LYNGBY-TAARBÆK KOMMUNE

Informations sikkerhedspolitik

for Lyngby-Taarbæk Kommune

2019-20

Informationssikkerhedspolitik for Lyngby-Taarbæk Kommune 2019-20

Lyngby-Taarbæk Kommune

Version 1.3, oktober 2019

Omslag: Jan Østergaard Rasmussen

Format: PDF-1.7

Publikationen kan hentes på kommunens intranet og hjemmeside

Indhold

1 Formål 4
2 Hovedmålsætninger og sikkerhedsniveau 4
3 Omfang 5
4 Organisation og ansvar 5
4.1 Kommunalbestyrelsen og Direktionen 5
4.2 Koncernchefgruppen 5
4.3 Digitalt lederforum og ad hoc grupper 5
4.4 Data- og systemejere 6
4.5 Medarbejdere 6
4.6 Tredje part (Eksterne aktører) 7
4.7 Uafhængighed af nøglepersoner 7
4.8 Funktionsadskillelse 7
5 Brugeradfærd 7
5.1 Ansættelsesforholdet 8
5.2 Før og efter ansættelse 8
6 Fysisk sikkerhed 9
6.1 Sikre områder 9
6.2 Fysisk adgangskontrol 9
6.3 Beskyttelse af udstyr 9
7 Styring af netværk og drift 9
7.1 Eksterne serviceleverandører 9
7.2 Styring af driftsmiljø 10
7.3 Sikkerhedskopiering 10
7.4 Netværkssikkerhed 10
7.4.1 Trådløse netværk 10
7.5 Logning og overvågning 11
7.6 Adgangsstyring 11
7.6.1 Administration af brugeradgang 11
7.7 Mobilt udstyr og fjernarbejdspladser 11
7.8 Cyber Security 11
8 Anskaffelse, udvikling og vedligeholdelse af it-systemer 11
8.1 Sikkerhed i udviklingsprocesser 12
9 Hændelsesstyring 12
10 Beredskabsstyring 12

10.1 IT-beredskabsplan 12
11 Afvigelser 13
12 Overtrædelse af politikken 13
13 Outsourcing 13
14 Compliance med lovgivning 13
14.1 Persondata og EU Regulering 13
15 Godkendelse af politikken 13

1 Formål

Informationssikkerhed er afgørende for overholdelse af Databeskyttelsesforordningen (GDPR), som trådte i kraft 25. maj 2018. Staten og KL fremhæver informationssikkerhed med selvstændige kapitler i de seneste digitaliseringsstrategier og understreger vigtigheden af dette arbejde.

Informationssikkerhedspolitikken for Lyngby-Taarbæk Kommune indeholder en beskrivelse af arbejdet med informationssikkerhed i kommunen. Sikkerhedspolitikken indeholder de overordnede målsætninger, og den er udgangspunkt for udformningen af tilhørende forretningsprocedurer, områdespecifikke politikker, retningslinjer og procedurer.

Sikkerhedspolitikken beskriver det ledelsesgodkendte niveau for sikkerhed. De forretningsgange/procedurer, der udformes for at understøtte sikkerhedspolitikkens målsætninger, skal sikre, at alle medarbejdere arbejder med og forholder sig til informationssikkerhed i det daglige arbejde.

Lyngby-Taarbæk Kommunes høje og balancerede sikkerhedsniveau skal sikre kvalitet, innovation og troværdighed for medarbejdere, samarbejdspartnere og borgere.

2 Hovedmålsætninger og sikkerhedsniveau

Lyngby-Taarbæk Kommune ønsker et balanceret informationssikkerhedsniveau for alle ansatte, samarbejdspartnere og borgere. Et informationssikkerhedsniveau (med en risikobaseret tilgang), som beskytter Lyngby-Taarbæk Kommunes vigtige informationer, herunder specielt persondata, tilstrækkeligt uden at skabe et system, som begrænser borgernes rettigheder og service eller medarbejdernes fleksibilitet, kreativitet og arbejdsglæde.

Løbende risikovurderinger sikrer balanceret sikkerhed, som dækker det, der er nødvendigt.

