Billund kommune

# Informationssikkerhedspolitik

ISO27001 & 27002

Version 1.0

Maj 2018

# Indhold

# Indledning

Informationssikkerhedspolitikken har til formål, at den tydeligt skal tilkendegive overfor alle der har relationer til Billund Kommune, hvilke standarder og retningslinjer der er fastlagt når det gælder informationssikkerhed.

Som medarbejder i Billund Kommune har du et medansvar for, at overholde informationssikkerhedsreglerne, samt udvise fornuftig adfærd i omgangen med personoplysninger. Den menneskelige faktor er afgørende for at skabe og opretholde den nødvendige sikkerhed. Derfor er måden hvorpå vi alle i Billund Kommune samarbejder afgørende for, at vi kan opretholde et acceptabelt sikkerhedsniveau.

Overtrædelse af informationssikkerhedsreglerne kan i værste tilfælde få alvorlige konsekvenser for kommunen, borgerne eller dig som medarbejder. Læs derfor informationssikkerhedspolitikken godt igennem, så der ikke opstår tvivl om hvorvidt en handling er i strid med sikkerheden.

Informationssikkerhedspolitikken gælder for alle ansatte i Billund Kommune

# Mål

Billund Kommune gennemfører alle nødvendige aktiviteter for at sikre:

- **Tilgængelighed** – At opnå en høj tilgængelighed med høje oppetider og minimeret risiko for nedbrud på IT-systemer.
- **Integritet** – At opnå en pålidelig og korrekt funktion af IT-systemerne med minimeret risiko for ukorrekt datagrundlag, f.eks. som følge af menneskelige og systemmæssige fejl eller udefrakommende hændelser.
- **Fortrolighed** – At etablere mulighed for fortrolig behandling og opbevaring af data, hvor kun autoriserede brugere har adgang.

# Holdninger og principper

Informationssikkerhed i Billund Kommune implementeres efter følgende overordnede holdninger:

- Billund Kommune arbejder med informationssikkerhed for at underbygge kommunens troværdighed over for omverdenen, herunder samarbejdspartnere og borgere.
- Billund Kommune vedligeholder, understøtter og fastholder vidensniveauet hos alle medarbejdere for at understøtte sikker behandling af informationer i kommunens IT-systemer.
- Såfremt eksterne parter berøres af sikkerhedshændelser hos Billund Kommune, vil kommunen kommunikere ærligt og troværdigt over for berørte parter.

# Opfølgning

Billund Kommune måler, vurderer og følger op på informationssikkerhedsområdet ved at gennemføre jævnlige evalueringer:

- Opfølgning på vidensniveau inden for informationssikkerhedsområdet i kommunen.
- Gennemførelse af jævnlige evalueringer af informationssikkerheden.

# Godkendt

Informationssikkerhedspolitikken er godkendt af Økonomiudvalget den 21.08.2018. Den erstatter hermed tidligere udgivelser: Regulativ version 1.0, God adfærd version 1.0 og Kvik vejledning version 1.0.

# 1. Informationssikkerhedspolitik

## 1.1 Definition på informationssikkerhed i Billund Kommune

Informationssikkerhed defineres som de samlede foranstaltninger til at sikre fortrolighed, tilgængelighed og integritet. Det er med til at sikre, at det kun er godkendte systemer og medarbejdere der får adgang til personoplysninger i Billund Kommune.

Informationssikkerhedspolitikken skal offentliggøres og kommunikeres ud til alle medarbejdere. Den vil herefter være at finde på Kommunettet samt på www.billund.dk.

## 1.2 Vedligeholdelse af politikken

Informationssikkerhedspolitikken skal vedligeholdes af IT-chefen.

# 2. Organisering af informationssikkerhed

Økonomiudvalget og Direktionen har det overordnede ansvar for at sikre, at politikken for informationssikkerheden er synlig, koordineret og i overensstemmelse med Billund Kommunes mål.

