Regler for informationssikkerhed

Ishøj Kommune

2022

Version 2.0

Ishøj Kommune

Indhold

Del 1: Indledning 1
1. Indledning - Strategi for informationssikkerhed 1
1.1 Håndbogens opbygning 1
1.2 De væsentligste dokumenter om informationssikkerhed 1
1.3 Gennemgang og revision af strategien for informationssikkerhed 1
2. Organisering af informationssikkerhed 2
2.1 Roller og ansvarsområder for informationssikkerhed 2
2.2 Ledelsens rolle og ansvar 2
2.3 Medarbejdernes rolle og ansvar 2
Del 2: Quickguide – De 10 bud for informationssikkerhed 3
Sikker Kommunikation 3
Ryddeligt skrivebord, låst skærm og print 3
Opbevaring af digitale dokumenter 3
Oplysningspligten 3
Brug af billed- og videomateriale 3
Brug af sociale medier 4
Indhentning af samtykke 4
Alle sikkerhedshændelser skal indberettes 4
Indkøb af systemer, apps mv., brug af mobile enheder og nye behandlingsaktiviteter 4
Brug af privat udstyr og hjemme/fjernarbejdspladser 4
Del 3: Regler for informationssikkerhed 5
3. Beskyttelse af fysiske og digitale dokumenter 5
3.1 Forretningskritiske dokumenter 5
3.2 Fysiske dokumenter med person- eller virksomhedsoplysninger 5
3.3 Digitale dokumenter med person- eller virksomhedsoplysninger 5
4. Kommunikation 5
4.1 Kommunikation med borgerne 5
4.2 Kommunikation med samarbejdspartnere og andre myndigheder 6
4.3 Kommunikation på sociale medier 6
4.4 Privat kommunikation i arbejdstiden 6
Brug af sociale medier og internet 6
Private mails 6
5. Kommunale hjemmesider 7

6. Kommunens oplysningspligt 7
7. Indhentning af samtykke 7
8. Dataminimering 7
9. Risikovurderinger 8
10. Sikkerhedsbrud 8
11. Brug af privat udstyr, hjemme/fjernarbejdspladser og mobile enheder 8
12. Brugerrettigheder 8
13. Adgangskoder og adgangskort 9
13.1 Adgangskoder 9
13.2 Adgangskort 9
14. Ryddeligt skrivebord, låst skærm og print 9
15. Anskaffelse af IT-systemer, apps, programmer m.v. 9
15.1 Databehandleraftaler med leverandøren 10
16. Installation af programmer på arbejdscomputere og PC'er. 10
17. Phishing 10
18. Lukning af døre/adgangskontrol 10
19. Inddragelse af sikkerhedsgruppen 10
20. Sanktioner 10
21. Opdatering og godkendelse af håndbogen 10
Bilag 1: Organisation for informationssikkerhed 11

Del 1: Indledning

1. Indledning - Strategi for informationssikkerhed

Denne håndbog er en del af Ishøj Kommunes overordnede strategi for informationssikkerhed. Håndbogen er et mere praktisk dokument, som konkret beskriver, hvilke regler de ansatte skal følge for at beskytte borgernes, virksomhedernes og kommunens oplysninger.

Denne håndbog skal være et opslagsværk, som er en hjælp for kommunens ansatte.

1.1 Håndbogens opbygning

Håndbogen indeholder følgende 3 dele:

1) En indledning, som sætter rammen omkring strategi for informationssikkerhed i Ishøj Kommune. Indledningen nævner de vigtigste dokumenter, som ansatte i Ishøj Kommune bør kigge på i forhold til informationssikkerhed. Indledningen er samtidig en læsevejledning til denne håndbog.
2) En kort quickguide med fokus på de vigtigste indsatsområder for kommunen. Idéen er, at den enkelte leder skal læse hele håndbogen og tilpasse quickguiden til eget område. Quickguiden kan herefter udskrives og omdeles/hænges op, så arbejdet med informationssikkerhed bliver nærværende og lettilgængeligt i dagligdagen.
3) Den fulde håndbog *Regler for Informationssikkerhed*, hvor du kan få svar på dine spørgsmål om informationssikkerhed. Håndbogen er et opslagsværk, som man kan orientere sig i via indholdsfortegnelsen.

1.2 De væsentligste dokumenter om informationssikkerhed

De væsentligste dokumenter, man som medarbejder bør kende, for at leve op til kommunens niveau for informationssikkerhed, er følgende:

- *Informationssikkerhedspolitikken*, som beskriver kommunens overordnede principper på området.
- *Regler for Informationssikkerhed*, som er denne håndbog, som beskriver de praktiske regler for informationssikkerhed.
- *Kommunens centrale procedurer*, som omhandler informationssikkerhed

Ovenstående er altid tilgængeligt på kommunens intranet,www.uglen.ishoj.dk/gdpr. Her ligger desuden relevante skabeloner og vejledninger, som også kan være nyttige at orientere sig i.

