KOMBIT

Version 1.1

Informations-sikkerhedspolitik for KOMBIT

Indholdsfortegnelse

Indholdsfortegnelse 2

1. Indledning 4

2. Informationssikkerhed i den kommunale digitale bevægelse 4

2.1 Konkrete cyberinitiativer 5

2.2 Informationssikkerhed i de kommunevendte it-løsninger 6

2.3 Styrkelse af KOMBITs egen sikkerhedsorganisering 7

3. Målsætninger 7

4. Principper for KOMBITs arbejde med informationssikkerhed 8

5. Krav til informationssikkerhed 9

6. Ansvar for informationssikkerhed 9

7. Governance om informationssikkerhed 9

7.1 Styringsdokumenter 10

7.2 Dokumentation, kommunikation, tilgængelighed og efterlevelse 10

7.3 Kontrol og forbedring 11

7.4 Dispensation 11

8. Risikovurdering og -styring 11

9. Awareness og uddannelse 12

10. Den løbende forbedring 12

11. Kommunikation 12

12. Versionshistorik 13

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, men også leveringen af nye strategiske cyberinitiativer.

Kristian Vengsgaard

Administrerende direktør/CEO

1. Indledning

For KOMBIT handler informationssikkerhed om at bevare fortrolighed, integritet og tilgængelighed af information, som det er defineret i ISO27000-standarden[1]. Dette indebærer, at data i de kommunale it-løsninger skal være sikret mod at blive kompromitteret og forvansket, og de skal samtidig være tilgængelige for de rette brugere.

Informationssikkerhed omfatter KOMBITs indsats indenfor it-sikkerhed, cybersikkerhed[2] samt persondatasikkerhed og anden databeskyttelse.

ISO-standarderne om informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse er toneangivende indenfor international best practice, og derfor vil KOMBIT styrke sin metodiske tilgang til informationssikkerhedsarbejdet ud fra disse standarder, men også inddrage andre relevante rammeværk på en sammenhængende og praktisk operationel måde.

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 den kommunale digitale bevægelse

KOMBIT har gennem årene haft et stadig større fokus på sikkerhed. Udviklingen har nøje flugtet med samfundets behov for driftssikkerhed ved den stigende digitalisering, øget bevidsthed om og krav til beskyttelse af borgernes personoplysninger, til i dag hvor cyberangreb rammer myndigheder og virksomheder hver eneste dag. Derfor er sikkerhed også et af tre centrale kommunale temaer for KOMBIT.

KOMBITs strategi har disse elementer:

[1] ISO/IEC 27000:2018 Informationsteknologi – sikkerhedsteknikker – ledelsessystemer for informationssikkerhed – oversigt og ordliste

[2] For definition af og sammenhæng mellem begreberne – informationssikkerhed, it-sikkerhed og cybersikkerhed – henvises til: www.cfcs.dk/da/cybertruslen/ordforklaringer/

Strategien er i perioden 2023 – 2027 afsæt for:

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

Samlet gælder, at KOMBIT skal arbejde med informationssikkerhed på et niveau, der er passende i forhold til den kommunale digitale udvikling i en foranderlig virkelighed. Det sker i fortsat tæt samarbejde med bl.a. kommuner, KL, it-leverandører og relevante statslige myndigheder. KOMBIT tilstræber det samme niveau af informationssikkerhed for de it-løsninger, som KOMBIT leverer til kommunerne, som for sin egen systemunderstøttelse.

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 over de kommende år udvikles til at være kommunernes SOC/SAC (security operations and analysis center) og sikre en sektorfælles tilgang til trussels- og sårbarhedsvurderinger, monitorering, beredskabs- og krisestøtte, rådgivning, vejledning og kompetenceudvikling.

KommuneCERT tilbyder i dag en række ydelser til danske kommuner bl.a. videndeling om varsler og best practice. Mere information om KommuneCERT og dens ydelser kan fåes 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. Lige som det er vigtigt for KOMBIT at bistå kommunerne med implementering og anvendelse af it-løsninger, er det centraltat støtte kommunerne i at håndtere den nødvendige informationssikkerhed, der følger med.

