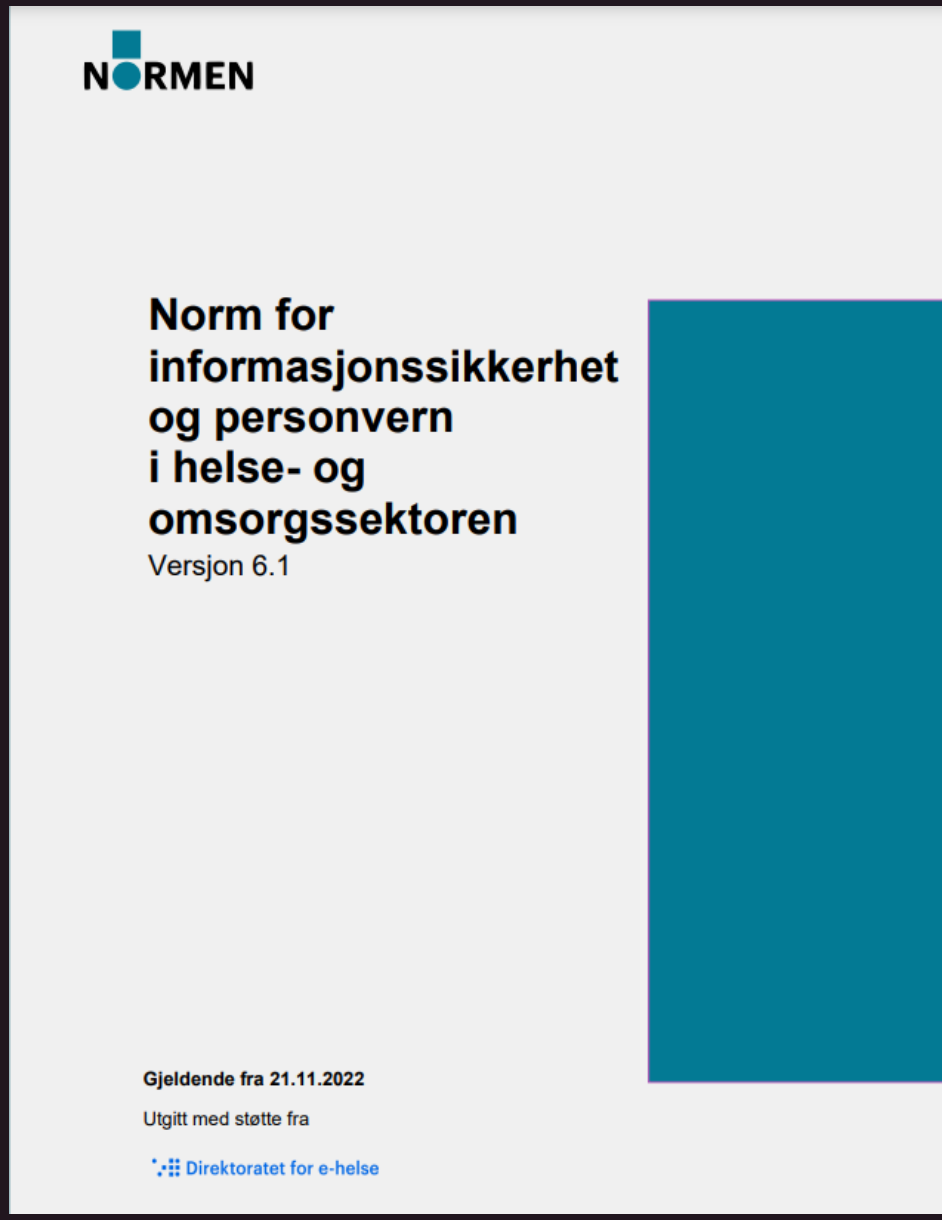
NORMEN

Et utvalg av Normens krav til informasjonssikkerhet

Introkurs Normen
10. januar 2024



Hvor i Normen er vi nå?