Ud over ovenstående er hensigten, at de enkelte områder udarbejder de nødvendige arbejdsgange og lokale procedurer, som sikrer det ønskede informationssikkerhedsniveau. Det kan eksempelvis være lokale procedurer omkring indhentning af samtykke, brug af billeder og video, sikker kommunikation med borgerne, sikker opbevaring af dokumenter mv.

1.3 Gennemgang og revision af strategien for informationssikkerhed

Ishøj Kommunes *Informationssikkerhedspolitik* skal revideres og godkendes af Byrådet årligt.

Håndbogen *Regler for informationssikkerhed* skal revideres og godkendes af Koncernledelsen årligt. Ved væsentlige ændringer, skal håndbogen godkendes i Hoved-MED forinden.

2. Organisering af informationssikkerhed

2.1 Roller og ansvarsområder for informationssikkerhed
Den overordnede fordeling af roller og ansvar i forbindelse med informationssikkerhedsarbejdet i Ishøj Kommune er beskrevet i Bilag 1.

2.2 Ledelsens rolle og ansvar
Koncernledelsen skal understøtte kommunens informationssikkerhed ved at udstikke klare retningslinjer, udvise synligt engagement samt sikre udarbejdelse af de nødvendige arbejdsgange og procedurer til at overholde det ønskede informationssikkerhedsniveau for deres område.

Det er den nærmeste personaleleders ansvar, at:

- Alle medarbejdere er tilstrækkeligt informeret om deres roller og ansvar i forbindelse med informationssikkerheden, før de tildeles adgang til kommunens systemer og data. De skal ligeledes være informeret om kommunens *Informationssikkerhedspolitik, Regler for Informationssikkerhed* samt relevante procedurer og arbejdsgange.
- Alle medarbejdere følger retningslinjerne i ovenstående dokumenter samt eventuelle lokalt fastsatte procedurer og arbejdsgange.
- Alle medarbejdere modtager løbende information om informationssikkerhed, herunder om ændringer af kommunens informationssikkerhedspolitik, regler for informationssikkerhed eller procedurer.
- At sørge for, at roller og rettigheder passer til medarbejderens kompetencer og arbejdsområde, samt at adgange bliver lukket eller ændret, så snart ansættelsen ændres eller ophører.

2.3 Medarbejdernes rolle og ansvar
Medarbejderne skal bidrage aktivt til beskyttelsen af kommunens data, og de har en pligt til at indberette eventuelle trusler og brud til nærmeste leder. Alle medarbejdere skal således gøre sig bekendt med kommunens Informationssikkerhedspolitik, håndbogen Regler for Informationssikkerhed og tilhørende procedurer. De har ligeledes pligt til at deltage i evt. obligatoriske forløb som e-læring, kurser mv.

Alle medarbejdere skal følge de arbejdsgange og procedurer, der er fastlagt inden for deres arbejdsområde. Det kan eksempelvis være procedurer omkring sikker kommunikation med borgerne, indhentning af samtykke, brug af billedmateriale mv.

Alle medarbejdere har tavshedspligt om de informationer, de får kendskab til under deres virke hos Ishøj Kommune. Tavshedspligten ophører ikke forbindelse med skifte af funktion eller fratrædelse.

Når man fratræder sin stilling, skal man aflevere de enheder (telefon, computer, tablet, adgangskort mv.), man har fået udleveret under sin ansættelse, tilbage til Ishøj Kommune.

Del 2: Quickguide – De 10 bud for informationssikkerhed

Vi anbefaler, at man som leder kigger hele håndbogen igennem og tilretter quickguiden i forhold til ens eget område. Quickguiden skal gerne kunne hænges op, så den er synlig for medarbejderne.

Sikker Kommunikation

Vi skal bruge Digital Post eller sikre systemer som eks. AULA, når vi skriver sammen med borgere eller virksomheder, hvis samtalen indeholder fortrolige eller følsomme oplysninger.

Det er sikkert at skrive internt mellem to @ishoj.dk mailadresser samt at skrive til medarbejdere i andre kommuner. Hvis du er i tvivl, om du sender sikkert, så klik på knappen Send Digitalt i Outlook, så bliver mailadressen grøn, hvis den er sikker.

Ryddeligt skrivebord, låst skærm og print

Fysiske dokumenter med forretningskritiske oplysninger, personoplysninger eller virksomhedsoplysninger skal journaliseres, hvis de er relevante for en sag.

