KOMBIT

Version 2.0

Informations-sikkerhedspolitik for KOMBIT

Indholdsfortegnelse

Forord fra ledelsen

KOMBIT har gennem mange år lagt vægt på informationssikkerhed. Med forretningsstrategien "Kommunal Digital Bevægelse" for perioden 2023 – 2027 går KOMBIT endnu videre for at bistå de danske kommuner med håndtering af det stadigt stigende trusselsniveau, der knytter sig til digitalisering. Det handler om at beskytte borgerne og deres velfærd, og denne informationssikkerhedspolitik udmønter strategien i den henseende.

KOMBIT forvalter de største it-løsninger for landets kommuner. Det indebærer, at KOMBIT på kommunernes vegne stiller krav til alle dele af en it-løsnings livscyklus; idé, udvikling, drift og udfasning. Det omfatter også krav om informationssikkerhed til bl.a. it-leverandørerne, hvilket er grundstenen for robuste kommunale it-løsninger.

Informationssikkerhed er samtidig en forudsætning for, at KOMBITs egen organisation på betryggende vis kan varetage forvaltningen af både de nuværende it-løsninger og leveringen af nye strategiske cyberinitiativer. Derfor er det et centralt mål, at KOMBIT opretholder compliance og lovmedholdelighed samt et sikkerhedsniveau, der sikrer en tilstrækkelig grad af resiliens i både organisationen og løsningerne.

Kristian Vengsgaard

Administrerende direktør/CEO

1. Indledning

For KOMBIT handler informationssikkerhed om at bevare fortrolighed, integritet og tilgængelighed af information. Dette indebærer, at data i de kommunale it-løsninger skal være sikret mod at blive kompromitteret og forvansket, samtidig med, at data er tilgængelige for de rette brugere til de rette formål.

Informationssikkerhed omfatter KOMBITs indsats inden for it-sikkerhed, cybersikkerhed[1] samt persondatasikkerhed og anden databeskyttelse.

KOMBIT bygger sin metodiske tilgang til informationssikkerhedsarbejdet på principperne i ledelsessystemet ISO/IEC 27001, Informationssikkerhed, og supplerer med andre relevante rammeværk på en sammenhængende og praktisk operationel måde, hvor det skønnes nyttigt.

Med afsæt i KOMBITs strategi "Kommunal Digital Bevægelse" for perioden 2023 – 2027 har denne informationssikkerhedspolitik til formål at sætte rammen om en passende, effektiv og ledelsesforankret styring af KOMBITs informationssikkerhed.

2. Informationssikkerhed i KOMBIT

KOMBIT har gennem årene haft et stadig større fokus på sikkerhed. Udviklingen har fulgt samfundets behov for driftssikkerhed i takt med den stigende digitalisering, øget bevidsthed om og krav til beskyttelse af borgernes personoplysninger – til i dag, hvor cyberangreb dagligt rammer myndigheder og virksomheder. Derfor er informationssikkerhed et af de centrale temaer i KOMBITs strategi.

Det er KOMBITs ansvar at leve op til lovkrav, så vi kan levere sikre løsninger til kommunerne og samtidig have styr på vores egen sikkerhed. Dermed bidrager vi til at sikre et højt cyber- og informationssikkerhedsniveau i det offentlige Danmark og understøtter det fortsat høje tillidsniveau mellem borgere og myndigheder.

For at omsætte politikken til praksis arbejder KOMBIT i perioden 2023–2027 med konkrete initiativer, herunder:

- Målrettede cyberinitiativer
- Informationssikkerhed i de kommunevendte it-løsninger
- Styrkelse af KOMBITs egen sikkerhedsorganisation

2.1 Konkrete cyberinitiativer

- **Støtte til best practice**
  Resultatet af en spørgeskemaundersøgelse, som KOMBIT foretog i 2023 blandt kommunale beslutningstagere, viste, at 90 pct. af borgmestre og kommunaldirektører gerne ser, at

KOMBIT bistår kommunerne med at opretholde en høj informations-, data- og cybersikkerhed. Det kan for eksempel være øget støtte til best practice i alle kommuner med mulighed for yderligere skræddersyet assistance til udvalgte kommuner.

