SLAGELSE
KOMMUNE

Slagelse Kommune

Informationssikkerhedspolitik

1. Indledning

It –anvendelsen i Slagelse Kommune skal understøtte en effektiv og digital organisation, hvor digitalisering ses som en væsentligt parameter i forhold til kommunens fortsatte udvikling.

Udviklingen i lovgivningen og samfundet generelt, vil medføre at kommunen på flere områder og i større omfang benytter it, for at kunne servicere virksomheder og borgere.

Kommunens digitale strategier beskriver bl.a. de strategiske mål og handleplaner for it-anvendelsen, og giver samlet set den overordnede ramme for kommunens samlede digitale indsats. Det betyder, at kommunens opgaveløsning vil være understøttet af sammenhængende digitale løsninger, der tager udgangspunkt i borger- og virksomhedsservicering en således, at de digitale løsninger bliver borgernes/virksomhedernes naturlige 1. valg.

Informationssikkerhedspolitikken skal til enhver tid understøtte digitaliseringsstrategien samt it-anvendelsen og fastsætter derfor hovedprincipperne for informationssikkerheden - herunder ansvar og organisering for og af informationssikkerhedsarbejdet. Den samlede informationssikkerhedsbeskrivelse er uddybet i denne informationssikkerhedspolitik samt med en række informationssikkerhedsregler, –procedurer og en it-beredskabsplan, som løbende vurderes ud fra det til en hver tid værende globale og nationale teknologiske fundament samt gældende lovgivning.

2. Formål

Slagelse Kommunes informationssikkerhedspolitik beskriver vigtigheden af arbejdet med informationssikkerhed i kommunen og fastlægger vores ambitionsniveau herfor. Informationssikkerhedspolitikken indeholder derfor de overordnede sikkerhedsmålsætninger og danner grundlag for udformning af kommunens informationssikkerhedskatalog, der forstås som fællesbetegnelsen af informationssikkerhedspolitikken med de underliggende informationssikkerhedsregler og -procedurer samt it-beredskabsplanen.

Informationssikkerhedspolitikken er en vigtig del af kommunens informationssikkerhedskatalog og beskriver det ledelsesgodkendte niveau for sikkerhed. Dermed skal politikken ligeledes understøtte bevidstheden om informationssikkerhed i kommunens organisation og virke. De retningslinjer, der udformes for at understøtte informationssikkerhedspolitikkens hovedmålsætninger, skal sikre, at alle, der arbejder med kommunens informationer, forholder sig til informationssikkerhed i det daglige arbejde.

Kommunen ser ikke kun et tilstrækkeligt sikkerhedsniveau som et krav for at kunne overholde lov- og myndighedskrav, men også som et kvalitetselement for at kunne tilbyde en sikker service for borgerne og behandlerne.
Informationssikkerhed er derfor en nøgleværdi hos kommunen, og den vil være en naturlig del af vores aktiviteter.

3. Omfang

Informationssikkerhedspolitikken er gældende for alle uden undtagelse med en fysisk eller logisk adgang til Slagelse Kommunes systemer, data og informationer.

Informationssikkerhedspolitikken omfatter alle typer af informationer herunder lyd, billede og tekst og uanset, hvordan informationerne anvendes og opbevares.

Informationssikkerhedspolitikken gælder for alle sammenhæng, hvor der sker en anvendelse og bearbejdning af kommunens informationer – Rådhus og øvrige kommunale bygninger, institutioner, hjemmearbejdspladser, eksterne adgange, adgang via mobile enheder mv.

I det omfang Slagelse Kommune udliciterer it-driftsafviklingen til eksterne leverandører, skal det sikres, at serviceleverandørerne overholder informationssikkerhedspolitikken, regler og procedurer således, at sikkerhedsniveauet er i overensstemmelse med hermed.

4. Hovedmålsætninger og sikkerhedsniveau

Sikkerhedsmålsætning:

> *"Vi vil have et tilstrækkeligt informationssikkerhedsniveau for alle med relation til kommunen og for anvendelsen af it-ressourcer."*

Et tilstrækkeligt informationssikkerhedsniveau skal opnås igennem sikringsforanstaltninger, der sikrer:

- Fortrolighed, integritet, tilgængelighed af og uafviselighed i kommunens systemer og data i forhold til den risikovurdering, der er fastsat for det enkelte system/data.
- Beskyttelse af kommunens informationsaktiver, organisationens image og informationer/data i kommunens varetægt.