Et tilstrækkeligt og balanceret informationssikkerhedsniveau opnås gennem sikringsforanstaltninger, der sikrer:

- fortrolighed, integritet, og tilgængelighed i Lyngby-Taarbæk Kommunes systemer og data i forhold til den gældende risikovurdering, der er fastsat for det enkelte informationssystem,
- beskyttelse af Lyngby-Taarbæk Kommunes borgere, aktiver, viden, informationer i Lyngby-Taarbæk Kommunes varetægt og image, inklusiv overholdelse af lov- og myndighedskrav.

For at fastholde det valgte sikkerhedsniveau skal Lyngby-Taarbæk Kommune sikre medarbejdernes kompetencer og løbende følge op, vedligeholde og optimere politikken og de dertilhørende procedurer.

Målet er at sikre en struktureret og kontinuerlig forbedringsproces.

3 Omfang

Informationssikkerhedspolitikkens omfang:

- politikken gælder for alle ansatte i Lyngby-Taarbæk Kommune uanset ansættelsesform,
- politikken gælder for alle systemer og alle informationer og data i Lyngby-Taarbæk Kommunes besiddelse,
- politikken skal overholdes af alle Lyngby-Taarbæk Kommunes leverandører, eksterne konsulenter, servicemedarbejdere, samarbejdspartnere og andre, som har fysisk eller logisk adgang til kommunens systemer og data.

4 Organisation og ansvar

4.1 Kommunalbestyrelsen og Direktionen

Lyngby-Taarbæk Kommunes Kommunalbestyrelse har det overordnede ansvar for informationssikkerheden i kommunen. Kommunalbestyrelsen skal godkende informationssikkerhedspolitikken herunder de overordnede retningslinjer for arbejdet med informationssikkerheden. Dermed har Kommunalbestyrelsen også fastsat det accepterede niveau for risiko.

Direktionen vil træffe de overordnede beslutninger indenfor Kommunalbestyrelsens besluttede ramme og godkende den årlige risikovurdering for informationssikkerhed. Kommunaldirektøren har ansvaret for, at relevant information og rapportering bliver præsenteret for Kommunalbestyrelsen.

4.2 Koncernchefgruppen

Koncernchefgruppen har ansvaret for, at der opnås det sikkerhedsniveau, som er besluttet af Kommunalbestyrelsen.

Koncernchefgruppen vil stå for at uddelegere ansvar, opgaver og beslutninger samt føre overordnet tilsyn med, at informationssikkerhedsarbejdet bliver udført som aftalt.

4.3 Digitalt lederforum og ad hoc grupper

Koordinering og udførelse af de overordnede opgaver for informationssikkerhed vil blive foretaget i det digitale lederforum med støtte fra forskellige sikkerhedsgrupper, som arbejder med specifikke områder af informationssikkerheden.

Disse grupper er:

- Koncernchefgruppen
- Digitalt lederforum
- Ad hoc grupper

Digitalt lederforum og Koncernchefgruppen er ansvarlige for implementeringen af informationssikkerhed efter de gældende retningslinjer. De skal koordinere og følge op på sikkerhedsrelaterede aktiviteter, f.eks. kommunens awareness-program og risikovurderinger samt rapportere alle relevante informationer tilbage til Koncernchefgruppen.

De enkelte centre/afdelinger har ansvar for, at informationssikkerhedspolitikken bliver implementeret på deres specifikke områder, så processer, kontroller og dokumentation etableres efter de besluttede retningslinjer.

Informationssikkerhedspolitikken for Lyngby-Taarbæk Kommune skal regelmæssigt – mindst én gang årligt eller ved større organisatoriske ændringer – revurderes.

Det digitale lederforum, sikkerhedsgrupperne og centre/afdelinger skal uddybe informationssikkerhedspolitikken i procedurer, arbejdsbeskrivelser og retningslinjer, der understøtter:

- ansvarsplacering, herunder placering af ejerskab for informationsprocesser og ressourcer,
- funktionsadskillelse med tilhørende overvågning,
- monitorering af faktisk informationssikkerhedsniveau samt iværksættelse af nødvendige korrigerende handlinger,
- sikkerhedsmæssig klassificering og prioritering af systemer og data,
- dokumentering af systemer (både basis- og brugersystemer) og konfiguration (hardware) samt ændringer hertil,
- sikkerhedskopiering af systemer og data, herunder opbevaring af sikkerhedskopierne,
- allokering af informationssikkerhedsressourcer,
- systemudvikling, konfigurering og vedligeholdelse samt afprøvning af nye og ændrede systemer sker betryggende,
- tests og anden kvalitetssikring,
- ændringshåndtering og problemstyring,
- adgangskontrol til systemer og data,
- fysisk sikkerhed, herunder fysisk adgangskontrol,
- beredskabsplanlægning.