- **Fælleskommunal cybersikkerhedsenhed**
  KOMBIT har etableret en fælleskommunal cybersikkerhedsenhed, KommuneCERT. Enheden skal i de kommende år gradvist udvikles med fokus på at styrke kommunernes evner til at opdage og reagere på cyberhændelser og understøtte fremtidige services inden for cybersikkerhed.
  Formålet med KommuneCERT vil løbende blive tydeliggjort og præciseret, efterhånden som arbejdet med at udvikle en sektorfælles tilgang til trussels- og sårbarhedsvurderinger, monitorering, beredskabs- og krisestøtte samt rådgivning og kompetenceopbygning skrider frem.
  Allerede i dag tilbyder KommuneCERT en række ydelser til danske kommuner, herunder videndeling om varsler og best practice.

  Yderligere information om KommuneCERT og dets tilbud kan findes på:
  KommuneCERT | Kommunernes fælles cybersikkerhedsenhed

- **Kompetence-, awareness- og beredskabsmæssige initiativer**
  KOMBIT vil gennemføre forskellige kompetence-, awareness- og beredskabsmæssige initiativer for at øge den kommunale modstandsdygtighed i forhold til cyberangreb. Ligesom det er vigtigt for KOMBIT at bistå kommunerne med implementering og anvendelse af it-løsninger, er det centralt at støtte kommunerne i at håndtere den nødvendige informationssikkerhed, der følger med. Herudover tilbyder KOMBIT, hvis kommunerne ønsker det, rådgivning inden for en bred vifte af informationssikkerhedsemner.

- **Effektivisering og optimering**
  KOMBIT vil simultant med NIS2 implementeringen sikre en effektivisering og optimering af måden, vi arbejder på, herunder ensretning af: formater og skabeloner, risikoanalyser samt KPI'er for informationssikkerhed og rapportering heraf.

2.2 Informationssikkerhed i de kommunevendte it-løsninger

KOMBITs arbejde med informationssikkerhed i de kommunevendte it-løsninger bygger på tydelige principper, som altid er en integreret del af vores praksis og udvikling af løsninger.

- **Informationssikkerhedskrav**
  Som forvalter af kommunernes it-løsninger påtager KOMBIT sig et klart ansvar for at efterleve gældende og kommende lovkrav – herunder NIS2-loven, NSIS, AI Act og GDPR. Vi arbejder systematisk med at sikre, at kravene er indarbejdet i løsningerne og i leverandørkæden, og at kommunerne løbende informeres og inddrages i afstemningen af krav og forventninger.

- **2. Security og privacy by design**
  Informationssikkerhed tænkes ind fra begyndelsen. Når KOMBIT udbygger og videreudvikler den kommunale it-portefølje – med nye teknologier som BI, AI og machine learning og med en målarkitektur, der understøtter flerleverandør-setup – sker det altid med sikkerhed og databeskyttelse som grundlæggende præmis. Principperne om *security/privacy by design*

sikrer, at borgernes data og samfundets tillid beskyttes samtidig med, at kommunerne får gevinsterne ved datadrevet forvaltningsledelse.

- **Samlet tilgang**
  Alle principper og initiativer samles i KOMBITs årshjul for informationssikkerhed, der er baseret på ISO27001. Det sikrer en helhedsorienteret og kontinuerlig proces, hvor vi altid arbejder med cyber- og informationssikkerhed som en integreret del af både vores egen praksis og de løsninger, vi leverer til kommunerne.

2.3 Styrkelse af KOMBITs egen sikkerhedsorganisering

KOMBITs sikkerhedsindsatser retter sig ikke kun mod kommunerne, men også mod KOMBIT selv. En stærk sikkerhedsorganisation er udgangspunktet for, at KOMBIT har de ressourcer, der skal skabe værdi for kommunerne i deres arbejde med informationssikkerhed. Hensigten er at opnå og bevare et niveau, hvor KOMBIT har en risikobaseret og målbar informationssikkerhed, der er i overensstemmelse med best practise. Dette vil sikre kommunerne en højt kvalificeret samarbejdspartner i KOMBIT fremadrettet.

3. Målsætninger

Denne informationssikkerhedspolitik skal på et overordnet niveau sikre informationssikkerheden i KOMBITs leverancer til kommunerne og i egen organisation i forhold til mennesker, processer, teknologier og lokationer.