For at fastholde det tilstrækkelige sikkerhedsniveau i kommunen skal følgende overholdes:

- Der skal forefindes regler og procedurer, som sikrer, at informationssikkerhed er en integreret del af kommunens drift og daglige arbejde.
- Kommunen skal igennem kontrakt- og leverandørstyring sikre, at brugen af eksterne konsulenter, samarbejdspartnere og leverandører ikke udhuler kommunens informationssikkerhedsniveau.
- Kommunen skal sikre en struktureret og kontinuerlig forbedringsproces af arbejdet med informationssikkerhed.

Informationssikkerhedspolitikken følger principperne i den internationale standard for informationssikkerhed, ISO 27001:2017 (DK), og er udarbejdet i et samarbejde mellem kommunerne i Digitaliseringsforening Sjælland. Målet er en udstrakt harmonisering af medlemskommunernes ledelse og styring af informationssikkerheden med henblik på et tæt samarbejde på at opnå effektiviseringer og øget kvalitet på informationssikkerhedsområdet.

5. Ansvar

Sikkerhedsmålsætning:

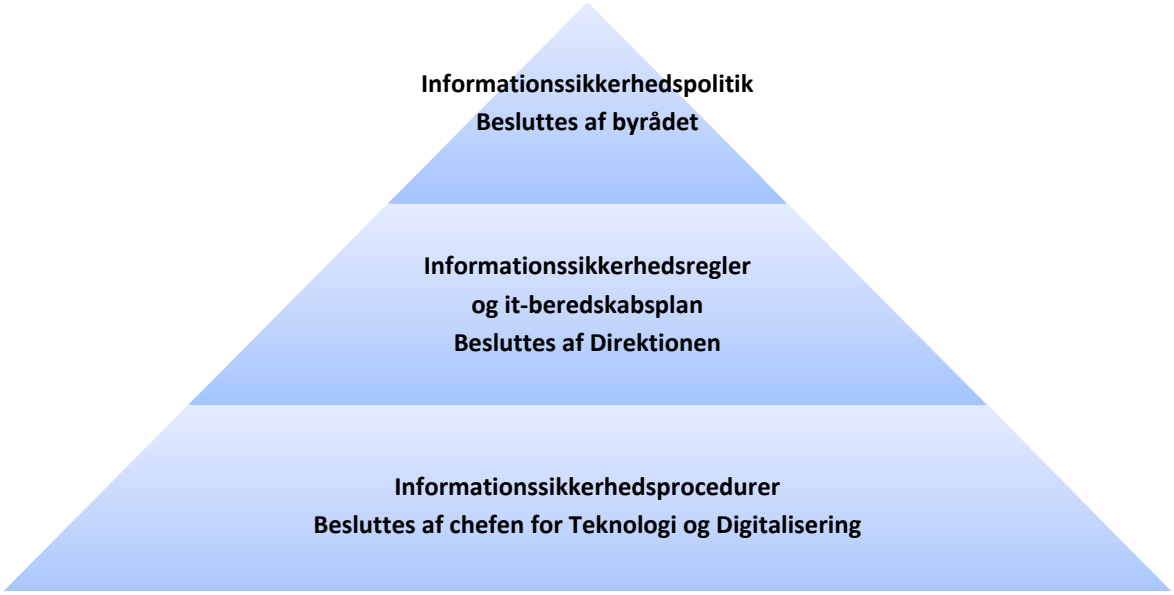
> *"Alle har ansvar for informationssikkerheden. De er bekendte med og efterlever kommunens informationssikkerhedspolitik, informationssikkerhedsregler og -procedurer."*

Planlægning, implementering og kontrol af informationssikkerhed defineres af kommunens ledelse.

Informationssikkerhedspolitikken revurderes mindst én gang hvert andet år eller i forbindelse med eventuelle situationer, der tilsiger det.

Alle skal kende informationssikkerhedspolitikken og er ansvarlige for at efterleve regler og procedurer for sikkerhed i det daglige arbejde.