### Sikkerhedsansvar for fagsystemer

Alle fagsystemer der kræver specialviden, færdighed eller erfaring skal identificeres, og der skal udpeges en systemejer (i Billund Kommune varetager områdecheferne rollen som systemejer). Disse systemejere har ansvaret for at sikre tilstrækkelig beskyttelse. Dette indebærer:

- Indhentning af databehandleraftaler (i dialog med kommunens Databeskyttelsesrådgiver)
- Adgangsstyring af systemer, herunder tildeling og fratagelse af rettigheder og adgange
- Løbende opdateringer af systemerne

### Sikring af fagsystemer

Fagsystemer skal sikres gennem korrekt tildeling af brugerprofiler for at hindre misbrug af disse. Der skal desuden være funktionsadskillelse i forhold til udviklings-, test- og driftsmiljøet. Dermed sikres det, at det ikke er den samme person der udvikler, tester og drifter.

### Beredskabsplaner

Ved brud på sikkerheden skal der være etableret en procedure for håndtering af bruddet og eventuelt kontakt med relevante myndigheder. Dette dokumenteres ved hjælp af beredskabsplaner for informationssikkerheden.

Der skal udarbejdes beredskabsplaner for alle kritiske IT-systemer. Ansvaret for udarbejdelsen ligger hos IT-afdelingen, dog i tæt samarbejde med systemejerne og kommunens Databeskyttelsesrådgiver.

# 3. Ledelse af informationssikkerhed

## 3.1 Ledelsesansvar

Det er ledelsens ansvar at alle medarbejdere:

- Er tilstrækkeligt informeret om deres roller og ansvar i forbindelse med informationssikkerheden.
- Er gjort bekendt med nødvendige retningslinjer, således at de kan leve op til kommunens informationssikkerhedspolitik.
- Er motiverede for at leve op til kommunens informationssikkerhedspolitik og retningslinjer.
- Modtager træning i kommunens informationssikkerhedspolitik og baggrundsviden omkring denne.
- Løbende modtager instruktioner i overholdelse af kommunens informationssikkerhedspolitik.

Alle nye medarbejdere skal hurtigst muligt introduceres for informationssikkerhedspolitikken.
Uddannelse skal ske i et samarbejde mellem den enkelte leder og Billund Kommunes Databeskyttelsesrådgiver (DPO).

## 3.2 Sanktioner ved overtrædelse af sikkerhedsretningslinjerne

Det er ledelsens ansvar, at sanktioner for brud på kommunens politikker, regler eller retningslinjer håndhæves konsekvent og i overensstemmelse med gældende lovgivning.

- Det er ikke tilladt at foretage uautoriseret afprøvning af sikkerheden.
- Det er ikke tilladt at forsøge at omgå sikkerhedsmekanismer.
- Hændelser hvor medarbejdere er involveret, skal håndteres konsekvent i overensstemmelse med gældende personalepolitik.
- Bevidste eller gentagne overtrædelser kan medføre disciplinære sanktioner.

# 4. Registrering og rettigheder

## 4.1 Ansvar for kommunens udstyr

### 4.1.1 Registrering af IT-udstyr

Det er IT-afdelingens ansvar, at alt IT-udstyr er registreret med ejer, bruger og placering. Der skal udarbejdes dokumentation over registreringen, som jævnligt skal holdes opdateret.

### 4.1.2 Sikkerhed omkring kommunens mobile enheder

IT-afdelingen skal sikre kommunens bærbare pc'er med antivirus og firewall.

Brugerne af iPads og mobiltelefoner er ansvarlige for at sikre disse med adgangskode efter gældende retningslinjer (se side 9), for at beskytte det data der opbevares og behandles på disse.

Mobile enheder må ikke efterlades uden opsyn i uaflåste rum

**Brug af privat udstyr**

Det er tilladt at koble privat udstyr op mod kommunens systemer, så længe kommunens sikkerhedsforanstaltninger ikke bliver omgået.

Medarbejderen forpligter sig til at overholde de samme regler, som gælder for øvrig brug af kommunens udstyr, herunder brugen af adgangskode. Billund Kommune er ikke erstatningspligtig for tyveri, bortkomst, skade eller tab af privat udstyr.

