere Informations- og it-sikkerhedspolitikker for disse selskaber og deres respektive datterselskaber hvor de har en bestemmende indflydelse. Disse politikker skal være i overensstemmelse med principperne i "Sikkerhedspolitikken".

I Sikkerhedspolitikken fastlægges de overordnede principper for sikkerhed i Coop. Principperne afspejler Coops tilgang til arbejdet med at beskytte vores datas fortrolighed, pålidelighed og tilgængelighed.

2. Sikkerhed i Coop

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

Fokus skal være på Coop som dagligvarevirksomhed med tilhørende investeringsselskab, Coop Invest.

En central opgave for Coop er, 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, kan kunden ikke købe varen, og de rette varer kan ikke komme frem til kunden.

Vores kunder og medlemmer er i centrum, og vores medlemsdata og vores omdømme er nogle af vores vigtigste aktiver. Med vores øgede indsats for at anvende digitale løsninger til at give kunderne en god indkøbsoplevelse, er det derfor afgørende, at vores kunder har tillid til vores løsninger.

3. Grundlæggende principper

Vores systemer skal være fremtidssikrede og gøre hverdagen lettere for vores kunder og vores butikker. Det betyder, at vi skal sikre en god struktur i løsningerne og

veldokumenterede arbejdsprocesser. Derfor skal der foretages en central registrering af data og it-systemer, som er anvendt på tværs af de virksomheder der er omfattet af denne politik. Følgende principper er fundamentet for sikkerhed i Coop:

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.

4. Styring af informationssikkerhedsarbejdet

Coop skal etablere og drive et ledelsessystem for informations- og it-sikkerhed, der er forankret i Coops forretning.

Ledelsessystemet er baseret på standarderne i ISO27000-serien, som er et internationalt anerkendt rammeværk for etablering af ledelse af informationssikkerhed. Dette for at sikre et gennemtestet ledelsessystem og et fælles sprog. Standarderne sættes ind i Coops kontekst og tilpasses den virkelighed, vi agerer i.

5. IT-sikkerhedsorganisationen og ansvar

I nærværende afsnit præciseres det ansvar og de opgaver, der påhviler de relevante aktører i Coop og de selvstændige brugsforeninger.

Coop amba

Coop amba bestyrelsen har det overordnede ansvar for overholdelse af politikken i ambas virke. Coop ambas bestyrelse har delegeret varetagelsen af informationssikkerhedsagendaen på vegne af amba til Coop Danmarks direktion.

Selvstændige brugsforeninger (Coop franchise)
De selvstændige brugsforeninger er selvejende virksomheder, som er meldt ind i Coop amba foreningen, og som har indgået en franchiseaftale med Coop Danmark. Derigennem er brugsforeningerne kontraktuelt forpligtet til at anvende Coops it-løsninger.

Som angivet i franchiseaftalen skal de selvstændige brugsforeninger anskaffe og installere nødvendig it-teknologi i forhold til Coop Danmarks instruktioner. Derudover skal de overholde de til enhver tid gældende retningslinjer, herunder retningslinjerne for sikkerhed (jf. Kæde og franchiseaftalen § 17).

Bestyrelserne i Coop Danmark og Coop Invest
Bestyrelserne har det overordnede ansvar for informations- og it-sikkerheden og skal fastlægge den overordnede risikoappetit.

Direktionerne i Coop Danmark og Coop Invest
Direktionerne i Coop Danmark og Coop Invest skal vedtage og sikre implementering af de nødvendige specifikke politikker, der udmønter denne koncernpolitik, og som sikrer den generelle styring af informationssikkerheden. Politikkerne skal omfatte datterselskaber, hvor Coop Danmark eller Coop Invest har bestemmende indflydelse.

Direktionerne har ansvaret for at igangsætte initiativer for at løfte it-sikkerheden i alle forretningsområder, hvor det måtte være påkrævet. Eksempelvis for at tilstræbe et forventeligt sikkerhedsniveau i forhold til sammenlignelige virksomheder eller for at opfylde relevant regulering.

Information Security
Coops Danmarks direktion har udpeget en chef for informationssikkerhed (CISO), der driver afdelingen Information Security.

Information Security har ansvaret for at sikre, at der er etableret de nødvendige rammer for arbejdet med informations- og it-sikkerhed i Coop Danmark.

Derudover varetager afdelingen, på vegne af Coop amba, den centrale rådgivningsfunktion om it-sikkerhedsmæssige forhold.

Forretningsledelse i direkte reference til direktionen
Den øverste forretningsledelse har det operationelle ansvar for en forsvarlig håndtering af informations- og it-sikkerheden samt udarbejdelse af planer for eventuelle mitigerende handlinger på deres ansvarsområder.

Eksterne konsulenter og leverandører
Ingen eksterne konsulenter og leverandører må varetage de ledelsesmæssige roller eller have bestemmende indflydelse på forretningsmæssige beslutninger.

De eksterne konsulenter og leverandører, der vurderes at have behov for adgang til systemer på Coops netværk, må alene tildeles adgang til de systemer, hvor der er et arbejdsbetinget behov.

6. Opfølgning

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

Opdatering af årstal ved revurdering sker uden forelæggelse for bestyrelse.