Dokumenterne må ikke være tilgængelige for uvedkommende, heller ikke når de er smidt i skraldespanden eller fordelt i et dueslag. Forretningskritiske dokumenter skal opbevares bag dobbelt lås, det kan eks. være i en aflåst skuffe eller i et aflåst kontorområde. I særlige tilfælde kan det være nødvendigt at opbevare dokumenterne i et brandsikkert skab.

Når man forlader sin plads ved endt arbejdsdag, skal ens skrivebord være ryddet for forretningskritiske dokumenter. Dokumenter med person- eller virksomhedsoplysninger skal ligge med bagsiden opad. Hvis de ligger et sted, hvor der er adgang for uvedkommende, skal disse dokumenter også låses inde.

Ens skærm/computer skal låses, når man forlader den (brug genvejstast ⊞+L for at låse skærmen).

Printere, som benyttes til udskrivning af fortrolige oplysninger, skal have en adgangskodefunktion som follow me eller tilsvarende. Hvis dette ikke er muligt, skal dokumenterne hentes fra printeren med det samme efter udskrift.

Opbevaring af digitale dokumenter

Digitale dokumenter med fortrolige eller følsomme oplysninger om personer eller virksomheder skal gemmes i et sikkert system som SBSYS eller et fagsystem. Dokumentet må kun ligge i Outlook eller på computeren i en meget begrænset periode, til man har mulighed for at journalisere det korrekt.

Oplysningspligten

Når vi modtager eller indhenter oplysninger om en borger, så har vi pligt til at oplyse borgeren om en række informationer i forbindelse med behandlingen af deres personoplysninger. Se kommunens skabelon til overholdelse af oplysningspligten på www.uglen.ishoj.dk/gdpr.

Brug af billed- og videomateriale

Når vi tager billeder eller video, skal vi overholde vores oplysningspligt (se ovenstående).

Følg Ishøj Kommunes vejledning om brug af billeder og video, hvis du skal bruge billed- eller videomateriale i dit arbejde.

Brug af sociale medier

Vi må aldrig dele eller drøfte fortrolige eller følsomme person- eller virksomhedsoplysninger på sociale medier. Ligeledes skal eventuelle opslag indeholdende disse typer af oplysninger slettes hurtigst muligt.

Da vi ikke har nogen aftaler med sociale medier om delt dataansvar, kan vi ikke overholde GDPR, når vi bruger disse tjenester.

Indhentning af samtykke

Hvis vi behandler personoplysninger uden direkte lovhjemmel, skal vi indhente et informeret samtykke, inden vi behandler oplysningerne. Samtykket skal kunne dokumenteres.

Alle sikkerhedshændelser skal indberettes

Følg kommunens procedure for håndtering af sikkerhedsbrud

Indkøb af systemer, apps mv., brug af mobile enheder og nye behandlingsaktiviteter

Al indkøb af systemer, apps mv. som skal indeholde personoplysninger skal godkendes af IT, så vi sikrer os, at systemet/appen lever op til de gældende kriterier for sikkerhed.

Alle mobile enheder, som indeholder følsomme, fortrolige eller forretningskritiske oplysninger (telefon, tablet, bærbar, USB mv.) skal krypteres eller være beskyttet med adgangskode.

Kommunens databeskyttelsesrådgiver skal altid inddrages i forbindelse med ibrugtagning af ny teknologi, indkøb af nye IT-systemer og introduktion af nye behandlingsaktiviteter, hvor der behandles personoplysninger (eks. nye projekter).

Brug af privat udstyr og hjemme/fjernarbejdspladser

Kommunens fortrolige og personhenførbare oplysninger må ikke opbevares på private enheder som mobiltelefoner, computere, tablets mv. Hvis en medarbejder ønsker at tilgå sin Outlook mail/kalender på en privat enhed, skal denne tilgås via websiden https://webpost.ishoj.dk/owa, så der ikke automatisk lagres information på enheden. Det er ikke i overensstemmelse med denne retningslinje at synkronisere sin arbejdsmail eller kalender ned på ens private mobil/enhed, medmindre enheden er til både privat og arbejdsbetinget brug.

3. Beskyttelse af fysiske og digitale dokumenter

3.1 Forretningskritiske dokumenter

Forretningskritiske dokumenter er dokumenter der kan have betydning for Ishøj Kommunes økonomi eller omdømme, hvis de kommer i forkerte hænder.

Forretningskritiske dokumenter, som kommunen ikke kan tåle at miste, skal journaliseres i kommunens ESDH-system (SBSYS) eller i et fagsystem hurtigst muligt, så de ikke går tabt. Forretningskritiske dokumenter, som ikke er journaliseret, skal opbevares bag dobbelt lås. Det kan eksempelvis være i en aflåst bygning/etage og derudover på et aflåst kontor eller i en aflåst skuffe/skab. Forretningskritiske dokumenter, som medfører en høj risiko for kommunen, bør opbevares i et brandsikkert skab. Der er et brandsikkert skab i kælderen på Rådhuset.