### 4.1.3 Fjern – og hjemmearbejdspladser

Ved fjern – og hjemmearbejdspladser skal der altid anvendes en krypteret forbindelse (VPN-forbindelse). Denne forbindelse oprettes automatisk når computeren får forbindelse til internettet.

## 4.2 Krav til adgangsstyring

### 4.2.1 Begrænset adgang til informationer

Adgang til IT-systemer og informationer for brugere og personer med supportfunktioner skal administreres efter princippet: *blokering af adgang til alt andet end det, som specifikt er tilladt.*

Brugere og medarbejdere med supportfunktioner må kun få adgang til systemfunktioner og informationer, hvis dette er forretningsmæssigt begrundet. Dette vil sige, hvis det er nødvendigt i udførelsen af deres arbejde.

### 4.2.2 Adgang og overvågning af netværk

Brugere skal godkendes ved hjælp af et certifikat, før der gives adgang til kommunens trådløse administrative netværk.

IT-afdelingen skal have den nødvendige viden og redskaber til overvågning af kommunens netværk, f.eks. til fejlretning og sporing af sikkerhedshændelser. IT-afdelingen er ligeledes ansvarlig for kontinuerligt at overvåge brugen og sikkerheden af kommunens netværksinfrastruktur.

## 4.3 Administration af brugeradgang

### 4.3.1 Tildeling af brugeradgang

IT-afdelingen bestemmer og tildeler brugerrettigheder på kommunens IT-systemer. IT-afdelingen skal samtidig vedligeholde en fortegnelse over, hvordan bruger-id eller rettigheder fjernes eller ændres ved ophør eller ændring af brugeres jobfunktion.

Systemejeren af et fagsystem bestemmer nødvendige brugerrettigheder for det specifikke fagsystem.

Ved ændringer af roller for medarbejderne skal rettigheder og privilegier revurderes. Dette gælder især for kritiske IT-systemer.

### 4.3.2 Brugerregistrering og -afmelding

Alle brugere skal have en unik identitet til personlig brug. Brugeridentiteten skal kunne spores til den person, der er ansvarlig for en given aktivitet. Der må ikke anvendes fælles adgangskoder eller brugerprofiler.

Alle brugerprofiler skal gennemgås mindst én gang årligt for at identificere inaktive profiler eller tilsvarende, der skal fjernes eller ændres.

Ved fratrædelse skal alle brugerprofiler og systemrettigheder for brugeren øjeblikkeligt nedlægges.

## 4.4 Adgangskoder

### 4.4.1 Krav til adgangskode

Billund Kommune har følgende krav til valg af adgangskode:

- Adgangskoden skal indeholde mindst 8 tegn.
- Det skal indeholde kombinationer fra mindst tre af følgende kategorier: Store bogstaver, små bogstaver, tal og specialtegn.
- Der må ikke anvendes samme kode som benyttes til private formål.

Alle adgangskoder udløber efter 90 dage. Ved behov for nulstilling af adgangskoden kan selvbetjeningsportalen *nemadgang.billund.dk* benyttes.

Din adgangskode er personligt og må ikke deles med andre.

### 4.4.2 Retningslinjer for midlertidige adgangskoder

IT-afdelingen skal etablere og vedligeholde en procedure for, hvordan en brugers identitet fastslås før en ny midlertidig adgangskode må udleveres.

Midlertidige adgangskoder skal være unikke, må ikke genbruges og skal opfylde de almindelige krav til adgangskoder. Ved brugeroprettelse eller nulstilling af adgangskode skal brugere tildeles en sikker midlertidig adgangskode, som derefter skal ændres.

# 5. Driftssikkerhed

## 5.1 Driftsprocedurer

IT-afdelingen er ansvarlig for drift og administration af fælles IT-systemer samt disses sikkerhed. Dette inkluderer efterlevelse af sikkerhedspolitikker, regler og procedurer.

### 5.1.1 Sikring af arbejdsstationer inden ibrugtagning

Alle arbejdsstationer skal installeres ved brug af fastlagte procedurer fra IT-afdelingen. Alle arbejdsstationer skal sikres inden brug. Minimum sikring inkluderer installation af seneste sikkerhedsrettelser for operativsystemet og et antivirusprogram.