4.4 Data- og systemejere

De enkelte data- og systemejere er ansvarlige for systemernes brugerautorisationer og informationssikkerhed. Data- og systemejerne foretager endvidere delegering af opgaver og ansvar vedrørende de enkelte funktionsområder, herunder også vejledning og instruktion af medarbejdere.

4.5 Medarbejdere

Enhver medarbejder i Lyngby-Taarbæk Kommune har et medansvar for informationssikkerheden. Medarbejderne vil blive holdt informeret om sikkerhedsmæssige problemer og om tiltag af betydning for at kunne leve op til dette ansvar.

Alle medarbejdere har således et ansvar for at beskytte Lyngby-Taarbæk Kommunes informationer mod uautoriseret adgang, misbrug, ændring, ødelæggelse eller tyveri. Alle medarbejdere er ansvarlige for at rapportere enhver form for sikkerhedsbrist eller potentielle brister via medarbejderservice.

4.6 Tredje part (Eksterne aktører)

Tredje part, som får adgang til informationer, data og systemer hos Lyngby-Taarbæk Kommune, skal efterkomme informationssikkerhedspolitikkens krav til håndtering af data, informationer og brugen af it-systemer. De enkelte centre/afdelinger, som laver kontrakten med tredje part, har ansvaret for at informere tredje part om deres ansvar i forbindelse med informationssikkerheden. Tredje part er også ansvarlig for at rapportere enhver form for sikkerhedsbrist eller potentielle brister til deres ansvarlige kontaktperson i kommunen.

4.7 Uafhængighed af nøglepersoner

Der tilstræbes uafhængighed af enkeltpersoner gennem videndeling og etablering af personbackup, hvor dette er muligt. Hvor videndeling ressourcemæssigt ikke er muligt, skal der etableres relevante kompenserende kontroller, der gør det muligt at udføre opgaverne og sikre den nødvendige dokumentation herfor.

4.8 Funktionsadskillelse

Funktionsadskillelse er det bærende kontrolprincip på både person- og organisationsniveau. Hvor det ikke er praktisk muligt, kompenseres med andre sikkerhedsforanstaltninger, der udmøntes i procedurer/retningslinjer/regler for systemadministration.

Funktionsadskillelse er en grundlæggende forudsætning for forebyggelse og begrænsning af konsekvenser hidrørende fra fejl, uheld og bevidst kritisable handlinger, f.eks.:

- tildeling og godkendelse af brugerrettigheder,
- godkendelse og betaling af regninger,

forårsaget af en eller flere personer. Grundlæggende skal godkendelse og igangsættelse af alle vigtige processer holdes adskilt.

Funktionsadskillelsen skal ske under hensyn til risikovurdering og it-organisationens størrelse.

5 Brugeradfærd

Alle medarbejdere i Lyngby-Taarbæk Kommune skal i det daglige arbejde fokusere på kommunens overordnede målsætninger og herunder informationssikkerhed og persondatareglerne som en integreret del.

Opretholdelse af det ønskede sikkerhedsniveau er afhængig af, at hele organisationen tager ansvar for informationssikkerheden. Alle ansatte skal være bekendt med informationssikkerhedspolitikken og gældende procedurer og vejledninger for ønsket adfærd. Områdespecifikke politikker og retningslinjer er tilgængelige for alle medarbejdere og indeholder detaljeret information om, hvordan medarbejderne skal forholde sig i relation til informationssikkerhed. Følgende punkter er retningsgivende for brugeradfærd i Lyngby-Taarbæk Kommune og vil blive understøttet af yderligere procedurer og vejledninger:

- Fortrolig intern kommunikation og persondata skal i alle tilfælde behandles fortroligt,
- fortrolige informationer (f.eks. personfølsomme data etc.) må kun udveksles via 'Sikker e-mail', 'Send Digitalt' og 'Digital Post' (f.eks. e-Boks, Borger.dk og Virk.dk),
- fortrolige informationer (f.eks. it-sårbarhedsregister og persondata etc.) må ikke udveksles på private enheder, via private applikationer og via private e-mailadresser,
- der anvendes personligt login og password. Password skal skiftes med 60 dages mellemrum,
- datamedier med vigtige informationer og data skal beskyttes mod uautoriseret adgang,
- mobilt udstyr skal beskyttes og opbevares, så uvedkommende ikke kan få adgang til information og data, f.eks. skal der være skærmlås med pin kode,
- der må kun anvendes godkendte it-systemer på Lyngby-Taarbæk Kommunes udstyr,
- arbejdsmail kan anvendes til privat kommunikation, så længe dette ikke går ud over de primære arbejdsopgaver og sikkerheden,
- medarbejdere i Lyngby-Taarbæk Kommune kan i begrænset omfang anvende internettet og sociale medier i arbejdstiden, så længe dette ikke går ud over de primære arbejdsopgaver og sikkerheden,
- det er ikke tilladt at publicere Lyngby-Taarbæk Kommunes interne materiale på internettet og sociale medier,
- det er kun tilladt for Lyngby-Taarbæk Kommunes medarbejdere at uploade internt materiale på godkendte cloud storage tjenester som f.eks. OneDrive og SharePoint (og ikke f.eks. Dropbox, iCloud, Google Drev etc.),
- tilgang til eller distribution af stof fra hjemmesider med racistisk, uetisk eller pornografisk indhold er ikke acceptabelt,
- alle tilslutninger af digitale enheder på Lyngby-Taarbæk Kommunes netværk skal godkendes af IT-afdelingen (Dette gælder ikke LTKAIR public Wi-Fi),
- medarbejderne skal holde sig opdateret med Lyngby-Taarbæk Kommunes awarenes kampagner på intranettet og offentlig tilgængelig viden, der oplyser om, hvordan man beskytter sig mod f.eks. phishing angreb.

5.1 Ansættelsesforholdet

Alle medarbejdere har et medansvar for at opretholde det ønskede sikkerhedsniveau. For at kunne leve op til dette medansvar skal den enkelte medarbejder:

- have et generelt kendskab til informationssikkerhed,
- kende eget ansvar for informationssikkerheden,
- beskytte egne personlige adgangskoder,
- passe på kommunens it-udstyr,
- deltage aktivt i rettelse af fejl, løsning af problemer og forbedringer af sikkerheden,
- rapportere hændelser, der kan indikere brud på sikkerheden,
- deltage aktivt i awareness kampagner og undervisning.

5.2 Før og efter ansættelse

Der skal være procedurer, der sikrer ansættelse af kompetente og sikkerhedsmæssigt egnede medarbejdere. Medarbejdere, der skal arbejde med fortrolige oplysninger, skal fremlægge straffeattest inden ansættelse. Det skal sikres, at der foreligger

ansættelseskontrakter på alle ansatte, hvor ansvar for informationssikkerheden er beskrevet under ansættelsesforholdet og efter ansættelsesforholdets ophør. Der skal være underskrevet tavshedserklæringer for samtlige ansatte såvel som eksterne konsulenter og servicepersonale, som arbejder med fortrolige informationer for Lyngby-Taarbæk Kommune.

6 Fysisk sikkerhed

Lyngby-Taarbæk Kommune skal sikre bygninger og installationer af lokaler, som indeholder it-udstyr og data. Kravene til sikring af centralt placeret it-udstyr og it-systemer er således væsentligt højere end kravene til sikring af udstyr i kontormiljøerne.

6.1 Sikre områder

Lokaler, hvor der opbevares fortrolige dokumenter eller persondata, skal være aflåst, når ingen er til stede. Datacentre skal være særligt sikret mod uvedkommende adgang, brand, vand og strømsvigt.

6.2 Fysisk adgangskontrol

Adgang til lokationer skal tildeles på baggrund af autorisationer og beskyttes med et hensigtsmæssigt adgangskontrolsystem.