3.2 Fysiske dokumenter med person- eller virksomhedsoplysninger

Fysiske dokumenter med person- eller virksomhedsoplysninger skal opbevares, så de ikke er tilgængelige for personer, der ikke bør have adgang til oplysningerne. Det kan eksempelvis være et sted med adgangskontrol, på et aflåst kontor eller i et aflåst skab, hvis der er adgang til etagen for uvedkommende.

Dette gælder også dokumenter, som er fordelt som post, i dueslag eller smidt i en skraldespand mv. Åbne skraldespande skal tømmes dagligt og indholdet skal smides i en større skraldespand eller container, som enten er utilgængelig for uvedkommende eller aflåst.

3.3 Digitale dokumenter med person- eller virksomhedsoplysninger

Digitale dokumenter med person- eller virksomhedsoplysninger skal gemmes i et fagsystem eller i SBSYS. Systemet skal være godkendt af IT til at kunne opbevare denne type oplysning.

Dokumenter med person- eller virksomhedsoplysninger må kun gemmes på en computer med adgangskode eller i Outlook i en meget begrænset periode, indtil man kan lægge det over i et fagsystem eller SBSYS, hvorefter dokumentet skal slettes.

4. Kommunikation

4.1 Kommunikation med borgerne

Når vi kommunikerer med borgerne om konkrete sager, skal det som altovervejende hovedregel ske via en sikker forbindelse, f.eks. Digital Post, AULA eller en telefonsamtale, hvor man verificerer (bekræfter), at den person, man taler med, er den rette. Mail og SMS er ikke sikre forbindelser.

Personhenførbare oplysninger må kun sendes via almindelig e-mail, hvis korrespondancen vedrører almindelig vejledning, som eksempelvis kan findes på en hjemmeside, og hvis der ikke er tale om *følsomme* eller *fortrolige* oplysninger (se nedenfor).

Hvis en borger eller andre sender en mail indeholdende fortrolige eller følsomme oplysninger, så skal indholdet i den oprindelige mail slettes, før mailen besvares. Alternativt skal svaret sendes via Digital Post.

Det er tilladt at sende en påmindelses-SMS til en borger, hvis denne ikke indeholder fortrolige eller følsomme oplysninger. Det er vigtigt, at oplysningerne ikke kan misbruges, hvis de kommer i uvedkommendes hænder. Derfor bør man også undlade at skrive borgerens fulde navn, adresse, alder o.l., hvis det er muligt.

I særlige tilfælde kan der dispenseres for ovenstående, hvis hensynet til borgeren vejer tungere end hensynet til beskyttelse af oplysningerne. Dette beror dog på en konkret vurdering, som skal foretages af den enkelte leder sammen med informationssikkerhedsteamet.

Følsomme oplysninger er helbredsoplysninger, oplysninger om fagforeningsmæssige tilhørsforhold, race, etnisk oprindelse, Genetiske data, biometriske data (med henblik på entydig identificering), seksuelle forhold og seksuel orientering.

Fortrolige oplysninger er oplysninger, som efter den almindelige opfattelse i samfundet ikke bør komme til offentlighedens kendskab. Det kan eks. være cpr.nr., strafbare forhold, økonomiske forhold, interne familieforhold, herunder f.eks. adoption, skilsmisse/separation, oplysninger om selvmordsforsøg og ulykkestilfælde.

4.2 Kommunikation med samarbejdspartnere og andre myndigheder

Det er kun tilladt at sende almindelige mails til samarbejdspartnere og andre myndigheder, hvis korrespondancen ikke indeholder følsomme eller fortrolige oplysninger.

Kommunikation, som indeholder følsomme eller fortrolige oplysninger, skal ske via sikre forbindelser som Digital Post, sikker mail eller en telefonsamtale, hvor man sikrer sig, at det er den rette, man taler med.

Det er muligt at skrive sikkert via Outlook til de fleste kommuner og til mange offentlige myndigheder. Hvis du er i tvivl, om du sender sikkert, så klik på knappen Send Digitalt i Outlook, så bliver mailadressen grøn, hvis den er sikker.

4.3 Kommunikation på sociale medier

Vi må aldrig dele eller drøfte fortrolige eller følsomme person- eller virksomhedsoplysninger på sociale medier. Ligeledes skal eventuelle opslag indeholdende disse typer af oplysninger slettes hurtigst muligt.