### 5.1.2 Ændringsstyring

Ændringer skal planlægges og afprøves så vidt det er muligt, inden de sættes i drift. Der skal foretages test af driftsfunktionaliteten før ændringer gennemføres.

IT-afdelingen skal oprette og vedligeholde procedurer for ændringsstyring for alle software- og systemkonfigurationsændringer (inklusiv netværksudstyr).

**Sikkerhed i opgraderinger, ændringer og nyanskaffelser af IT-systemer**

Ved planlægning af dette skal sikkerhedsbetragtninger altid medtages i overvejelserne. IT-sikkerhedskrav skal tages i betragtning ved design, testning, implementering og opgradering af IT-systemer samt ved systemændringer.

Kommunens Databeskyttelsesrådgiver (DPO) skal altid medtages i ovennævnte tilfælde.

## 5.2 Antivirusprogrammer

IT-afdelingen skal sikre, at der er installeret aktive antivirus-produkter på samtlige computere i kommunen. Programmerne skal jævnligt opdateres.

IT-afdelingen skal ligeledes udføre en regelmæssig scanning og gennemgang af malwarebeskyttede systemer for at sikre, at alle systemer er beskyttet og har opdaterede signaturfiler.

## 5.3 Logning og overvågning

IT-afdelingen skal logge væsentlige brugeraktiviteter på kommunens systemer. Der skal blandt andet føres log over forsøg på adgang, så uautoriseret aktivitet kan spores.

Alle sikkerhedshændelser skal logges og opbevares i en fastlagt periode.

## 5.4 Softwareopdatering

IT-afdelingen skal holde sig informeret om systemrettelser til IT-systemer der anvendes i kommunen og snarest installere disse på alle computere, f.eks. servere og arbejdsstationer, når det vurderes, at rettelserne har positiv indflydelse på den samlede sikkerhed.

## 5.5 Sårbarhedsstyring

### 5.5.1 Opdateringer

Når større opdateringer (f.eks. service-packs) er gjort tilgængelige fra leverandører, skal IT-afdelingen vurdere om disse skal installeres. Større opdateringer skal, så vidt det er muligt, testes i et testmiljø inden opdateringerne installeres i produktionsmiljøet.

### 5.5.2 Styring af antivirus

IT-afdelingen skal kunne styre antivirus på alle systemer centralt, og dermed overvåge om alle antivirusprogrammer er aktivt kørende, styre tvungen opdatering, scanning, oprydning og generering af opfølgningslog.

### 5.5.3 Administration af softwarelicenser

Registrering af software licenser sker gennem IT-afdelingen. Det er IT-chefens overordnede ansvar, at der er et tilstrækkeligt antal licenser.

## 5.6 Revision

Følgende retningslinjer skal overholdes i forbindelse med revision:

- De personer der udfører revisionen, skal være uafhængige af det reviderede område.
- Hvis revisionen nødvendiggør mere end læseadgang, må dette kun tillades på kopier af de berørte filer, der skal slettes efter brug.
- Revisionskrav af systemer i drift skal planlægges omhyggeligt og aftales med de involverede, for at minimere risikoen for forstyrrelser af kommunens forretningsaktiviteter.

# 6. Fysisk sikring

## 6.1 Sikre områder

### 6.1.1 Overvågning i sikre områder

Videokameraer, som benyttes til overvågning af sikre områder, skal placeres inden for det sikre område eller på anden vis beskyttes mod modifikationer og deaktivering. Videooptagelser fra sikre områder skal opbevares i mindst én måned. Adgangen til de sikre områder skal beskyttes med kodelås, og koden må kun kendes af sikkerhedsgodkendte medarbejdere.

**Gæsters adgang**
Gæster må ikke lukkes ind i sikrede områder, medmindre tilladelse til dette er indhentet af den relevante ansvarlige.

**Indbrudsalarmer**
Kommunen skal anvende passende alarmsystemer på samtlige bygninger og lokaler.

### 6.1.2 Beskyttelse af serverrum

**Miljømæssig sikring af serverrum**
Serverrum, krydsfelter og tilsvarende områder skal på forsvarlig vis sikres mod miljømæssige hændelser som brand, vand, eksplosion og tilsvarende påvirkninger.