Alle medarbejdere skal sørge for, at der ikke gives adgang til andre end medarbejdere med gyldig adgangsautorisation til områder uden offentlig adgang.

6.3 Beskyttelse af udstyr

It-udstyr skal beskyttes mod brand, vandskade, strømsvigt og andre skader, som udspringer af hændelser i det omkringliggende miljø. It-udstyr skal overvåges og vedligeholdes efter IT-afdelingens anvisninger. Ved bortskaffelse, reparation eller genbrug af it-udstyr skal det sikres, at udstyret er forsvarligt renset for alle data. Når it-udstyr bortskaffes eller på anden måde udskiftes, skal alle data slettes.

7 Styring af netværk og drift

Lyngby-Taarbæk Kommune stiller høje krav til tilgængelighed af kritiske systemer og fortrolige informationer. Der skal bl.a. være udarbejdet driftsmanualer, som sikrer en stabil og sikker drift.

Driftsforstyrrelser skal imødegås gennem:

- forebyggende foranstaltninger (kvalitetssikring, ændringshåndtering, teknisk dokumentation, etc.),
- hændelseshåndtering, der sikrer hurtig skadeudbedring og imødegåelse af konsekvenser ved brud på sikkerheden.

7.1 Eksterne serviceleverandører

Der skal eksistere procedurer for eksterne serviceleverandører, således at de overholder gældende sikkerhedskrav. Kravene er gældende ved f.eks.:

- VPN (fjernadgang),
- eksternt hosted systemer og udstyr,
- fysisk adgang til lokaliteter,
- service på udstyr i alt almindelighed,
- adgang ved rengøring og anden bygningsvedligehold.

7.2 Styring af driftsmiljø

Styring af driftsmiljøet skal ske gennem:

- udarbejdelse af driftsmanualer, der sikrer stabilitet i driftsmiljøet,
- ændringsstyring som sikrer at ændringer ikke skaber nedbrud og sårbarheder,
- løbende overvågning af kapaciteten på servere med kritiske systemer og informationer, med henblik på at sikre pålidelig drift og tilgængelighed,
- adskillelse af udviklings-, test- og driftsmiljøer,
- implementering og opdatering af systemer, som beskytter mod ondsindede programkoder,
- løbende vurderinger af tilgængelige sikkerhedsrettelser, f.eks. "patches" og "hot fixes" til anvendte operativsystemer,
- planlægning af opgraderinger af eksisterende systemer, således at der er mulighed for reetablering og fejlhåndtering,
- hændelsesstyring som tager hånd om alle identificerede sikkerhedshændelser og udbedrer eventuelle sårbarheder,
- løbende indhentning af informationer om sårbarheder i de anvendte systemer. Sårbarhederne skal evalueres, risici vurderes og på baggrund af dette implementeres passende foranstaltninger.

7.3 Sikkerhedskopiering

Der skal foretages backup af kritisk information og forretningskritiske systemer.

Der skal være udarbejdet procedurer for sikkerhedskopiering og backup med faste intervaller balanceret i forhold til den forretningsmæssige risikovurdering (kritikalitet).

Aftaler med eksterne leverandører skal indeholde krav svarende til procedurer, frekvenser mv., som gælder for Lyngby-Taarbæk Kommune.

Regelmæssige test skal sikre, at sikkerhedskopierne kan genindlæses. Sikkerhedskopierne skal opbevares på en anden lokation adskilt fra produktionsdata.

7.4 Netværkssikkerhed

IT-afdelingen i Lyngby-Taarbæk Kommune skal sikre netværket imod uautoriseret adgang. Der må således ikke installeres netværksudstyr (f.eks. trådløse modem) uden IT-afdelingens godkendelse, ligesom der skal være etableret firewall-løsninger.

Netværket skal overvåges løbende med henblik på at opdage og udbedre brud på sikkerheden.

IT-afdelingen skal opstille regler for brug af bærbart udstyr (f.eks. tablets og mobiltelefoner) med adgang til netværket.

