Slagelse Kommune

Informationssikkerhedspolitik

Politikken er senest opdateret den 21/4 2022

Slagelse Kommune, Rådhuspladsen 11, 4200 Slagelse
Tlf: 58 57 36 00, e-mail slagelse@slagelse.dk, web: www.slagelse.dk

1. Indledning

It –anvendelsen i Slagelse Kommune skal understøtte en effektiv organisation, hvor digitalisering ses som en væsentlig 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.

De fælles offentlige 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 digitaliseringsstrategierne 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 informationssikkerhedshåndbog, der forstås som fællesbetegnelsen for informationssikkerhedspolitikken, informationssikkerhedsreglerne og informationssikkerhedsprocedurerne samt it-beredskabsplanen.

Informationssikkerhedspolitikken er en vigtig del af kommunens informationssikkerhedshåndbog 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.
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 – digitalt eller fysisk - herunder lyd, billede og tekst og uanset, hvordan informationerne anvendes og opbevares.

Informationssikkerhedspolitikken gælder i 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 systemejer sikre, 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 omdømme og informationer/data i kommunens varetægt.
- Sikring af databeskyttelse for fysiske personer, blandt andet ved efterlevelse af databeskyttelseslovgivningen – herunder udpegning af en Databeskyttelsesrådgiver og udarbejdelse af en privatlivspolitik.

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 samarbejdspartnere, leverandører og eksterne konsulenter 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 ansatte har ansvar for informationssikkerheden. De er bekendte med og efterlever kommunens informationssikkerhedspolitik, informationssikkerhedsregler og -procedurer."*

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

Kommunaldirektøren er kommunens øverste informationssikkerhedsansvarlige. Kommunaldirektøren er ansvarlig for at arbejde med informationssikkerhed på et strategisk niveau, således at informationssikkerhedsmæssige overvejelser inddrages i alle væsentlige beslutninger. Ledere og medarbejdere er ansvarlige for at efterleve retningslinjer og procedurer for sikkerhed i det daglige arbejde.

Planlægning, implementering og kontrol af informationssikkerhed er defineret af Kommunens ledelse. Informationssikkerhedskoordinatoren er ansvarlig for implementering og vedligeholdelse af informationssikkerhedssystemet i Kommunen og er ansvarlig for opfølgning på sikkerhedshændelser.

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. Informationssikkerhedshåndbogen

Informationssikkerhedspolitikken indeholder de overordnede sikkerhedsmålsætninger og rammer for informationssikkerhed i kommunen.
Informationssikkerhedspolitikken uddybes i Informationssikkerhedsregler, Informations-sikkerhedsprocedurer og Informationssikkerhedsvejledninger. Tilsammen udgør disse sammen med it-beredskabsplanen Kommunens informationssikkerhedshåndbog.

Informationssikkerhedsregler
Overordnede regler for informationssikkerhedsarbejdet som behandles af informationssikker-hedsudvalget og godkendes af formanden for Informationssikkerhedsudvalget. Reglerne skal fastlægge rammerne for udarbejdelse af de konkrete informationssikkerhedsprocedurer og -vejledninger baseret på informationssikkerhedsstandarden ISO 27001.

Informationssikkerhedsprocedurer
Operationelle procedurer gældende for hele kommunen eller for et chefområde, som konkret beskriver de enkelte informationssikkerhedselementer set ud fra koncernens, ledelsens og den enkelte medarbejders anvendelse. Informationssikkerhedsprocedurer dækkende hele kommunen besluttes og godkendes af formanden for Informationssikkerhedsudvalget. Procedurer for et enkelt chefområde besluttes og godkendes af den enkelte chef. Alle procedurer skal være i overensstemmelse med de udstukne informationssikkerhedsregler.

Informationssikkerhedsvejledninger
Operationelle vejledninger gældende for den enkelte leders område, som konkret beskriver de enkelte informationssikkerhedselementer set ud fra lederens og den enkelte medarbejders anvendelse. Informationssikkerhedsvejledninger besluttes af den enkelte leder, og skal være i overensstemmelse med de udstukne informationssikkerhedsregler og informationssikkerhedsprocedurer.

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 formanden for Informationssikkerhedsudvalget.

7. 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.

Kommunens overordnede risikovurdering opdateres mindst én gang årligt, samt ved eventuelle større ændringer i det aktuelle risikobillede, 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.

8. Fysisk adgang, TV-overvågning, logning og adgang til data

For at få adgang til kommunens administrative bygninger eller til bygninger og/eller områder med særlige beskyttelsesværdigt it-udstyr skal der anvendes adgangskort.

Slagelse Kommune registrerer (logger) medarbejdernes aktiviteter, når de anvender kommunens it-systemer og services – herunder medarbejdernes anvendelse af deres arbejdstelefoner, iPads og lignende. Endvidere logges brugen af adgangskort. Dette sker af drifts- og sikkerhedsmæssige årsager samt for at kontrollere brug/misbrug.
I forbindelse med medarbejderes anvendelse af kommunens køretøjer kan der være GPS overvågning af disse, som også logges.