Kapittel 1: Om Normen

Kapittel 2: Ledelse og ansvar

Kapittel 3: Risikostyring

Kapittel 4: Grunnleggende krav til behandling av helse- og personopplysninger

Kapittel 5: Krav til informasjonssikkerhet

Vedlegg

Kapittel 5 – Krav til informasjonssikkerhet

1. Ansatte, kompetanse og holdningsskapende arbeid
2. Tilgangsstyring
3. Fysisk sikkerhet og håndtering av utstyr
4. Sikker IT-drift
5. Kommunikasjonssikkerhet
6. Digital kommunikasjon til den registrerte
7. Leverandørforhold og avtaler
8. Håndtering av informasjonssikkerhetsbrudd
9. Nødrutiner

nrk Logg inn

Troms og Finnmark Tips oss Se Nordnytt Hør P1 Finnmark Hør P1 Troms Hør Ettermiddagssending i Troms

Datainnbrudd mot ambulanser på flere sykehus i Nord-Norge: – Et alvorlig datainnbrudd

Det er kommunikasjonssystemet mellom AMK-sentralen og luftambulanser og ambulansene som er rammet.

Skadevaren er oppdaget i et IKT-program som benyttes i ambulanser og luftambulansehelikoptre i Helgelandssykehuset, Nordlandssykehuset, Universitetssykehuset Nord-Norge og Finnmarkssykehuset.
FOTO: ESKIL MEHREN / NRK

Ida Louise Rostad
Journalist
Torgeir Skeie
Journalist
Rune N. Andreassen
Journalist
Gisle Forland
Journalist
Linda Pedersen
Journalist

Vi rapporterer fra Tromsø

Publisert 8. apr. kl. 14:06
Oppdatert 8. apr. kl. 18:58

Datatilsynet roper varsko om it-sikkerhet på sykehusene

Datatilsynet frykter at nedskjæringene ved landets sykehus vil ramme IT-sikkerheten og personvernet til pasientene. Nå ber de om øremerkede midler.

Norske sykehus trues av russiske hackergrupper

Russiske hackergrupper truer lørdag sykehus og helseinstitusjoner i Norge og flere vestlige land.

Sikkerhet på medisinsk teknisk utstyr bekymrer

Teknologien som skal ta vare på helsen vår er en potensiell sikkerhetsbombe i helsesektoren.

Gjennomsnittlig løsepengekrav nærmer seg en million dollar

Løsepengeutbetalingene som følge av ransomware øker. I snitt utbetales det nå 925.162 dollar, ifølge Palo Alto Networks forskningsavdeling Unit 42.

Henning Meese

PUBLISERT Onsdag 08. juni 2022 - 12:26

Frykter for sikkerheten i norske kommuner

Norske kommuner sliter med å rekruttere og holde på sikkerhetsfolk. Friske midler fra Stortinget og mer samarbeid på tvers skal gjøre oss tryggere.

PLUSS E-AVIS TIPS OSS

Helse-apper på eget ansvar?

Helsedata har mer verdi enn finansielle data. Dette bør være en tankevekker.

Dagbladet avslører:

Russere angrep vannsystemet i Drammen

Kort tid etter at hackere forsøkte å forgifte drikkevannet til 15 000 i USA, brøt russiske hackere seg inn på vannsystemet til Drammen kommune. Da gikk alarmen.

Forventer sterk vekst i cyberangrep drevet av AI i 2024

Cybersikkerhetsselskapet Trend Micro retter en kraftig advarsel mot de transformative og potensielt farlige implikasjonene av generativ kunstig intelligens (GenAI) i cybersikkerhetslandskapet.