7.4.1 Trådløse netværk

Der er etableret trådløst netværk på alle Lyngby-Taarbæk Kommunes lokationer. Der må kun etableres trådløst lokalnet efter IT-afdelingens godkendelse. Nettet skal konfigureres således, at uautoriseret adgang og aflytning ikke er mulig. Adgang til trådløst netværk skal kræve gyldigt brugernavn og password. Der er et trådløst gæstenetværk, hvor det tilstræbes at overvåge og logge gæsters anvendelse af internettet.

7.5 Logning og overvågning

Lyngby-Taarbæk Kommune skal foretage logning og overvågning af kritiske systemer. Logningerne skal anvendes med henblik på at opdage og spore uautoriserede handlinger, således at disse handlinger kan føres tilbage til enkeltpersoner eller identificerbart netværksudstyr.

7.6 Adgangsstyring

Alle informationsaktiver (applikationer, data, informationer, udstyr og medier) skal være beskyttet mod uautoriseret adgang. Der skal periodisk tages stilling til adgangsforhold til it-systemerne, både fysisk og via netværk.

Der skal anvendes elektroniske adgangskontrolsystemer, som ud over adgangskontrol kan alarmere og via logning danne grundlag for efterfølgende kontroller.

7.6.1 Administration af brugeradgang

Tildeling, ændring og sletning af brugeradgang til systemer og data skal ske ud fra arbejdsbetingede behov. Review af fysiske adgangstildelinger og brugerrettigheder til netværk og systemer skal mindst gennemføres én gang om året.

Anvendelsen af administratorrettigheder skal løbende registreres og i videst muligt omfang begrænses.

7.7 Mobilt udstyr og fjernarbejdspladser

Informationssikkerhedspolitikken skal gælde for alt it-udstyr, som anvendes til behandling af information og informationssystemer for Lyngby-Taarbæk Kommune, herunder alt mobilt udstyr og udstyr i hjemmet.

7.8 Cyber Security

I Lyngby-Taarbæk Kommune har cyber security særlig stor opmærksomhed grundet de seneste års udvikling på området. Området skal passes ind i de eksisterende aktiviteter for informationssikkerhed.

Lyngby-Taarbæk Kommune vil sikre:

- Beskyttelse af kritisk infrastruktur og de vigtigste informationssystemer imod cybertrusler,
- kontinuerlig forbedring af vores evne til at identificere og indberette cyberhændelser,
- kontinuerlig forbedring af medarbejdernes bevidsthed om risici fra cybertrusler.

8 Anskaffelse, udvikling og vedligeholdelse af it-systemer

De sikkerhedskrav, der stilles til systemers behandling af data, skal indgå i vurderingen, som foretages ved indkøb og test af eksternt udviklede systemer. Det enkelte system skal have implementeret sikringsforanstaltninger (f.eks. adgangskontrol, logning, kryptering og særlige beskyttelse i henhold til GDPR lovgivning i tilfælde af persondata behandling), der er tilstrækkelige i forhold til de informationer og forretningsmæssige funktioner, som systemet behandler.

Installation af nye systemer skal ske i overensstemmelse med procedurer, der sikrer stabilt driftsmiljø.

Data, der anvendes til test, skal udvælges omhyggeligt og nøje kontrolleres, så det ikke forårsager tab af fortrolighed for kritisk forretningsinformation.

8.1 Sikkerhed i udviklingsprocesser

IT-afdelingen skal etablere godkendelsesprocedurer for nye systemer, nye versioner og opdateringer af eksisterende systemer. Godkendelsesprocedurerne skal indeholde krav til dokumentation, specifikationer, test, kvalitetskontrol og en styret implementeringsproces.

Der skal foretages en risikovurdering af ændringerne i forhold til eksisterende sikringsforanstaltninger og eventuelt opståede behov for nye sikringsforanstaltninger.

Når driftsmiljøet ændres skal kritiske forretningssystemer gennemgås og testes for at sikre, at ændringerne ikke har utilsigtede afledte virkninger på den daglige drift og sikkerhed.

Nye systemer skal opfylde kravene om security by design.