Da vi ikke har nogen aftaler med sociale medier om delt dataansvar, kan vi ikke overholde GDPR, når vi bruger disse tjenester.

4.4 Privat kommunikation i arbejdstiden

<u>Brug af sociale medier og internet</u>
Medarbejderne må i begrænset omfang gøre brug af internettet og sociale medier til privat brug i arbejdstiden, så længe dette ikke påvirker ens arbejdsopgaver.

Det er ikke tilladt at bruge Citrix til at streame TV, downloade film eller til andet, som belaster netværket unødigt, hvis det ikke sker i forbindelse med ens opgavevaretagelse.

<u>Private mails</u>
Medarbejderne må anvende kommunens mailsystemer til personligt brug i begrænset omfang, hvis dette ikke har indflydelse på kommunens drift og sikkerhed i øvrigt. Medarbejderne skal i så fald markere samtalen som privat i emnefeltet.

Kommunen forbeholder sig ret til at skaffe sig adgang til data og e-mail for medarbejdere, hvis dette sker af drifts- eller sikkerhedshensyn. Kommunen vil så vidt muligt undgå at åbne mailkorrespondance, som er markeret med 'privat'.

5. Kommunale hjemmesider

Kommunale hjemmesider skal være 'tracking frie' zoner jf. den fælles vejledning fra Erhvervsstyrelsen og Digitaliseringsstyrelsen. Det vil sige, at:

1) Det er tilladt at bruge cookies til at indsamle statistik om brugernes færden på hjemmesiden for at optimere hjemmesiden eller ens tilbud.
2) Det er ikke tilladt at bruge cookies fra tjenester som Google Analytics og lignende, som indsamler data om de besøgende og videregiver disse til tredje part (dvs. andre virksomheder).
3) Det er ikke tilladt at have cookies på hjemmesiden, som indsamler data om den besøgende, inden denne har givet sin accept hertil.
4) Vi skal overholde oplysningspligten, når vi indsamler cookies.

6. Kommunens oplysningspligt

Kommunen skal altid overholde sin oplysningspligt. Det vil sige, at når vi indsamler eller modtager oplysninger om en borger, har vi en pligt til at oplyse borgeren om, at vi behandler personoplysninger om vedkommende.

Som en del af oplysningspligten skal borgeren bl.a. have oplysninger om formål og hjemmel for behandlingen, hvilke oplysninger vi gemmer og hvor længe, vi gemmer oplysninger, hvem vi indsamler og videregiver oplysninger til mv. Borgeren skal ligeledes oplyses om deres rettigheder i forbindelse med behandlingen.

Oplysningspligten gælder også, hvis der indsamles data om en bruger via cookies på en hjemmeside.

Du kan hente en skabelon til opfyldelse af oplysningspligten på Uglen. På Uglen kan du ligeledes finde databeskyttelsesrådgiverens vejledning om overholdelse af oplysningspligten.

7. Indhentning af samtykke

Vi må kun behandle personoplysninger, hvis vi har enten lovhjemmel til det eller har indhentet et samtykke til behandlingen. Hvis vi ikke har lovhjemmel, skal borgeren give sit informerede samtykke. Det betyder, at borgeren, i et letforståeligt sprog, bl.a. skal være informeret om, hvem der er ansvarlig for behandlingen (Ishøj Kommune), formålet med behandlingen, hvilke oplysninger der indsamles, hvad vi gør med oplysningerne samt, at borgeren kan trække sit samtykke tilbage. Der findes en skabelon til indhentning af samtykke på Uglen.

Vi skal efterfølgende kunne dokumentere, at der er indhentet et informeret samtykke.

Hvis formålet med behandlingen ændrer sig, skal der indhentes et nyt samtykke.

8. Dataminimering

Som kommune må vi kun indsamle de personoplysninger, der er nødvendige for, at vi kan løse vores opgave som myndighed. Vi må ikke indsamle og gemme oplysninger, fordi de kan være rare at have i fremtiden. Dog er vi forpligtet til at registrere og gemme de oplysninger, vi modtager om en borger eller virksomhed, da vi samtidig har notatpligt efter forvaltningsloven.

9. Risikovurderinger

Alle områder skal lave en risikovurdering, når de ændrer arbejdsgange, procedurer, påbegynder nye behandlingsaktiviteter eller tager ny teknologi eller IT-system i brug. Dette er en vigtig øvelse at gøre, så vi kan bruge risikovurderingen til at iværksætte de nødvendige organisatoriske og tekniske foranstaltninger og derved sikre, at vores daglige arbejde med kommunens informationer sker i overensstemmelse med det ønskede sikkerhedsniveau. Center for Borger, Økonomi og IT har en skabelon til formålet.

Risikovurderingen skal kunne dokumenteres.