Bygninger og områder bliver flere steder videoovervåget med henblik på at forebygge kriminalitet samt give bedre sikkerhed for medarbejdere og borgere.

Slagelse Kommune forbeholder sig ret til at tilgå data og e-mails hos medarbejdere, hvis det sker af drifts-eller sikkerhedshensyn. Ligeledes vil en leder af arbejdsmæssige hensyn inden for sit område kunne tillade, at en anden medarbejder midlertidigt tildeles adgang til en medarbejders data og e-mails.
Da kommunen jf. pkt. 12 i begrænset omfang tillader brug af mail til privat brug, skal en sådan brug fremgå tydeligt ved at skrive "PRIVAT" i emnefeltet på mailen, hvorefter disse mails ikke vil blive tilgået, med mindre drifts- eller sikkerhedshensyn gør det nødvendigt.
En leder skal ved tildeling af midlertidig adgang til en anden medarbejders e-mails meddele den medarbejder, som tildeles adgang, at vedkommende ikke må åbne mails mærket med "PRIVAT".

9. Distancearbejde

Udviklingen i dag betyder, at der er blevet et behov for at kunne arbejde digitalt fra distancen. Kommunen ser dette som en mulighed for en øget fleksibilitet, men det øger samtidigt risikoen for læk af interne informationer, uautoriseret adgang til interne informationer samt øget risiko for kompromittering. Dette kræver derfor, at tilgang til disse informationer skal beskyttes bedst muligt. Derfor skal al distanceadgang ske under anvendelse af en multifaktor autorisation (MFA) ligesom, at opkobling til kommunens netværk skal ske under anvendelse af en VPN-forbindelse med mindre særlige omstændigheder undtagelsesvis skulle hindre dette.
For så vidt angår medbringelse af kommunens udstyr i forbindelse med distancearbejde eller til rejser må det kun ske, såfremt det pågældende udstyr er krypteret – det gælder både pc'er, laptops, USB-Sticks eller andet lagermedie.
Når der arbejdes fra en distancearbejdsplads, skal man også huske den fysiske sikkerhed, både med hensyn til udstyret, men også i forhold til eventuelle fysiske dokumenter og lignende samt muligheden for eventuel overhørelse af et videomøde.

10. Uddannelse

For at sikre at kommunens medarbejdere har det nødvendige kendskab til databeskyttelse, skal ledelsen på alle niveauer sørge for, at medarbejdere, der har permanent eller regelmæssig adgang til personoplysninger, har den nødvendige viden og kompetence omkring databeskyttelse. Det skal sikres, at denne viden vedligeholdes og opdateres med jævne mellemrum.

11. Anvendelse af privat udstyr

Privat udstyr må ikke anvendes til behandling eller opbevaring af kommunens data. Hvis der anvendes privat udstyr i anden sammenhæng fx til at tilgå kommunens Outlook Web Acces (OWA) skal man sørge for, at det udstyr, der anvendes, er godt beskyttet blandt andet med opdateret operativsystem, antivirus osv.

12. Privat brug af kommunens digitale enheder og 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.

13. 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.

14. Afvigelser

Hvis der opstår situationer, hvor kravene i informationssikkerhedspolitikken og de underliggende Informationssikkerhedsregler ikke kan efterleves, skal der skriftligt anmodes om dispensation hos formanden for Informationssikkerhedsudvalget. Eventuelle afvigelser fra kravene skal dokumenteres, og der skal indføres alternative sikringsforanstaltninger og en udløbsdato.

15. Opfølgning

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

- Den samlede informationssikkerhedspolitik 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 kommunens øverste ledelse og økonomiudvalget, der giver en status for informationssikkerheds-arbejdet. 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.
- Databeskyttelsesrådgiveren skal årligt gennemføre et tilsyn med kommunens efterlevelse af databeskyttelseslovgivningen og fremlægge resultatet for kommunens øverste ledelse og økonomiudvalget.

16. Udarbejdelse og ikrafttrædelse

Håndtering af ændringer i sikkerhedsdokumentationen foretages på følgende måde:

- Informationssikkerhedspolitikken: Godkendes af byrådet.
- Informationssikkerhedsregler: Godkendes af formanden for Informations-sikkerhedsudvalget.
- Informationssikkerhedsprocedurer: Godkendes af formanden for Informations-sikkerhedsudvalget.
- It-beredskabsplanen: Godkendes af formanden for Informationssikkerhedsudvalget.
- Operationelle vejledninger: Kan foretages af den lokale ledelse.

Informationssikkerhedspolitikken er godkendt i Byrådet den dd. mmmm 2022 og erstatter den tidligere it-sikkerhedspolitik godkendt i Byrådet den 28. maj 2018.

Informationssikkerhedspolitikken træder i kraft ved godkendelsen i Byrådet.