9 Hændelsesstyring

Alvorlige hændelser som påvirker informationssikkerheden skal registreres og analyseres:

- Hændelser, der har indflydelse eller potentiel indflydelse på informationssikkerheden, skal rapporteres til Medarbejderservice og registreres i hændelsesregistret.
- Hændelser vedrørende brud på persondata skal registreres i SBSYS jf. vejledning om håndtering af brud på persondatasikkerheden.
- Hændelser, der har indflydelse på informationssikkerheden, skal afklares i overensstemmelse med gældende serviceaftaler for det enkelt system.
- Hændelser, der ikke kan afklares inden for aftalt tid, skal håndteres i overensstemmelse med procedurer for denne type hændelser, herunder regler for eskalering til eventuelt beredskabsplanen. Hvor der kan komme et økonomisk eller retsligt efterspil skal dokumentation sikres, indsamles og opbevares.

10 Beredskabsstyring

Lyngby-Taarbæk Kommune skal have en IT-beredskabsplan for kritiske systemer og data. På baggrund af en konsekvensvurdering fastlægges mål for de enkelte it-systemers maksimale nedbrudstid. Resultatet af konsekvensvurderingen dokumenteres i en IT-beredskabsplan.

10.1 IT-beredskabsplan

It-beredskabsplanen skal beskrive organisation og fremgangsmåde ved beskyttelse og begrænsning af tab af data og systemer i forbindelse med katastrofer og alvorlige sikkerhedsbrister.

It-beredskabsplanen skal løbende afprøves og opdateres for at sikre, at de er tidssvarende og effektive.

11 Afvigelser

Såfremt det bliver nødvendigt helt eller delvist at afvige fra informationssikkerhedspolitikken, kræves der godkendelse fra Direktionen.

12 Overtrædelse af politikken

Enhver afvigelse fra og brud på politikken kan have alvorlige konsekvenser for Lyngby-Taarbæk Kommune, hvorfor ethvert brud vil blive betragtet som meget alvorligt.

Ved brud på informationssikkerhedspolitikken vil Direktionen vurdere sagen og dernæst træffe foranstaltninger, der sikrer, at overtrædelsen bringes til ophør. Det kan få ansættelsesretslige konsekvenser, hvis ikke informationssikkerhedspolitikken overholdes.

Hvis en medarbejder er vidende om, at Lyngby-Taarbæk Kommunes informationssikkerhed overtrædes, skal det meddeles til ledelsen hurtigst muligt.

Ved tvivlsspørgsmål og overtrædelser af retningslinjerne kan der indhentes rådgivning og vejledning fra Koncernchefgruppen.

13 Outsourcing

Beslutning om outsourcing af væsentlige aktiviteter på it-området træffes af Direktionen efter fastlagte retningslinjer.

Det er en direktionsbeslutning på baggrund af økonomi, sikkerhed, hastighed, fleksibilitet (den samlede vurdering), der ligger til grund for outsourcings spørgsmål.

14 Compliance med lovgivning

Lyngby-Taarbæk Kommune skal efterleve regler og love, som er gældende for Lyngby-Taarbæk Kommune i forbindelse med national og regional lovgivning samt betingelser og regler i kontrakter og samarbejdsaftaler.

Der skal være procedurer, der sikrer, at relevante sikkerhedskrav i lovgivning, bekendtgørelser, egne målsætninger for informationssikkerhed samt i kontraktlige forpligtelser, styres og overholdes for de enkelte data og systemer.

Den fornødne juridiske ekspertise skal inddrages i vurderingen af disse krav samt kommunens databeskyttelsesrådgiver (DPO) og informationssikkerhedskoordinatorer.

14.1 Persondata og EU Regulering

Lyngby-Taarbæk Kommune efterlever gældende og ny lovgivning, som har til hensigt at beskytte den enkelte borger og dennes rettigheder over egne persondata som f.eks. EU's databeskyttelsesforordning (GDPR) vedrørende beskyttelse af personoplysninger.

15 Godkendelse af politikken

Informationssikkerhedspolitikken er godkendt den 11.06.2019 af Direktionen og af Økonomiudvalget den 14.11.2019.

LYNGBY-TAARBÆK
KOMMUNE

Center for
Kultur, IT, Politik og Organisation
Lyngby Rådhus

Lyngby Torv 17
2800 Kgs. Lyngby

45 97 30 00
lyngby@ltk.dk
www.ltk.dk