**Brandsikring**
Serverrum må ikke benyttes som lager for brændbare materialer. Rummet skal sikres med veldimensioneret brandslukningsudstyr.

## 6.2 Udstyr

### 6.2.1 Placering og beskyttelse af udstyr

**Adgang til serverrum og hovedkrydsfelter**
Adgang til serverrum og hovedkrydsfelter tillades kun med sikkerhedsgodkendelse eller ved overvåget adgang af medarbejdere fra IT-afdelingen.
Alle hovedkrydsfelter og lignende teknikrum skal være aflåste.

**Spisning og rygning**
Der må ikke spises, drikkes eller ryges i nærheden af forretningskritisk udstyr og i serverrum.

### 6.2.2 Køling og nødstrømsanlæg

Serverrum skal sikres med veldimensionerede airconditionanlæg. Alle server-systemer skal beskyttes med nødstrømsanlæg for at sikre hurtig og korrekt system-nedlukning i tilfælde af strømudfald.

### 6.2.3 Sikring af kabler

Kabler til datakommunikation skal beskyttes mod uautoriserede indgreb og skader. Faste kabler og udstyr skal mærkes klart og entydigt.

### 6.2.4 Vedligeholdelse af IT-udstyr

IT-afdelingen er ansvarlig for, at der føres log over alle fejl og mangler samt reparationer og forbyggende vedligeholdelse af udstyr. Kun godkendte leverandører må udføre reparationer og vedligeholdelse af udstyr.

### 6.2.5 Sikker bortskaffelse eller genbrug af IT-udstyr

Når IT-udstyr bortskaffes eller genbruges, skal personoplysninger og licensbelagte systemer fjernes eller overskrives.

### 6.2.6 Placering af IT-udstyr

Udstyr skal placeres eller beskyttes, så risikoen for skader og uautoriseret adgang minimeres. Udstyr der benyttes til at behandle personoplysninger, skal placeres så informationerne ikke kan ses af uvedkommende.

### 6.2.7 Pauseskærm og fysiske dokumenter

**Brug af pauseskærm**
Adgangskodebeskyttet skærmlås skal slås til hver gang skrivebordet forlades. Dette sikrer, at uvedkommende ikke får adgang til computeren og de data der er på den.

**Opbevaring af fysiske dokumenter**
Dokumenter med personoplysninger må ikke ligge med forsiden opad, når skrivebordet forlades i løbet af arbejdsdagen. Skrivebordet skal ryddes for disse dokumenter ved arbejdsdagens afslutning. Dokumenterne skal gemmes forsvarligt i et aflåst skab.

# 7. Kommunikationssikkerhed

## 7.1 Krav til firewall

For at kunne opdage og undgå web-baserede angreb, skal der installeres en applikations-firewall foran alle applikationer, der kan tilgås fra internettet. Firewallen skal blokere al ind- og udgående trafik, som ikke er specifikt tilladt.

Alle servere skal benytte firewalls for at sikre, at der kun gives adgang til nødvendige services.

## 7.2 Anvendelse af sociale netværk og cloudløsninger

Sociale netværk må gerne anvendes fra kommunens IT-systemer. Brugere af sociale netværk skal dog være specielt opmærksomme på at:

- De sociale netværk der bruges kan registrere og gemme oplysninger om dig, herunder hvilke informationer du søger og bruger.
- Informationer der lægges ud på et socialt netværk kan højest sandsynligt ikke trækkes tilbage igen.
- Du kan komme ud for, at nogen forsøger at franarre dig dine bruger-id'er og/eller dine adgangskoder
- Du har selv et arbejdsmæssigt ansvar for at kontrollere dit tidsforbrug på sociale netværk.
- Din brug af sociale netværk må ikke genere almindelig drift og brug af kommunens IT-systemer.

HUSK: Personoplysninger må aldrig deles på sociale netværk!

