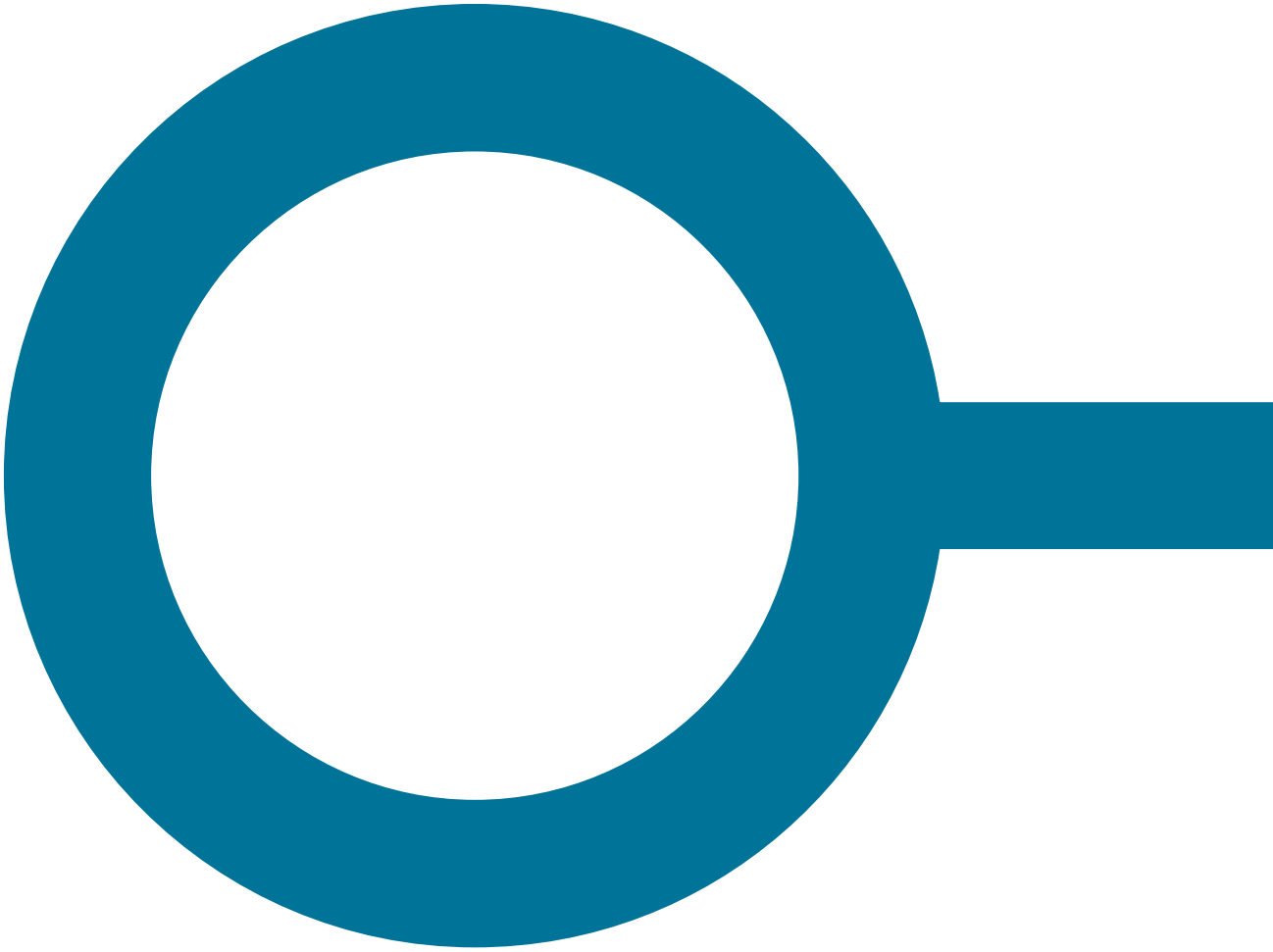

INFORMATIONSSIKKERHED

KOMBITS IT-SIKKERHEDSPOLITIK

Version 1.0

10. december 2019

KOMBIT

Kommunernes it-fællesskab

Versionshistorik

Versions-nummer	Dato	Afsnit der er ændret
1.0	10.12.2019	Gældende version

INDHOLDSFORTEGNELSE

1 FORMÅL

It-sikkerhedspolitikkens overordnede formål er at sætte rammerne for KOMBITs arbejde med it-sikkerhed og sikre konsistens i den mere konkrete udmøntning af KOMBITs informationssikkerhedsstrategi i forhold til en række it-sikkerhedsmæssige emner. Ved siden af it-sikkerhedspolitikken findes KOMBITs privatlivspolitk og de to politikker danner sammen grundelementerne i informationssikkerhedsstrategien.

2 OMFANG

KOMBITs it-sikkerhedspolitik gælder både eksternt i forhold til KOMBITs leverandører og samarbejdspartnere og internt i forhold til KOMBITs medarbejdere. KOMBIT stiller krav til leverandører og samarbejdspartnere om at understøtte KOMBITs it-sikkerhedspolitik.

It-sikkerhedspolitikken udmøntes i en række interne og eksterne retningslinjer og procedurer på udvalgte it-sikkerhedsmæssige områder som danner det samlede grundlag for KOMBITs sikring af en fortsat professionel håndtering af it-sikkerheden indenfor emner som fx:

- brugere, medarbejdere og eksterne samarbejdspartnere,
- fysisk sikkerhed,
- styring af netværk og drift,
- adgangsstyring og overvågning,
- sikkerhedskrav til it-systemer og løsninger,
- styring af og beredskab i forhold til cyberangreb og sikkerhedsbrud,
- risikovurdering og håndtering,
- sikkerhedsklassifikation af it-systemer, løsninger og data.