- **Skræddersyet rådgivning om sikkerhed**
  KOMBIT vil tilbyde skræddersyet rådgivning om f.eks. GDPR-implementering og cybersikkerhed i forbindelse med både fælleskommunale it-løsninger og kommunernes egne løsninger. Med strategien vil KOMBIT nødvendigvis fortsætte sin oprustning af kompetencer om informationssikkerhed over en bred kam, og det bør komme kommunerne til gode i videst muligt omfang.

2.2 Informationssikkerhed i de kommunevendte it-løsninger

- **Security/privacy by design**
  KOMBIT vil til gavn for kommunerne udbygge og videreudvikle den kommunale it-infrastruktur. I den forbindelse vil KOMBIT styrke arbejdet med bl.a. at indsamle, sammenstille, validere og udstille data til brug for kommunernes opgaveløsning. Nye teknologier som BI, AI og machine learning vil blive taget i brug, og ny målarkitektur til fremme etableringen af et fler-leverandør-setup. Det er en forudsætning for at kunne opnå gevinsterne ved datadrevet forvaltningsledelse og samtidig beskytte borgerne og samfundet, at sikring af informationssikkerheden tænkes ind allerede fra begyndelsen f.eks. som security/privacy by design.

- **Informationssikkerhedskrav**
  Allerede i dag indebærer rollen som forvalter af it-løsninger på vegne af kommunerne, at KOMBIT påtager sig en række forpligtelser i forbindelse med efterlevelse af krav i it-løsningerne og i leverandørkæden. Der gælder bl.a. lovkrav vedrørende sikring af personoplysninger og data om finansielle transaktioner, underretning om brud på persondatasikkerheden samt implementering af NSIS-standarden. KOMBITs bistand til kommunerne skal styrkes yderligere, ikke mindst i lyset af den kommende NIS2-lovgivning, som implementerer cybersikkerhedsdirektivet (også kaldet NIS2), som vil træde i kraft den 1. juli 2025.

- **Styrket leverandørtilsyn**
  KOMBIT fører desuden tilsyn på kommunernes vegne ved indhentning og vurdering af revisionserklæringer fra leverandørerne af de it-løsningerne, som KOMBIT har indgået kontrakt, herunder databehandleraftale med. KOMBIT vil fortsat supplere og styrke sit tilsyn

med it-leverandører ved proaktivt og effektivt at stille dokumentation til rådighed for kommunerne. Det gælder for dokumentation af såvel it-leverandørernes efterlevelse af databehandleraftaler og for lovmedholdelighed i it-løsningerne, herunder af GDPR og hvis relevant NIS2. KOMBIT vil også indgå i en tættere dialog med kommunerne om deres behov i denne henseende.

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 vil kunne blive certificeret i henhold til ISO27001-standarden[3]. Det vil sikre kommunerne en højt kvalificeret samarbejdspartner i KOMBIT fremadrettet.

- Konkret vil KOMBIT opgradere sit ledelsessystem for informationssikkerhed (ISMS) med dertil hørende governance, trusselsidentifikation og risikovurdering, organisatorisk og teknisk faglige kompetencer samt it-understøttelse. Det vil skabe fundamentet for, at KOMBIT kan styrke indsatsen med bl.a. security/privacy by design, informationssikkerhedskrav og leverandørtilsyn på egne vegne såvel som på kommunernes vegne.

3. Målsætninger

Denne informationssikkerhedspolitik skal på et overordnet niveau sikre informationssikkerhed, herunder cybersikkerhed og databeskyttelse i KOMBITs leverancer til kommunerne og i sin egen organisation i forhold til mennesker, processer, teknologier og lokationer.

KOMBITs målsætninger for informationssikkerhed er følgende:

1. KOMBIT skal gennem de strategiske initiativer, der er beskrevet nærmere ovenfor, anerkendes som en værdiskabende og nær samarbejdspartner af kommunerne i bestræbelserne på at styrke informationssikkerheden. KOMBIT skal forstå kommunernes forvaltningsopgaver indgående for at bistå med relevante sikkerhedstiltag.

2. KOMBIT skal over de kommende år udvikle sin fælleskommunale cybersikkerhedsenhed, KommuneCERT, til at være kommunernes SOC/SAC (security operations and analysis center) og sikre 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 indenfor rammeværket, NIST Cybersecurity framework.