5.1 Ansatte, kompetanse og holdningsskapende arbeid

- Kontinuerlig opplæring i taushetsplikt, informasjonssikkerhet og personvern
  - Bør følges opp og dokumenteres
- Taushetserklæring
- Instruks for informasjonssikkerhet og personvern
- Retningslinjer for privat bruk av informasjonssystemer og utstyr
- Opphør av arbeidsforhold
  - Tilbakelevering av ansattkort og medier
  - Sperre tilganger
  - Rutiner for opprydding i informasjon brukeren kan ha lagret

HELSE HELSE NORD-TRØNDELAG LEVANGER NAMSOS DATATILSYNET

SIKKERHET

Populær passordtjeneste etter hacking: Angriperne fikk tilgang til passordhvelv

Titusenvis av pasienter rammet av datalekkasje

Finsk hacker stjal pasientjournaler – krevde løsepenger i kryptovaluta

Aleksanteri Julius Kivimäki er siktet for datainnbruddet hos det finske psykoterapisenteret Vastaamo i 2018. Nå er han pågrepet etter å ha vært på rømmen i Frankrike.

Dine pasientdata skal sendes til amerikansk sky – Datatilsynet advarer

I løpet av noen uker skal Helse Sør-Øst ta i bruk en skytjeneste for å håndtere nordmenns pasientdata. Datatilsynet advarer om at USA ikke er ansett som et trygt land å sende slike opplysninger til, og ber dem sette på bremsen.

Legetjeneste delte med Facebook hva brukerne tittet på

Ereksjonssvikt, bakteriell vaginose, hårtap, og klamydia. Legetjenestene Maja og Hans delte med Facebook hva brukerne gjorde på nettsidene.

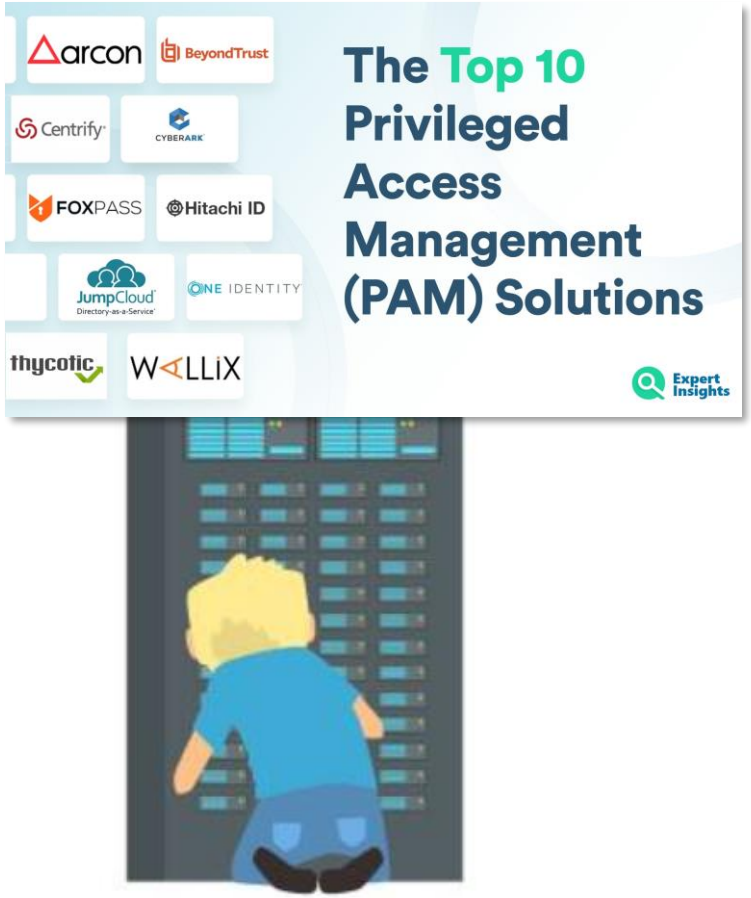
NORMEN

5.2 Tilgangsstyring

- All tilgang skal baseres på tildelt autorisasjon i fagsystemet og **tjenstlig behov**
- Autorisasjon skal skille rettigheter for å lese, registrere, redigere, rette, slette og sperre helse- og personopplysninger
- Autorisasjon skal være **tidsbegrenset**
- **Fellesbruker** for tilgang til helse- og personopplysninger er **ikke tillatt**
- All tildeling av autorisasjon skal registreres i et **autorisasjonsregister**