Kommunens databeskyttelsesrådgiver skal inddrages, når der tages ny teknologi i brug, der indkøbes nye systemer eller, hvis man opstarter en ny behandlingsaktivitet, eks. et projekt.

10. Sikkerhedsbrud

Alle sikkerhedsbrud som vedrører data, Ishøj Kommune er dataansvarlig for, skal indberettes og håndteres ved at følge Ishøj Kommunes *Procedure for håndtering af brud på persondatasikkerheden*.

11. Brug af privat udstyr, hjemme/fjernarbejdspladser og mobile enheder

Kommunens fortrolige og personhenførbare oplysninger må som udgangspunkt ikke opbevares på private enheder som mobiltelefoner, computere, tablets mv., medmindre enheden er udleveret til både privat og arbejdsbetinget brug. Hvis en medarbejder ønsker at tilgå sin Outlook mail/kalender på en privat enhed, skal denne tilgås via websiden https://webpost.ishoj.dk/owa, så der ikke automatisk lagres information på enheden. Det er ikke i overensstemmelse med denne retningslinje at synkronisere sin arbejdsmail eller kalender med sin private mobil/enhed, medmindre enheden er udleveret af Ishøj Kommune til både privat og arbejdsbetinget brug.

I særlige tilfælde, og efter aftale med sin leder, kan der dispenseres for ovenstående regel, hvis dokumenterne ikke indeholder følsomme eller forretningskritiske oplysninger, og hvis dokumenterne slettes indenfor en meget begrænset periode.

Hvis der gives tilladelse til dette, skal enheden beskyttes med et sikkerhedsprogram, som skal installeres af IT afdelingen. Sikkerhedsprogrammet sikrer, at IT kan slette indholdet på telefonen, hvis det bliver nødvendigt.

Alle enheder (også private), som indeholder persondata, som Ishøj kommune er dataansvarlig for, skal altid være beskyttet af en adgangskode eller tilsvarende (fingeraftryk, ansigtskendelse mv.), så uvedkommende ikke kan få adgang til informationerne.

12. Brugerrettigheder

Alle ansatte må kun have adgang til de informationer og systemer, som er nødvendige for, at de kan udføre deres arbejde.

Alle ansattes brugeradgangsrettigheder skal gennemgås 2 gange om året, så vi sikrer, at rettighederne afspejler medarbejderens aktuelle funktion. Det er lederens ansvar at sikre, at medarbejderens adgangsrettigheder passer med medarbejderens arbejdsmæssige behov.

Medarbejderne skal returnere alle udleverede enheder samt adgangskort, nøgler mv. fra arbejdsstedet ved ansættelsens ophør, og deres brugerrettigheder skal fjernes.

Databeskyttelsesrådgiveren har desuden udarbejdet en vejledning om emnet, som findes på Uglen.

13. Adgangskoder og adgangskort

13.1 Adgangskoder

Medarbejderne må ikke anvende samme adgangskode til kommunens infrastruktur som til adgang til tredjepartsudstyr, f.eks. internet-websteder og netbanker. Omfattende brug af samme adgangskode på tredjepartsystemer øger sandsynligheden for, at adgangskodens fortrolighed brydes.

Adgangskoder skal indeholde mindst 8 tegn. Adgangskoder skal indeholde kombinationer af både tal samt store og små bogstaver.

Der må ikke benyttes brugernavn eller navn som en del af adgangskoden.

Adgangskoder skal skiftes efter højst 90 dage.

Adgangskoder er strengt personlige og må ikke deles med andre. Adgangskoden må ikke gemmes på skrivebordet, skærmen eller lignende.

13.2 Adgangskort

ID-kort/adgangskort er strengt personlige og må ikke deles med andre. Adgangskort skal bestilles af nærmeste leder.

14. Ryddeligt skrivebord, låst skærm og print

Medarbejderne skal sætte deres skærm i pause, så den er adgangsbeskyttet, når de forlader deres computer (brug genvejstast ⊞+L).

Skriveborde skal ryddes for fortrolige dokumenter senest ved arbejdsdagens afslutning.

Forretningskritiske dokumenter må ikke ligge fremme. De skal lægges i en aflåst skuffe eller skab (dobbelt lås).

Dokumenter med personhenførbare oplysninger må ikke ligge med forsiden opad, når skrivebordet forlades. Hvis der er adgang til ens skrivebord for personer, der ikke er ansatte af kommunen, skal dokumenterne låses inde.

Øvrige dokumenter må gerne ligge fremme, såfremt kontorarealer er aflåste.