[3] ISO/IEC 27001:2021 Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse – Ledelsessystemer for informationssikkerhed - Krav

3. KOMBITs tilgang til informationssikkerhed er risikobaseret med afsæt i ISO27005-standarden[4]. KOMBIT vil styrke og i videst mulig udstrækning ensrette sin metodiske tilgang til risikovurdering i forhold til KOMBITs forretning, herunder politiske forhold, økonomi, kontraktuelle og regulatoriske forpligtelser samt informationssikkerhed.

4. Udover denne generelle informationssikkerhedspolitik for KOMBIT udarbejdes og implementeres en række underliggende specifikke emnepolitikker, der fastsætter målsætninger og metode for særlige områder indenfor KOMBITs forretning: Bl.a. styring af aktiver, kryptering, logning, backup og restore samt sletning af data, administration af dataadgange, systemvedligeholdelse, leverandørstyring samt håndtering af sikkerhedshændelser og beredskab. Det kan også være hensigtsmæssigt at forankre brugen af nye teknologier såsom kunstig intelligens og machine learning og nye forretningsmodeller i emnepolitikker. Direktionen fastsætter hvilke emnepolitikker, der løbende er nødvendige, og hvilke organisatoriske enheder ansvaret for emnepolitikker kan delegeres til.

5. KOMBIT gennemfører et internt projekt, der har til formål at opgradere og udbygge det eksisterende ledelsessystem for informationssikkerhed (ISMS) til et niveau, der kan sikre lovmedholdelighed i forhold til NIS2-lovgivning og som nævnt kan kvalificere til en certificering i henhold til ISO27001-standarden. Det er centralt, at dette ISMS understøtter KOMBITs strategi og indgår i den overordnede governance for KOMBITs forretning.

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:

- Informationssikkerhed er det beskyttelsesniveau for information, som passer til hele KOMBITs forretning, og som derfor skal forankres i KOMBITs direktion og bestyrelse.

- Informationssikkerhed sikres gennem medarbejdernes adfærd, forretningens processer og fysiske rammer samt et sammenhængende og effektivt teknisk systemlandskab.

- Informationssikkerhed tilrettelægges så vidt muligt på en enkel, ensartet og effektiv måde i overensstemmelse med den fastlagte governance.

- Informationssikkerhed er en integreret del af udvikling og drift af kommunevendte it-løsninger samt i KOMBITs egen organisation.

- Informationssikkerhed i KOMBIT tager højde for de behov, som kommunerne, KL og øvrige væsentlige interessenter har til partnerskabet med KOMBIT.

[4] ISO/IEC 27005:2022 Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse – Vejledning i styring af informationssikkerhedsrisici

5. Krav til informationssikkerhed

KOMBITs forretning er underlagt en række lovgivningskrav, der specifikt vedrører nogle af de it-løsninger, som KOMBIT forvalter. De påvirker direkte eller indirekte informationssikkerheden, hvorfor sikkerhedsforanstaltninger er påkrævet. KOMBITs forretning er også underlagt generelle lovgivningskrav om informationssikkerhed, bl.a. GDPR og i et givent omfang NIS2. Disse to eksempler på regulering omfatter konkrete sikkerhedskrav, men forpligter også til, at der gennemføres risikovurderinger med henblik på fastlæggelse af passende organisatoriske og tekniske sikkerhedsforanstaltninger. KOMBIT sikrer efterlevelsen af alle sådanne lovgivningskrav som en del af sit ISMS.

Indenfor området for kontrol med kontraktbaserede sikkerhedskrav til leverandørerne af de kommunevendte it-løsninger, anvender KOMBIT ITIL-standarden. Tilsvarende gælder i forhold til håndtering af sikkerhedshændelser. Derfor vil ISO-standarden på disse områder blive anvendt sammen med ITIL.

6. Ansvar for informationssikkerhed

Informationssikkerhed er en integreret del af KOMBITs forretning. Ansvar for informationssikkerhed skal derfor følge ansvaret for den øvrige forretnings organisering, således som direktionen har fastsat. Det er et ledelsesansvar at vurdere og eje risici for KOMBITs forretning, herunder også risici for informationssikkerheden.

KOMBIT har etableret et informationssikkerhedsteam (InfoSec), som en stabsfunktion under ledelse af KOMBITs informationssikkerhedschef, hvis ansvar det er at gennemføre de informationssikkerhedsindsatser, der er tværorganisatoriske. Der er i KOMBIT desuden oprettet en DPO-funktion, som varetages i overensstemmelse med GDPRs krav hertil.