KOMBITs målsætninger for informationssikkerhed er følgende:

- KOMBIT skaber resiliente it-miljøer, hvor sikkerheden er implementeret ud fra en risikobaseret tilgang, for på denne måde at sikre, at der er implementeret de nødvendige kontroller, at de er proportionelt implementeret, så omkostningen ved sikkerhedsforanstaltninger står mål med behandlingerne, og sidst, at sikre, at der er implementeret tilstrækkelige kontroller for at mitigere relevante og aktuelle trusler.
- KOMBIT bliver gennem de strategiske initiativer, der er beskrevet nærmere ovenfor, anerkendt som en værdiskabende og tæt samarbejdspartner af kommunerne i bestræbelserne på at styrke informationssikkerheden i det kommunale Danmark. KOMBIT forstår kommunernes forvaltningsopgaver indgående for at kunne bistå med relevante sikkerhedstiltag.
- KOMBIT udvikler over de kommende år sin fælleskommunale cybersikkerhedsenhed, KommuneCERT, for at kunne bidrage til en sektorfælles tilgang til trussels- og sårbarhedsvurderinger, monitorering, beredskabs- og krisestøtte, rådgivning, vejledning og kompetenceudvikling. KOMBIT samarbejder tæt med KL og relevante statslige myndigheder i udbygningen af KommuneCERT, der udvikles med udgangspunkt i anerkendte cybersikkerhedsrammeværker.
- KOMBITs tilgang til informationssikkerhed er risikobaseret med afsæt i ISO 31000, Enterprise Risk Management. KOMBIT styrker og ensretter - i videst mulig udstrækning - sin metodiske tilgang til risikovurdering i forhold til KOMBITs forretning, herunder politiske forhold, økonomi, kontraktuelle og regulatoriske forpligtelser samt informationssikkerhed.

- Udover denne generelle informationssikkerhedspolitik for KOMBIT udarbejdes og implementeres en række underliggende specifikke emnepolitikker, der fastsætter målsætninger og metode for særlige områder inden for KOMBITs forretning. Disse vil blive udarbejdet/opdateret efter best practice og vil være i overensstemmelse med gældende lovgivning. Direktionen godkender alle emnepolitikker, så den nødvendige ledelsesforankring løbende sikres.
- KOMBIT gennemfører som en del af NIS2 implementeringen en opgradering og tilpasning af den eksisterende metodik, til et niveau, der kan sikre lovmedholdelighed i it-miljøerne, både i forhold til gældende lovgivninger, og at den kan rumme fremtidige lovgivninger. KOMBITs metodikker inden for informationssikkerhed bygges efter principperne på anerkendte rammeværker.

4. Principper for KOMBITs arbejde med informationssikkerhed

KOMBITs principper med henblik på at vise vejen for alle KOMBITs aktiviteter i relation til informationssikkerhed er følgende:

- I KOMBIT har vi implementeret en risikobaseret tilgang til arbejdet med informationssikkerhed, der har til formål at sikre, at informationssikkerheden hele tiden er tilstrækkelig jf. de behandlinger, vi udfører, at der er implementeret den nødvendige sikkerhed jf. lovgivning og kommunale krav, og at sikkerhedstiltag er proportionale i forhold til både trusler og omkostninger forbundet hermed.
- I KOMBIT sikrer vi det rette beskyttelsesniveau gennem en kombination af et effektivt teknisk systemlandskab, teknologiske sikkerhedstiltag, forretningens processer, de fysiske rammer og medarbejdernes adfærd.
- I KOMBIT arbejder vi med informationssikkerhed som en integreret del af udvikling og drift af kommunevendte it-løsninger samt i KOMBITs egen organisation.
- I KOMBIT tager arbejdet med informationssikkerhed højde for de behov, som kommunerne, KL og øvrige væsentlige interessenter har i relation til partnerskabet med KOMBIT.

5. Ansvar for informationssikkerhed

Tilstrækkelig informationssikkerhed er et strategisk ledelsesansvar. Det øverste ansvar ligger hos KOMBITs direktion og bestyrelse.

KOMBIT har valgt at organisere arbejdet med informationssikkerhed, så det følger ansvaret for den øvrige forretningsorganisering. Det betyder, at fx systemejere varetager den udførende opgave og har ansvaret for, at ledelsen kan vurdere og handle rettidigt på de risici, der knytter sig til KOMBITs forretning – herunder risici for informationssikkerheden.

For at understøtte dette ansvar er der, under direktionen, etableret et team under ledelse af KOMBITs chef for Cyber, Analyse og Informationssikkerhed. Teamet gennemfører tværorganisatoriske indsatser og sikrer, at informationssikkerhed altid er integreret i KOMBITs praksis. Derudover er der oprettet en DPO-rolle, som varetages i overensstemmelse med GDPR's krav.