Printere som benyttes til udskrivning af fortrolige eller følsomme personoplysninger skal have en adgangskodefunktion som *follow me* eller tilsvarende, der sikrer, at kun de rette medarbejdere får adgang til udskrifterne. Hvis det ikke er muligt at installere en adgangsfunktion, skal dokumenterne hentes fra printeren med det samme efter udskrift.

15. Anskaffelse af IT-systemer, apps, programmer m.v.

Anskaffelse af IT-systemer, apps, programmer mv. skal godkendes af IT eller Skole-IT. Ligeledes skal kommunens databeskyttelsesrådgiver inddrages. Hvis systemet indeholder personoplysninger, skal der udarbejdes en risikovurdering inden anskaffelsen.

15.1 Databehandleraftaler med leverandøren

Hvis man vil anskaffe et IT-system, app mv., som skal indeholde persondata, så skal der indgås en databehandleraftale, inden systemet tages i brug. Databehandleraftalen skal godkendes af systemejeren med bistand fra en informationssikkerhedskoordinator.

Databehandleraftalen skal sikre, at kommunens oplysninger opbevares og behandles efter gældende regler og love samt kommunens informationssikkerhedspolitik. Det er systemejeren, der er ansvarlig for databehandleraftalen og brugen af systemet

16. Installation af programmer på arbejdscomputere og PC'er.

Der må kun hentes programmer ned på ens PC eller bærbar, som er nødvendige for ens opgavevaretagelse. Programmet skal være godkendt af IT-afdelingen.

Der må ikke hentes spil, apps eller programmer, som er til privat brug eller underholdning.

17. Phishing

Medarbejderne skal være særligt opmærksomme på forsøg på phishing, hvor andre prøver at få adgang til kommunens informationer. Det kan eksempelvis være ved at sende en mail med et link, man skal klikke på, hvorefter man har givet personen adgang til sin computer. Det kan også være ved at aflure et kodeord eller at få en til at downloade et program med virus.

18. Lukning af døre/adgangskontrol

Områder med fortrolige, følsomme eller forretningskritiske oplysninger skal sikres med lås eller adgangskontrol.

19. Inddragelse af sikkerhedsgruppen

Kommunens informationssikkerhedsteam skal inddrages i forbindelse med drøftelser om væsentlige informationssikkerhedsspørgsmål i kommunen. Gruppen har som en del af sit virke pligt til at inddrage kommunens Databeskyttelsesrådgiver.

20. Sanktioner

Manglende efterlevelse af ovenstående regler, tilsidesættelse af kommunens informationssikkerhedspolitik eller manglende efterlevelse af kommunens øvrige procedurer omkring informationssikkerhed kan have ansættelsesretlige konsekvenser.

21. Opdatering og godkendelse af håndbogen

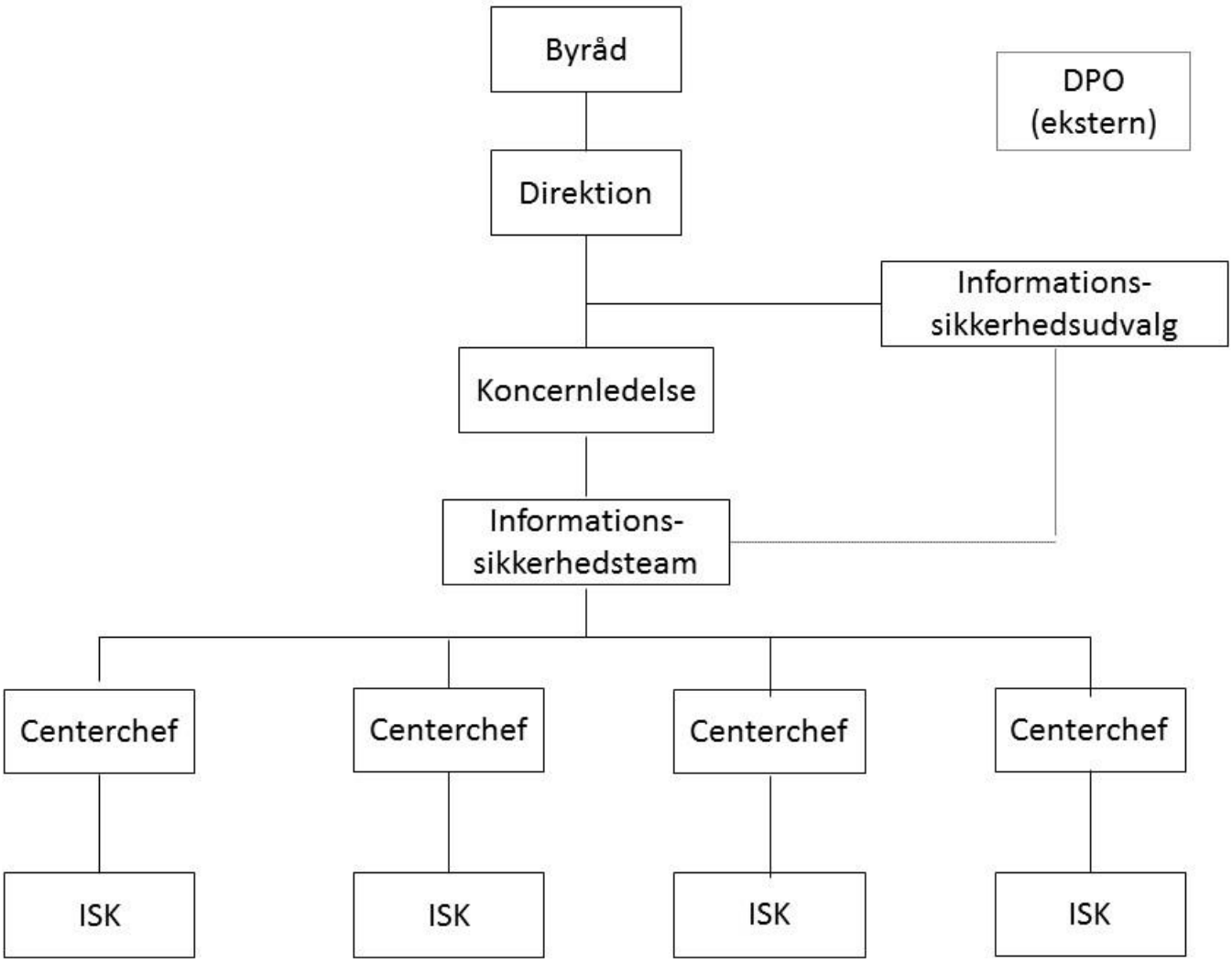
Center for Borger, Økonomi og IT opdaterer håndbogen efter behov og mindst en gang om året.