Tilgang for teknisk personell

- Tilgangsstyring skal etableres for **administrator- og systembrukere**
- Bruker med administratortilganger skal benytte **personlig separat brukerkonto for administratoroppgaver**
- Driftspersonell skal ha **personlige brukerkontoer** for oppgaver som **ikke krever administratortilganger**
- Det skal etableres tiltak slik at mulig **misbruk** skal kunne avdekkes
  - For eksempel sterk autentisering, logging, kontroller



Autorisasjonsregister

- Virksomheten skal opprette et **autorisasjonsregister**
- Registeret skal som minimum inneholde:
  - **hvem** som er tildelt autorisasjon
  - til hvilken **rolle** autorisasjonen er tildelt (om rollen benyttes i virksomheten)
  - **formålet** med autorisasjonen
  - **tidspunkt** for når autorisasjonen ble gitt og eventuelt tilbakekalt
  - informasjon om hvilken **virksomhet** den autoriserte er knyttet til
  - helsepersonells autorisasjon for tilgang til helseopplysninger i annen virksomhet
    - kun om tilgang til helseopplysninger i annen virksomhet er tatt i bruk

Autentisering

- Den autoriserte skal bekrefte sin identitet på en sikker måte
  - Sikker måte må besluttes på grunnlag av en risikovurdering
  - Nivå ”Betydelig” eller ”Høyt” (les mer hos Nasjonal kommunikasjonsmyndighet)
- Ikke fellesbruker for tilgang til helse- og personopplysninger
- Alle standardpassord (fabrikkinnstillinger) på systemer og utstyr skal endres
- Ved bruk av trådløse nettverk skal den autoriserte brukeren autentiseres med sikker autentiseringsløsning
- Benyttes roller så skal ulike roller identifiseres, og ved behov gis ny autentisering

Med «sikker autentiseringsløsning» menes i Normen en autentiseringsløsning som for eksempel er basert på personlig kvalifisert sertifikat, eller annen autentiseringsløsning som gjennom en risikovurdering viser at den har tilstrekkelig sikkerhet

Oppdaga at 185 tilsette hadde lese journalen til mannen – kommunen nektar å ha snoka

Kona måtte gå heilt til retten for å få journalen. Då ho oppdaga kor mange som allereie hadde sett den, fekk ho sjokk.

Juss og samfunn

Helseansatt oppsagt etter journalsnoking – kan ha pågått i flere år

– Det ser ut til at vedkommende har slått opp i journaler over lengre tid, sier politifullmektig.

Janne Cecilie fikk sjokk da hun skjønte at sjefen hadde snoket i helseopplysningene hennes

FriFagbevegelse.no | 11. januar 7:00 | 1808 ord | 1 deling

Ansatt (69) ved Ullevål sykehus tatt for årevis med snoking i pasientjournal. Mister likevel ikke jobben

I årevis snoket den helseansatte ved barneklinikken på Ullevål sykehus i en pasientjournal hun ikke har lov til å se. Flere titalls ulovlige oppslag i journalen ble avslørt av digitale spor. Likevel mister ikke kvinnen jobben.

Arnsten Linstad
JOURNALIST

PUBLISERT Mandag 25. april 2022 - 23:17

Sykehusansatt fikk sparken etter journalsnoking

En ansatt i Helse Bergen skal urettmessig ha slått opp i journaler i lengre tid. Nå har vedkommende fått sparken.

(©NTB)
Publisert: 2022-06-17 — 08.51

«Snoking» i pasientjournalar

Fylkesmannen har hatt fleire tilsynssaker som gjeld såkalla «snoking» i pasientjournalar, det vil seie at helsepersonell utan lov gjer seg kjent med opplysningar i ein pasientjournal.