Sikkerhed i arkitekturen ejes af KOMBITs arkitekturfunktion, som har ansvar for at indarbejde informationssikkerhed i den overordnede målarkitektur og sikre, at principperne for sikkerhed og databeskyttelse er tænkt ind i alle løsninger fra starten.

Dermed er informationssikkerhed i KOMBIT forankret i den strategiske ledelse og omsat til en klar organisatorisk struktur, hvor ansvar og indsats går hånd i hånd.

6. Styring af informationssikkerheden

I KOMBIT er styring af informationssikkerhed – også kaldet governance – en praktisk tilgang til at sikre, at forretningens håndtering af informationer sker i overensstemmelse med gældende lovgivning og relevante krav. KOMBITs governance- og informationssikkerhedsledelsessystem etablerer klare rammer for ansvarsfordeling og for, hvordan informationssikkerheden understøttes, styres og vedligeholdes i hverdagen på tværs af hele organisationen.

Informationssikkerhedsledelsessystemet er:

- **Konsistent**: Der er en ensartet tilgang til styring, dokumentation og opfølgning. Metoder og rammer er genkendelige og gennemgående, uanset hvor i organisationen man befinder sig.
- **Cyklisk**: Systemet er bygget op omkring gentagelige processer. Aktiviteter er lagt i et årshjul, så det sikres, at sikkerheden løbende vedligeholdes og udvikles.
- **Understøttet af eksisterende systemer**: Informationssikkerhedssystemet bygges i og omkring de systemer og værktøjer, der allerede er i brug i KOMBIT, fx, til dokumentation, opgavestyring og rapportering – så implementeringen er effektiv og forankret i praksis.

Helt overordnet betyder det, at KOMBITs informationssikkerhedssystem understøtter en styring, der er risikobaseret og som er forankret i de tre centrale principper:

- **Nødvendig:** Beskyttelsen tager udgangspunkt i reelle risici og behov.
- **Proportional:** Indsatserne står mål med truslerne og er ikke mere omfattende end nødvendigt.
- **Tilstrækkelig:** Foranstaltningerne er dækkende og sikrer, at krav og forventninger faktisk bliver opfyldt.

6.1 Styringsdokumenter

Styringsdokumenterne til informationssikkerhed i KOMBIT er forankret i et enkelt og hierarkisk opbygget system af: politikker, regler og procedurer, og sammenhængen mellem dem fremgår tydeligt, så ethvert dokument altid henviser til det ovenstående dokument i hierarkiet. Derudover kan der i et

dokument henvises til andre dokumenter, hvor der er en vis emnemæssig tilknytning. Forståelsen af og formatet for politikker, regler og procedurer svarer i videst muligt omfang til de tilsvarende styringsdokumenter, der generelt anvendes i KOMBITs forretning.

Styringsdokumenter er som udgangspunkt udarbejdet af og ejes af den organisatoriske enhed i KOMBIT, der har det nødvendige ledelsesmandat, den faglige ekspertise og den grundlæggende forvaltningsforståelse.

Alle dokumenter etableres efter en fastlagt metodik, som illustreret nedenfor:

6.2 Dokumentation, kommunikation, tilgængelighed og efterlevelse

Alle styringsdokumenter er dokumenteret, kommunikeret og let tilgængelige, så det er muligt at arbejde effektivt efter dem.

Effektiv efterlevelse af de fastsatte ansvarsområder og arbejdsgange i styringsdokumenterne er omdrejningspunktet for, at der er reel informationssikkerhed. KOMBIT sikrer derfor, at der er arbejdet metodisk med roller og ansvar samt gennemsigtigheden heri.

For at sikre, at viden om efterlevelse af informationssikkerhedspolitikken og styringsdokumenterne er forankret i forhold til roller og ansvar, tilvejebringes løbende rollebaseret uddannelse inden for cyber- og informationssikkerhed, der sikrer, at alle roller forstår deres ansvar.

6.3 Kontrol og forbedring

En central del af informationssikkerhedsledelsessystemet er kontrol og forbedring. Systemet er derfor opbygget med løbende rapportering af målepunkter og KPI'er til direktionen.

Kravet om dokumentation af styringsdokumenter og deres efterlevelse er en forudsætning for, at kontrol kan finde sted. KOMBIT vil som en del af årshjulsaktiviteterne føre kontrol af den påkrævede

dokumentation. Der udføres årligt en ekstern kontrol af KOMBIT i forhold til efterlevelsen af KOMBITs databehandleraftaler med kommunerne.