Ledelsen på alle niveauer er ansvarlig for, at informationssikkerheden overholdes. Ledelsen skal ligeledes sikre, at den nødvendige viden og kompetence omkring informationssikkerhed kommunikeres til alle, der arbejder med kommunens informationer, og at der løbende arbejdes med holdninger, forståelse for og viden omkring informationssikkerhed.



6. Organisation

Byrådet har det overordnede ansvar for og godkender Slagelse Kommunes informationssikkerhedspolitik.

Direktionen har det overordnede ansvar for informationssikkerheden i organisationen, herunder at fastlægge sikkerhedsniveauet gennem den årlige godkendelse af ledelsesrapporten, som bl.a. skal indeholde en beskrivelse af, hvorvidt sikkerhedskravene i informationssikkerhedsstandarden ISO 27001 efterleves. Dette sker ved udfærdigelse af ISO 27001 kontrolmålsdokument "Statement of Applicability (SoA)".
Direktionen træffer de overordnede beslutninger vedrørende informationssikkerhed og forholder sig til afledte økonomiske, ressourcemæssige og organisatoriske konsekvenser.
Direktionen har det overordnede ansvar for og godkender Slagelse Kommunes informationssikkerhedsregler.

Kommunaldirektøren er den øverste informationssikkerhedsansvarlige og er ansvarlig for at arbejde med informationssikkerhed på et strategisk niveau, således at informationssikkerhedsmæssige overvejelser inddrages i alle væsentlige beslutninger.
Det daglige informationssikkerhedsarbejde er uddelegeret til informationssikkerhedskoordinatoren.

Informationssikkerhedsudvalget er en tværfaglig gruppe med et direktionsmedlem/stabschef som formand. Udvalget medvirker til, at kommunen opfylder sine forpligtigelser på informationssikkerhedsområdet og understøtter, at informationssikkerheden realiseres og implementeres i organisationen. Udvalget behandler og rådgiver om emner vedrørende informationssikkerhedspolitik og informationssikkerhedsreglerne og indstiller til videre behandling/godkendelse i direktionen.
Informationssikkerhedskoordinatoren er sekretær for udvalget. DPO rådgiver og støtter udvalget i forvaltningen af interne politikker i forhold til beskyttelse af personoplysninger.

Systemejere/risikoejere har ansvar for informationssikkerheden, for det/de systemer de "ejer", herunder ansvaret for at der bliver udarbejdet (detaljerede) procedurer, instrukser og tjeklister inden for rammerne af de sikkerhedsniveauer direktionen har fastlagt. Endvidere er det systemejernes ansvar at føre løbende kontrol med overholdelsen af regler og procedurer samt at sikre vedligeholdelse af overblik over system(er), herunder processer, interessenter, aktiver, kontrakter etc. De konkrete opgaver kan uddelegeres til en medarbejder, der udpeges som systemansvarlig og/eller dataejer.

Dataejer har dispositionsret til data og ansvar for behandling af data og skal skabe sig et overblik over, hvilke forretningsprocesser data understøtter.

Centercheferne er ansvarlige for at informationssikkerheden overholdes i centret.
Centercheferne udpeger systemansvarlige/risikoansvarlige i deres centre og fører tilsyn med at politik, regler og procedurer overholdes. Det er ligeledes centerchefens ansvar at sikre medarbejdernes kendskab til gældende politik, regler og procedurer.

Informationssikkerhedskoordinatoren er organisationens daglige informationssikkerhedsleder og sekretær for informationssikkerhedsudvalget.
Informationssikkerhedskoordinatoren er ansvarlig for implementering og vedligeholdelse af et Information Security Management System (ISMS) i kommunen og er ansvarlig for opfølgning på sikkerhedshændelser.

Databeskyttelsesrådgiver ("Data Protection Officer" (DPO) skal overvåge, at organisationen overholder både lovgivningen og interne politikker i forhold til beskyttelse af følsomme persondata. DPO'en involveres i alle spørgsmål vedrørende databeskyttelse og fungerer desuden som kontaktperson for registrerede og databeskyttelsesmyndighederne.