Som led i den almindelige netværksovervågning bliver netværkstrafik til sociale netværk også overvåget. Browsere på kommunens pc'er gemmer blandt andet information om din brug af sociale netværk, og du må forvente, at kommunen kan få adgang til denne information.

### Anvendelse af cloudløsninger

Cloud-løsninger må anvendes, hvis der er et arbejdsmæssigt behov, og hvis der ikke er væsentlige sikkerhedsmæssige risici forbundet med løsningen.

Det er dog ikke tilladt at dele eller opbevare personoplysninger i 'skyen', ved brug af cloud-serviceudbydere som eksempelvis Dropbox. Personoplysninger skal altid opbevares i et fagsystem eller kommunens ESDH-system.

## 7.3 Data

### 7.3.1 Opbevaring og bortskaffelse af data

Elektroniske kopier af dokumenter med personoplysninger (f.eks. indscannede dokumenter og faxer), må kun behandles og lagres på passende IT-udstyr.

Der skal foreligge en procedure for håndtering af opbevaringstiden for data, da data kun må opbevares i det tidsrum der er nødvendigt.

### 7.3.2 Elektroniske meddelelser

**Brug af e-mail**

- E-mails der indeholder personoplysninger skal behandles i overensstemmelse med persondataloven.
- E-mails med følsomt indhold skal krypteres med godkendt software. Dette gælder især for klassificeret, fortrolig eller følsom persondata, der sendes over internettet.

**Sagsbehandling og journalisering af e-mail**

- Modtagne og afsendte e-mails skal håndteres på samme måde som traditionel post og fax.
- Modtagne og afsendte e-mails med personoplysninger skal journaliseres i kommunens ESDH system eller et fagsystem og herefter slettes fra mailen.

**Privat brug af e-mail**

Medarbejdere i Billund Kommune må anvende mailsystemerne til personligt brug i begrænset omfang, hvis dette ikke har indflydelse på kommunens drift og sikkerhed i øvrigt. Medarbejderne skal markere private e-mails med teksten 'privat' i emnefeltet, eller alternativt gemme private mails i en folder, hvor teksten 'privat' indgår i folderens navn.

Billund Kommune forbeholder sig dog ret til at skaffe sig adgang til data og e-mails fra medarbejdere, hvis dette sker af drifts- eller sikkerhedshensyn. Kommunen vil så vidt muligt forsøge at undgå at åbne eventuel privat e-mail korrespondance.

HUSK: Al mailtrafik må betragtes som kommunens ejendom.

# 8. Leverandørforhold

Relevante sikkerhedskrav skal identificeres og aftales med leverandører der har adgang til, behandler eller opbevarer data for kommunen. En aftale med en leverandør som har adgang til dette skal indeholde:

- Formålet med behandlingen
- Varigheden af behandlingen
- Behandlingens karakter
- Typen af personoplysninger
- Den dataansvarliges forpligtelser
- Databehandlerens pligter i forhold til at varetage opgaven
- Retten til at føre revision

Dette skal sammensættes i en databehandleraftale. En databehandleraftale skal klart og tydeligt afklare hvem der er dataansvarlig og hvem der er databehandler.

# 9. Databeskyttelse

## 9.1 Data og personoplysninger

### Klassifikation af data

Alle ansatte i Billund Kommune skal modtage instruktioner om, hvordan data og dokumenter klassificeres. Ansvaret for udarbejdelse af disse instrukser ligger hos IT-afdelingen.

Informationer og data skal klassificeres som følger:

- **Offentligt** – Materiale der frit må udleveres til offentligheden.
- **Personhenførbart** – Data der er relateret til et individ, f.eks. en borger eller en medarbejder.

### Opbevaring og behandling af personoplysninger

Lov om behandling af personoplysninger gælder ved enhver opbevaring og behandling af persondata.

Der må ikke behandles personoplysninger på privat pc, medmindre kryptering anvendes og bekendtgørelse nr. 528 om personoplysninger overholdes.

## 9.2 Beskyttelse af personoplysninger

### Principper for behandling af personoplysninger

Kommunen skal sikre at personoplysninger behandles loyalt, lovligt og på en transparent måde for den registrerede.

Personoplysninger skal være relevante, tilstrækkelige og må kun bruges til det fastsatte formål.