Håndbogen skal godkendes af Koncernledelsen.

Denne version af håndbogen er godkendt af Koncernledelsen den 14. september 2022.

Bilag 1: Organisation for informationssikkerhed

Arbejdet med informationssikkerhed er forankret i organisationen på forskellige niveauer. Hvert niveau har en rolle med forskellige aktiviteter og tilknyttet ansvar.



**ISK = InformationsSikkerhedsKoordinator*

Byrådet	• Godkender informationssikkerhedspolitikken
Direktionen	• Sammensætter Informationssikkerhedsudvalget og udpeger CISO*. CISO samt leder af informationssikkerhedsteamet er fødte medlemmer af informationssikkerhedsudvalget • Opfølgning på informationssikkerheden i Ishøj Kommune • Informerer Byrådet om relevante emner vedrørende informationssikkerheden
Informations-sikkerhedsudvalget	• Udarbejde informationssikkerhedspolitikken • Udarbejde organisatorisk årshjul for informationssikkerhed. • Udarbejde plan for implementering af informationssikkerhedspolitikken, herunder ○ Igangsætte implementering (aktiviteter) for informationssikkerhedspolitikken ○ Opfølgning på implementering (styring af aktiviteter) for informationssikkerhedspolitikken (governance). • Udarbejde retningslinjer og politikker for informationssikkerhed. • Udarbejde årlig rapport på informationssikkerhed til Direktionen. •Sørger for at inddrage relevante centerchefer
Koncernledelsen	• Årlig opfølgning på informationssikkerheden i Ishøj kommune •Sikrer tilstrækkelige ressourcer •Godkender organisatoriske tiltag og aktiviteter på baggrund af oplæg fra Informationssikkerhedsudvalget
Informations-sikkerhedsteamet	•Understøtter informationssikkerhedsudvalgets arbejde •Udførende på informationssikkerhedsudvalgets opgaver •Udførende på centrale opgaver som vedrører informationssikkerheden •Rådgivning og koordinering med de lokale informationssikkerhedskoordinatorer •Rapporterer til informationssikkerhedsudvalget •Rådgivning af centerchefer/KCL
Centerchefer	•Ansvarlig for implementering af informationssikkerhedspolitikken og tilhørende aktiviteter i eget center •Ansvarlig for implementering af lokale initiativer •Ansvarlige for opfølgning på informationssikkerheden i eget center
ISK	• Koordinerer og kontrollerer lokale aktiviteter ifm. Informationssikkerhed. • Udarbejder og implementerer lokale procedurer og retningslinjer • Lokalt kontaktpunkt for centerets medarbejdere • Kontakt til Informationssikkerhedsteamet • Deltagelse i koordinatornetværket

* CISO = Chief Information Security Officer (øverste ansvarlige for informationssikkerheden i Ishøj Kommune