NORMEN

Kontroll av tilgang og tildelte autorisasjoner

- **Jevnlig** kontroll av hvem som har hatt tilgang
- Gjennomgang og kontroll av tilgangsstyring, herunder **tildelte autorisasjoner**, skal foretas av den enkelte leder:
  - ved organisasjonsendringer, overflytting av personell til annen enhet/avdeling eller endring av arbeidsområde
  - minimum årlig (gjerne i forbindelse med sikkerhetsrevisjon)
  - ved sikkerhetsbrudd - for det som blir berørt av bruddet
- Varsling til ledelsen ved mistanke om urettmessig tilgang
- Misbruk av selvautorisering skal følges opp som avvik
- Dersom kontrollen viser at det har skjedd en urettmessig tilgang, skal dette behandles som et avvik

Kontroll av:

- **Hvem som har hatt tilgang**
- **Tildelte autorisasjoner**
  - **F.eks. brukere som har sluttet**

Logging (1)

- Hva skal logges?
  - Autorisert bruk, selvautorisering, system- og administratorbruk
  - Endring av konfigurasjon og programvare, sikkerhetshendelser
  - Forsøk på uautorisert bruk
- Minimum innhold i logger
  - Identiteten til den som har lest, rettet, registrert, endret og/eller slettet opplysninger
  - Organisatorisk tilhørighet, grunnlag og tidsperiode for tilgjengeliggjøringen
- Andre krav
  - Rutiner for å kunne sammenholde loggene med autorisasjonsregister
  - Logger og autorisasjonsregister skal sikres mot endring og sletting
  - Logger skal ha korrekt tidsstempel
  - Logger som genereres ved ytelse av helsehjelp skal lagres til det ikke antas å være bruk for dem
  - Logger av sikkerhetsmessig betydning bør oppbevares så lenge som nødvendig for å oppnå formålet

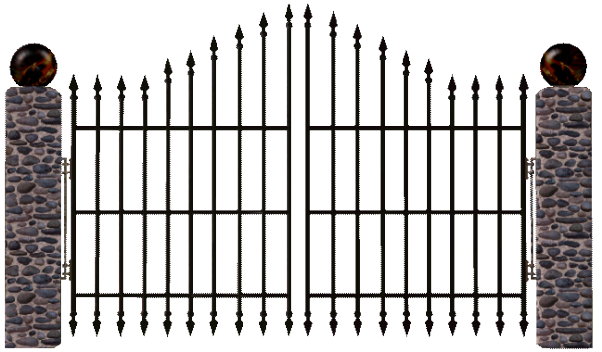
NORMEN

Logging (2)

- Loggene skal enkelt kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd
- Det skal etableres rutiner for å analysere loggene slik at hendelser oppdages før de får alvorlige konsekvenser – proaktiv analyse av logger
  - Dersom brudd avdekkes – håndter som avvik
- Fra kap. 4.2.3 Innsyn:
  - Virksomheten skal sikre at den registrerte kan få innsyn i opplysninger registrert om seg selv. Dette innsynet **gjelder også loggen** over hvem, og fra hvilken virksomhet, som har tilegnet seg hvilke opplysninger, og på hvilket tidspunkt

Kap. 5.3 Fysisk sikkerhet og håndtering av utstyr

- Sikkerhetstiltak skal hindre at uautoriserte får tilgang til helse- og personopplysninger
- Det skal etableres rutine for administrasjon av nøkler/adgangskort i adgangskontrollsystemet
- Adgangskontroll av lokaler med utstyr (husk medisinsk utstyr)
- Utstyret sikres mot misbruk eller uautorisert innsyn
- Hindre at annet enn autorisert personell får adgang til infrastruktur
- Alle lagringsmedier skal slettes forsvarlig når de tas ut av bruk
- Risikovurdering og rutiner før mobilt utstyr og hjemmekontor tas i bruk
- Helse- og personopplysninger skal bare lagres lokalt på utstyret når dette er nødvendig ut fra tjenstlig behov, og skal alltid lagres kryptert