Det øverste ansvar for informationssikkerheden tilfalder KOMBITs direktion og bestyrelse.

7. Governance om informationssikkerhed

I en virksomhed som KOMBIT skal et ISMS tilgodese behovet for et fælles fundament for styring af informationssikkerhed. Det er af grundlæggende betydning, at medarbejderne har det samme fokus og metodeforståelse ved identifikation af væsentlige forretningsaktiver, risikovurdering og compliance mv. Samtidig skal systemet være forandringsparat i forhold til en samfundsmæssig kontekst, som er præget af en konstant og kraftig udvikling i teknologi og trusler. Der skal også være en agilitet i systemet, der tilgodeser, at KOMBIT leverer en række af forskellige it-løsninger til kommunerne, og med strategien vil yderligere differentiering i porteføljen kunne forventes.

7.1 Styringsdokumenter

Governance om informationssikkerhed i KOMBIT skal være forankret i et enkelt og hierarkisk opbygget system af styringsdokumenter: Politikker, regler og procedurer. Der skal i ethvert dokument henvises til dét 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 skal i videst mulig udstrækning svare til de tilsvarende styringsdokumenter, der anvendes i KOMBITs forretning generelt.

Styringsdokumenter udarbejdes og ejes af de organisatoriske enheder i KOMBIT, der har det nødvendige ledelsesmandat, faglige ekspertise og grundlæggende forvaltningsforståelse, der er påkrævet.

- **Politikker**
  Øverste i hierarkiet er den generelle informationssikkerhedspolitik og de specifikke emnepolitikker. Under den 4. målsætning i afsnit 3 er anvendelsen af emnepolitikker nærmere beskrevet.

- **Regler**
  Hver politik udmøntes i regler, som fremgår af et dokument, hvori der nærmere redegøres for, hvilke konkrete krav, der forpligter KOMBIT indenfor den respektive politik. Regler indenfor et område af KOMBITs virke, der ikke er dækket af en emnepolitik, forankres direkte i informationssikkerhedspolitikken.

- **Procedurer**
  Hvordan reglerne efterleves i KOMBIT, skal fremgå af procedurer. Procedurer i KOMBIT skal overordnet set have den samme funktion; nemlig at anvise en fremgangsmåde eller arbejdsgang, der skal følges af medarbejdere i et forløb (en proces). Der er til dette formål en række grundelementer, som vil skulle beskrives i alle typer af procedurer. Derudover kan der være behov for en vis grad af forskellighed med hensyn til, hvor omfattende og uddybende en procedure bør være for at tjene sit formål i en konkret sammenhæng og indenfor et konkret emne. Nogle procedurer vil være forholdsvis enkle og overordnede, mens andre procedurer bør være instruerende på detailniveau som en manual. Til en procedure kan der bilægges procesbeskrivelse, flowdiagram, skabeloner til dokumentation og lignende, hvis det er formålstjenesteligt.

7.2 Dokumentation, kommunikation, tilgængelighed og efterlevelse

Alle styringsdokumenter skal dokumenteres, kommunikeres og være let tilgængelige, så det er muligt at arbejde effektivt efter dem. Dette skal samtidig ske på en måde, der sikrer den fortrolighed, som knytter sig til et dokuments klassifikation.

Effektiv efterlevelse af de fastsatte ansvarsområder og arbejdsgange i styringsdokumenter er omdrejningspunktet for, at der er reel informationssikkerhed. Styringsdokumenter, der ikke efterleves, udgør omvendt en trussel mod informationssikkerheden i KOMBIT. Derfor er det nødvendigt, at

efterlevelsen dokumenteres i et givent format, og at direktionen står på mål for at fremme efterlevelse af kravene i styringsdokumenter og træffer de nødvendige forholdsregler, hvis det ikke sker.

7.3 Kontrol og forbedring

Kravet om dokumentation af styringsdokumenter og deres efterlevelse er desuden nødvendig for at eksistensen af begge dele kan bevises i forhold til intern og ekstern kontrol. Internt i KOMBIT vil der løbende blive udført kontrol af den påkrævede dokumentation som led i KOMBITs almindelige ledelsesstruktur og af KOMBITs informationssikkerhedsteam (InfoSec). Der udføres årligt en ekstern kontrol af KOMBIT i forhold til efterlevelsen af KOMBITs databehandleraftaler med kommunerne.