3 PRINCIPPER

3.1 Principper

KOMBITs principper for arbejdet med it-sikkerhed handler om at være bevidste om kendte og potentielle risici, som kan have en betydning for it-sikkerheden og med baggrund heri forholde os konkret hertil med henblik på at etablere et passende it-sikkerhedsniveau til imødegåelse af disse risici.

Målsætningen er at KOMBIT til enhver tid er i stand til at efterleve relevante gældende lov- og myndighedskrav samt de kontrakt- og aftalemæssige krav, der er aftalt for KOMBITs arbejde med it-sikkerhed. Endvidere skal KOMBIT proaktivt være i stand til at dæmme op for fremtidige risici.

3.2 Virkemidler

Virkemidler skal forstås som de forudsætninger, der skal være tilstede for at sikre effektiv styring af it-sikkerheden i KOMBIT. KOMBIT arbejder løbende på at sikre, at de nødvendige virkemidler er tilstede i tilstrækkelig grad for at sikre de af KOMBIT fastlagte retningslinjer og procedurer i forhold til it-sikkerheden efterleves og dermed sikrer et passende niveau for it-sikkerhed.

3.3 Ressourcer

I KOMBIT sikres det, at der er allokeret tilstrækkelige ressourcer til at kunne håndtere og i praksis udmønte KOMBITs Informationssikkerhedstrategi og KOMBITs it-sikkerhedspolitik med tilhørende retningslinjer og procedurer. De allokerede ressourcer vurderes løbende for at sikre, at der til enhver tid er de nødvendige ressourcer til at understøtte KOMBITs opgavevaretagelse i forhold til arbejdet med it-sikkerhed.

3.4 Kompetencer

I KOMBIT sikres det, at der er adgang til de fornødne It-sikkerhedsmæssige kompetencer og herunder, at det løbende prioriteres, at kompetencerne opdateres i takt med, at risikolandskabet og truslerne udvikler og ændrer sig. KOMBIT arbejder målrettet med at udbrede viden om KOMBITs arbejde med informations- og it-sikkerhed internt i KOMBIT, således at området bliver en del af det daglige arbejde for KOMBITs medarbejdere og, at kompetencerne dermed bliver bredt forankret i organisationen.

3.5 Dokumentation

I KOMBIT udarbejdes der løbende dokumentation for arbejdet med it-sikkerhed.

KOMBIT gennemfører en risikovurdering af alle it-systemer, hvor der er fokus på såvel det forretningsmæssige som det persondataretlige i forhold til hændelser, der kan resultere i enten tab af fortrolighed, integritet og/eller tilgængelighed, hvor risici, trusler og sårbarheder systematisk bliver vurderet i forhold til sandsynlighed og konsekvens.

KOMBITs ledelse deltager i og tager ansvar for gennemførelsen af risikovurderingerne, og stiller krav om, at risikovurderingerne gennemføres som minimum en gang årligt, eller når der sker ændringer, som kan få betydning for it-sikkerheden i systemet.

3.6 Styring og rapportering

I KOMBIT tager ledelsen arbejdet med it-sikkerhed alvorligt, og for at sikre den rette ledelsesmæssige prioritering og et stadigt skærpet fokus i hele organisationen i forhold til arbejdet med it-sikkerhed, er der etableret en styrings- og rapporteringsmodel, der giver ledelsen til nødvendige oplysninger til at kunne sikre og fastholde et sådant skærpet fokus i hele organisationen.

3.7 Intern audit

I KOMBIT gennemføres der i relevant omfang interne tekniske audits og kontroller af KOMBITs overholdelse af retningslinjer og procedurer i forhold til KOMBITs arbejde med it-sikkerhed. Resultaterne af

den interne audit analyseres og rapporteres til KOMBITs ledelse, der evaluerer resultaterne. Resultaterne af den interne audit indgår i KOMBITs årsplan for it-sikkerhedsområdet, der danner baggrund for det videre arbejde med håndtering af afvigelser i governance for it-sikkerhed samt løbende forbedringer af arbejdet.

3.8 Opfølgning

I KOMBIT gennemføres der, med henblik på sikringen af en løbende optimering, en opfølgning på arbejdet med it-sikkerhed i KOMBIT. Opfølgningen sker blandt andet med baggrund i oplysninger fra de systematiske rapporteringer til ledelsen og resultaterne af de interne audits, opfølgninger på de eksisterende retningslinjer, procedurer og planer. Opfølgningen sker via en årsplan, der udarbejdes for it-sikkerhedsområdet, der fungerer som en handlingsplan for det fremadrettede arbejde med It-sikkerheden i KOMBIT.

4 CHIEF INFORMATION SECURITY OFFICER (CISO)

KOMBIT har en Chief Information Security Manager (CISO).

Ledelsen af det løbende arbejde med it-sikkerhedspolitikken og tilhørende retningslinjer og procedurer er placeret hos KOMBITs CISO, som har det overordnede ansvar for, at dokumenterne er retvisende og kendte og anvendte i KOMBIT og hos KOMBITs interessenter.

Hvis du har spørgsmål til KOMBITs it-sikkerhedspolitik, kan du til enhver tid kontakte KOMBITs CISO.

Du kan finde kontaktoplysninger på KOMBITs CISO eller søge mere information på KOMBIT.dk.