Der er altid et forbedringspotentiale at overveje, og derfor skal alle styringsdokumenter genbesøges jævnligt og opdateres ved væsentlige ændringer. Dette sker for at sikre, at styringsdokumenterne til enhver tid er tidssvarende og effektive i forhold til den aktuelle forvaltnings-, forretnings-, trussels- og samfundskontekst.

6.4 Dispensation

Der kan opstå situationer, hvor der konkret er behov for at fravige de foreliggende styringsdokumenter i større eller mindre omfang. I sådanne situationer kan der dispenseres fra det, der er angivet i et styringsdokument, ved en beslutning af KOMBITs direktion på baggrund af en konkret begrundet forespørgsel. Denne beslutning dokumenteres og journaliseres. Det bør i tilfælde af dispensation overvejes, om der er behov for en opdatering af det pågældende styringsdokument.

7. Risikovurdering og -styring

Informationssikkerhed hænger sammen med politiske forhold, økonomi, kontraktuelle forpligtelser og regulatoriske krav. Dette samspil er grundlaget for KOMBITs ensartede tilgang til risikovurdering og giver en helhedsorienteret indsigt i risici for forretningen. Indsigten styrker prioritering af indsatser og ressourcer på strategisk, taktisk og operationelt niveau.

Risikostyringen bygger på DS/ISO 31000:2018 og KOMBITs risikoledelsespolitik. Gennem Enterprise Risk Management anvendes risikolister, modeller og procestrin, der sikrer rettidig og tilstrækkelig håndtering af risici.

KOMBIT arbejder risikobaseret med kontroller i politikker og procedurer. En klassificeringsmodel sikrer, at kritiske it-systemer får den højeste grad af sikkerhed, mens mindre kritiske beskyttes proportionelt. Vurderinger sker i fagligt fællesskab, så løsningerne er tilstrækkelige, nødvendige og proportionelle – og samtidig omkostningseffektive.

For at følge med i et dynamisk trusselsbillede anvender KOMBIT KPI'er på udvalgte kontroller, så sikkerheden løbende kan vurderes og justeres.

8. Awareness og uddannelse

Alle ansatte i KOMBIT skal have et tilstrækkeligt fokus på informationssikkerhed til at forstå, hvorfor det er vigtigt for forretningen, og for at forstå, hvad de selv kan gøre for at sikre et tilstrækkeligt niveau af cyber- og informationssikkerhed. Menneskers ageren er fortsat det mest sårbare led i værnet om cyber- og informationssikkerhed, da langt de fleste cyberangreb lykkes gennem sårbarheder på medarbejderniveau. For at styrke KOMBIT på dette område gennemfører medarbejdere, indstationerede og eksterne konsulenter hvert år uddannelse indenfor GDPR, informations- og cybersikkerhed.

KOMBIT sørger derudover for, at uddannelse i informationssikkerhed på et højere niveau gennemføres af alle de medarbejdere, for hvem det er nødvendigt i forhold til deres roller og ansvar i organisationen. Dette behov afdækkes gennem de løbende medarbejdersamtaler. Det kan f.eks. være inden for cybersikkerhed, databeskyttelse, risikovurdering og sikkerhed i nye teknologier såsom cloud, BI og AI.

9. Den løbende forbedring

KOMBITs informationssikkerhedspolitik skal til enhver tid være i overensstemmelse med KOMBITs strategi og dens forretningsmæssige udmøntning i organisationen. Derfor skal dette dokument, tillige med alle styringsdokumenter vedrørende informationssikkerhed, vedligeholdes, dvs., gennemgås og, hvis nødvendigt, opdateres ved væsentlige ændringer og mindst én gang årligt.

Opdateringer dokumenteres i det pågældende dokuments versionshistorik.

10. Kommunikation

For at informationssikkerhedspolitikken kan fungere efter sit formål, skal den til enhver tid opdaterede version kommunikeres direkte og i øvrigt være lettilgængelig for alle medarbejdere. Medarbejderne i KOMBIT skal kende til informationssikkerhedspolitikkens indhold og betydning for deres daglige arbejde. Politikken vil desuden blive offentliggjort på KOMBITs hjemmeside, så den også er lettilgængelig for KOMBITs interessenter.

Versionshistorik

Versionsnr.	Enhed, navn, titel	Opdatering:	Dato
2.0	CAI, MZN	Godkendt af direktionen	27.01.2026