Ledere er ansvarlige for operativ implementering og løbende kontrol med overholdelsen af informationssikkerhedspolitikken, -regler, -procedurer mv. De bidrager i øvrigt til at højne opmærksomheden omkring informationssikkerhed, og fungerer som daglig sparringspartner for medarbejderne i forhold til efterlevelse af sikkerhedsforanstaltningerne.

Medarbejdere generelt, har ansvaret for at kende og overholde sikkerheden omkring informationsanvendelse ved overholdelse af informationssikkerhedspolitikken, -regler og relaterede procedurer samt at påpege eventuelle mangler eller uhensigtsmæssigheder.

7. Opbygning af informationssikkerhedskataloget

Informationssikkerhedskataloget består af denne informationssikkerhedspolitik, som uddybes i nogle informationssikkerhedsregler og -procedurer samt en it-beredskabsplan.

Informationssikkerhedspolitikken
Den, af Byrådet fastlagte, overordnede ramme for informationssikkerhed i kommunen som lægges til grund for informationssikkerhedsreglerne.

Informationssikkerhedsregler
Overordnede regler for informationssikkerhedsarbejdet som behandles af informationssikkerhedsudvalget og godkendes af direktionen. Reglerne skal fastlægge rammerne for udarbejdelse af de konkrete informationssikkerhedsprocedurer inden for 20 områder (baseret på ISO 27001 standarden), som beskriver:

- Overordnede retningslinjer for informationssikkerhed
- Risikovurdering og håndtering
- Organisering af informationssikkerhed
- Personalesikkerhed
- Styring af aktiver
- Klassifikation af information
- Mediehåndtering
- Adgangsstyring
- Kryptografi
- Fysisk sikring og miljøsikring
- Driftssikkerhed
- Backup
- Logning og overvågning
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af sikkerhedsbrud
- Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
- Overensstemmelse med lovbestemte krav
- Gennemgang af informationssikkerhed

Informationssikkerhedsprocedurer
Operationelle procedurer som konkret beskriver de enkelte informationssikkerhedselementer set ud fra koncernens, ledelsens og den enkelte medarbejders anvendelse. Informationssikkerhedsprocedurer besluttes af chefen for Center for Teknologi og Digitalisering og skal være i overensstemmelse med de af informationssikkerhedsudvalget udstukne informationssikkerhedsregler.

Eksempler på informationssikkerhedsprocedurer kunne f.eks. være:

- Autorisationsprocedure, herunder f. eks. anvendelsen af 2-faktor autentifikation
- Backup procedure
- Passwordkompleksitet
- Logning
- Firewall
- Fysisk sikkerhed for datacentre mm.
- Ansvar for system-/risikoejere

It-beredskabsplan
Plan som konkret beskriver de enkelte it-beredskabsforanstaltninger, som skal gennemføres for at sikre en hurtig ageren i tilfælde af en nødsituation samt prioriteringer ved behov for en reetablering. It-beredskabsplanen skal udarbejdes i respekt til kommunens samlede beredskabsplan, men skal kunne fungere selvstændigt.
It-beredskabsplanen skal koordineres af informationssikkerhedsudvalget og godkendes af direktionen.

8. Risikovurdering og klassifikation

Risikovurdering
Informationssikkerheden i kommunen skal være på et niveau, der tilgodeser lov- og myndighedskrav, kontraktlige forpligtelser samt forpligtelser overfor de aktører, der skal anvende kommunens informationsaktiver.
Kommunen ønsker ikke at sikre sig for enhver pris, men ønsker at være bevidst om enhver risiko og forholde sig tilfredsstillende til disse, hvormed tilstrækkeligt sikkerhedsniveau etableres.

Ledelsen deltager altid aktivt i risikovurderinger og er ansvarlige for at vurdere trusler, konsekvenser og risici af informationssystemer og andre relevante områder.

Risikovurderingen opdateres mindst én gang årligt, samt ved eventuelle større ændringer i opgaver, leverandører, informationssystemer eller anvendelsen deraf.

Klassifikation
Kommunens informationer skal klassificeres efter lovmæssige krav, værdi og efter, hvor kritisk og følsom informationen er i forhold til uautoriseret offentliggørelse eller ændring.