Af tilsvarende betydning er det, at styringsdokumenter til enhver tid er tidssvarende og effektive i forhold til den aktuelle forvaltnings-, forretnings-, trussels- og samfundskontekst. Der er med andre ord altid et forbedringspotentiale at overveje, og derfor skal alle styringsdokumenter genbesøges og eventuelt opdateres ved væsentlige ændringer, og mindst en gang årligt. Der skal foreligge dokumentation herfor i et givent format.

7.4 Dispensation

Der kan opstå situationer, hvor der konkret er et 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 i et givent format. Det skal i tilfælde af dispensation overvejes, om der er behov for en opdatering af det pågældende styringsdokument.

8. Risikovurdering og -styring

Risikovurdering på informationssikkerhedsområdet vil tage udgangspunkt i ISO27005-standarden: Gennem identifikation af aktiver og analyse af disse aktivers sårbarheder mod relevante trusler afklares risici, der enten nedbringes ved organisatoriske, personrelaterede, fysiske og teknologiske sikkerhedsforanstaltninger[5] eller accepteres af direktionen efter fastsatte risikoacceptkriterier. De nødvendige sikkerhedsforanstaltninger skal dokumenteres i en Statement of Applicability (SoA) og danner grundlaget for de krav, som KOMBIT stiller til sig selv og til leverandørerne af de kommunevendte it-løsninger. Risikovurderinger om informationssikkerhed i KOMBIT kommunikeres løbende til direktion og bestyrelsen.

Ligesom trusler ændrer sig løbende, gør også effekten af trufne sikkerhedsforanstaltninger. Der er derfor behov for at sikre, at risikovurderinger er tidssvarende, og at nødvendige sikkerhedsforanstaltninger er på plads. Som følge heraf skal risikovurderinger ligesom styringsdokumenter genbesøges og eventuelt opdateres ved væsentlige ændringer, og mindst en gang årligt. Der skal foreligge dokumentation herfor i et givent format.

[5] Der vil i risikohåndteringen som minimum blive taget stilling til ISO/IEC 27002:2022 Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse – Foranstaltninger til informationssikkerhed

Informationssikkerhed er et område, der spiller sammen med andre forretningsområder såsom politiske forhold, økonomi, kontraktuelle og regulatoriske forpligtelser. Dette samspil skal tydeliggøres. Samspillet er forudsætningen for at kunne ensrette og forenkle KOMBITs metodiske tilgang til risikovurdering, og dermed skabe en harmonisk, helhedsorienteret og forståelig indsigt i risici mod KOMBITs forretning. Denne indsigt skal bidrage til at give KOMBIT det stærkeste grundlag for prioritering af indsatser og ressourcer på både strategisk, taktisk og operationelt niveau.

9. Awareness og uddannelse

Alle ansatte i KOMBIT skal have et tilstrækkeligt fokus på informationssikkerhed til at forstå, hvorfor det er vigtigt for forretningen, og hvad ens eget ansvar er. Mennesker er i vid udstrækning det sårbareste led i værnet af cyber- og informationssikkerhed, og langt de fleste cyberangreb lykkes gennem sårbarheder på medarbejderniveau. Derfor gennemfører KOMBITs medarbejdere, indstationerede og eksterne konsulenter hvert år e-læring indenfor GDPR, information- og cybersikkerhed. E-læringsmodulerne er obligatoriske for alle, og gennemførelse af dem dokumenteres med et certifikat. Nyansatte er forpligtet at gennemføre e-læringsmodulerne senest 14 dage efter den første arbejdsdag.

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

10. Den løbende forbedring

KOMBITs informationssikkerhedspolitik skal til enhver tid være i overensstemmelse med KOMBITs strategi og dennes 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 en gang årligt.

Opdateringen dokumenteres i den pågældende dokuments versionshistorik.

11. 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 informationspolitikkens indhold og betydning for deres daglige arbejde. Politikken vil desuden blive offentliggjort på KOMBITs hjemmeside, så den også er lettilgængelig for KOMBITs interessenter.

12. Versionshistorik

Versionsnr.	Enhed, navn, titel	Opdatering:	Dato
1.0	InfoSec	Ny informationssikkerheds-politik for KOMBIT	6. december 2023
1.1	InfoSec	Review	5.december 2024