Det må ikke opbevares længere end nødvendigt.

### Lovlig behandling af personoplysninger

Behandling af personoplysninger må kun ske hvis der er behandlingsgrundlag ved hjemmel i lov, eller hvis den registrerede har givet sit samtykke.

### Ret til indsigt i personoplysninger

Borgeren har til enhver tid ret til at anmode kommunen om, at få indsigt i hvilke personoplysninger der behandles om vedkommende. Kommunen skal sikre, at det er muligt at kunne udlevere alle oplysninger i et klart og letforståeligt sprog, som er tilpasset borgeren.

### Udpegning af Databeskyttelsesrådgiver (DPO)

Billund Kommune skal udpege en Databeskyttelsesrådgiver (DPO), som blandt andet skal kunne rådgive kommunens ansatte og borgere om databeskyttelse.

# 10. Styring af informationssikkerhedsbrud

## 10.1 Styring af informationssikkerhedsbrud og forbedringer

### 10.1.1 Ansvar og procedurer

Direktionen har det overordnede ansvar for håndtering af informationssikkerhedsbrud. IT-afdelingen er ansvarlig for at fastlægge forretningsgange, der sikrer en hurtig, effektiv og metodisk håndtering af disse sikkerhedsbrud. Denne procedure skal dokumenteres i en beredskabsplan for informationssikkerhed.

Der skal etableres en proces der sikrer, at beredskabsplanen løbende evalueres og tilpasses i overensstemmelse med indsamlet erfaring og generel udvikling.

**Rapportering af formodede sikkerhedshændelser**
Den enkelte medarbejder skal rapportere om sikkerhedshændelser for informationssikkerhed, der kan påvirke, eller formodes at ville påvirke kommunens informationer, til sin nærmeste leder.

Det er herefter lederens ansvar, at sikkerhedshændelsen bliver indrapporteret til Billund Kommunes Databeskyttelsesrådgiver (DPO). Kontaktoplysninger på vedkommende vil fremgå af Kommunettet samt på www.billund.dk.

Årsager til sikkerhedshændelser kan omfatte:

- Brud på fortrolighed, integritet og tilgængelighed
- Menneskelige fejl
- Brud på fysisk sikkerhed
- Manglende efterlevelse af politikker eller procedurer
- Brud på logisk adgang
- Sikkerhedshændelser ved brug af privat udstyr

**Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden**
Hvis der sker et brud på persondatasikkerheden, skal kommunen senest 72 timer efter foretage anmeldelse til Datatilsynet. Det er kommunens Databeskyttelsesrådgiver (DPO) der er kontaktperson til Datatilsynet, og dermed også vedkommende der anmelder det.

Billund Kommune er forpligtet til at indberette enhver observeret sikkerhedshændelse eller mistanke herom internt. Det er derefter DPO´en der vurderer, om hændelsen skal indberettes til Datatilsynet.

Alle sikkerhedshændelser skal dokumenteres, både brud på informationssikkerheden og brud på persondatasikkerheden.

**Sikkerhedshændelser hos leverandør**
Leverandøren registrerer sikkerhedshændelser (f.eks. brud på fortrolighed, tilgængelighed eller integritet) i eget system. Leverandøren skal underrette kommunens IT-chef, hvis der sker en sikkerhedshændelse.

### 10.1.2 Rapportering af informationssikkerhedssvagheder

Hvis der observeres virus eller mistanke om virus, skal det omgående rapporteres til IT-afdelingen.

Brugere der observerer programfejl skal rapportere dette til IT-afdelingen.

### 10.1.3 Kontrol og opfølgning på sikkerhedsbrud

Brud på sikkerheden, uautoriseret adgang og forsøg på uautoriseret adgang til systemer, informationer og data skal logges og registreres af IT-afdelingen.

## 11. Evaluering

Mindst én gang om året skal der udføres uddybende sikkerhedstest af sikkerhedsniveauet i internt netværksudstyr og servere.

Det skal samtidig sikres, at de ansatte i Billund Kommune løbende får testet deres viden om kommunens informationssikkerhed.