Sikkerhedsforanstaltninger
Baseret på klassifikationen samt risikovurderingen etableres relevante sikkerhedsforanstaltninger, der sikrer kommunen et af ledelsen accepteret risikoniveau.

9. Privat brug af kommunens netværk

Kommunens digitale enheder og internetadgang må i begrænset omfang anvendes til private formål såfremt, at informationssikkerhedspolitikken i øvrigt overholdes, og arbejdsrelateret brug ikke generes på nogen måde.
Der må ikke installeres programmer eller services til privat brug.
Ved brug af internet skal man være opmærksom på, at hjemmesiderne bruger cookies, som sætter spor, der kan føres tilbage til Slagelse Kommune. Man skal derfor altid opfatte sig som en ambassadør, udvise omhu ved benyttelsen af internet og må ikke anvende internettet imod kommunens interesse. Opmærksomheden skal især henledes på følgende forhold:

- Slagelse Kommune ønsker ikke at blive identificeret med, hvad der generelt opfattes som stødende eller uetiske emner, der ikke lever op til kommunens Visioner og Værdigrundlag.
- Der må ikke søges efter – eller anvende – websteder, som indeholder materiale vedr. hacking, terrororganisationer, børneporno og andre beslægtede steder.
- Internettet må ikke bruges til aktiviteter, herunder download, publicering eller udbredelse af materiale, som er forbudt ifølge dansk lovgivning, herunder regler og love om ophavsret.

10. Overtrædelse af informationssikkerhedspolitikken

Alle i kommunen er forpligtet til at efterleve den til enhver tid gældende informationssikkerhedspolitik med tilhørende regler, procedurer og relaterede bilag. En overtrædelse kan, efter omstændighederne, medføre sanktioner, herunder ansættelsesretslige konsekvenser og/eller politianmeldelse.

Hvis en medarbejder er vidende om, at kommunens informationssikkerhedspolitik overtrædes eller kompromitteres, skal det straks meddeles til ledelsen.

11. Afvigelser

Hvis der opstår situationer, hvor kravene i informationssikkerhedskataloget ikke kan efterleves, skal der skriftligt anmodes om dispensation hos chefen for Center for Teknologi og Digitalisering. Eventuelle afvigelser fra kravene skal dokumenteres, og der skal indføres alternative sikringsforanstaltninger og en udløbsdato.

12. Opfølgning

Kommunen måler, vurderer og følger op på informationssikkerhedsområdet på følgende områder:

- Det samlede informationssikkerhedskatalog skal i tilfælde af væsentlige ændringer og mindst én gang hvert andet året vurderes og opdateres for at sikre dets fortsatte egnethed, tilstrækkelighed og effektivitet.
- Hændelser inden for informationssikkerhedsområdet bliver registreret løbende, og der skal løbende følges op på relevante hændelser.
- Der skal mindst én gang om året - eller ved større tekniske eller større organisatoriske ændringer - gennemføres en risikovurdering således, at kommunens ledelse kan holdes orienteret om det aktuelle risikobillede.
- Der skal årligt gennemføres en uafhængig tredjepartsrevision og evaluering af informationssikkerheden.
- En gang årligt, primo året, skal der udarbejdes en ledelsesrapport til direktionen, der giver en status for informationssikkerhedsarbejdet. Rapporten skal bl.a. indeholde et Statement of Applicability (SoA) jf. ISO 27001 samt oversigt over årets informationssikkerhedshændelser – herunder en beskrivelse af de konkrete tiltag, der er foretaget.

13. Udarbejdelse og ikrafttrædelse

Håndtering af ændringer i sikkerhedsdokumentationen foretages på følgende måde:

- Informationssikkerhedspolitikken: Godkendes af byrådet.
- Informationssikkerhedsregler: Godkendes af direktionen.
- Informationssikkerhedsprocedurer: Godkendes af chefen for Teknologi og Digitalisering.
- It-beredskabsplanen: Godkendes af direktionen.
- Operationelle procedurer: Kan foretages af den lokale ledelse.

Informationssikkerhedspolitikken er godkendt i Byrådet den XX. marts 2018 og erstatter den tidligere it-sikkerhedspolitik godkendt i Byrådet den 24. februar 2014.

Informationssikkerhedspolitikken træder i kraft ved godkendelsen i Byrådet.