Her skal legen ha brent over 500 kilo med pasientjournaler

Sensitive person-opplysninger lå strødd

Titusenvis av pasienter rammet av datalekkasje

Fant pasientlister med helseopplysninger

Glemt på do og i P-hus

Festet innlegg

Ukraina: 127 helseinstitusjoner ødelagt

i dag kl 12:19 av NTB DEL

Ruinene av et psykiatrisk sykehus etter et russisk angrep i Kramatorsk i regionen Donetsk i begynnelsen av august. Foto: Kostiantyn Liberov / AP / NTB

127 helseinstitusjoner er blitt ødelagt siden Russland begynte invasjonen av Ukraina, ifølge helsedepartementet i landet. 826 andre skal ha blitt påført skader.

Mistet journal med pasientopplysninger på McDonald´s

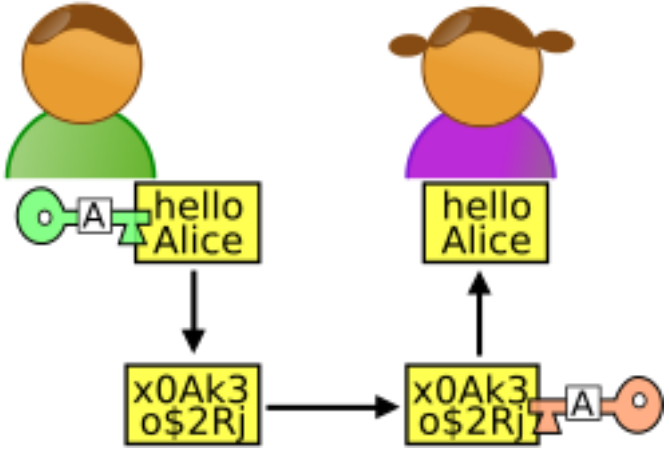
En ambulansearbeider mistet et dokument med pasientopplysninger på en McDonald´s-restaurant i Sarpsborg.

Publisert 11. aug. 2022 kl. 12:46

NORMEN

Kryptering

- Tekniske tiltak skal etableres slik at all kommunikasjon av helse- og personopplysninger utenfor virksomhetens kontroll krypteres
- Kryptering og dekryptering mellom kommunikasjonspunkter i infrastrukturen skal gjøres i godkjent utstyr virksomheten har kontroll med
  - Kontrollen kan ivaretas gjennom avtale
- All kommunikasjon, enten dette skjer ved hjelp av trådløst samband eller ved hjelp av linjer, skal sikres ved kryptering
- Kryptering av lagrede helse- og personopplysninger kan vurderes som et sikkerhetstiltak



Sikkerhet på medisinsk teknisk utstyr bekymrer

Teknologien som skal ta vare på helsen vår er en potensiell sikkerhetsbombe i helsesektoren.

Anders Løvøy

PUBLISERT Tirsdag 21. februar 2023 - 10:47

Ikke forberedt på langvarig IKT-STOPP

Bioingeniøren | 10. des. 2021 | side 14 - 17 | 1304 ord

Populære helse-apper har alvorlige sikkerhetsmangler

– Datahøsting-bonanza. Slik beskriver Mozilla flere apper som markedsføres som hjelp til mindfulness og bedre psykisk helse.

Små lege- og tannlegekontor betaler løsepenger etter hacking

Sensitive pasientdata på avveie er marerittet små lege- og tannlegekontorer bør sikre seg mot, mener lederne i NFA og Tannlegeforeningen.

Kjersti Flugstad Eriksen
JOURNALIST

PUBLISERT Tirsdag 14. februar 2023 - 06:00

Hvert fjerde helseforetak måtte stoppe driften etter løsepengevirusangrep

En undersøkelse viser at flertallet av helseforetakene innrømmer å ha blitt utsatt for løsepengevirus i løpet av de siste tre årene.

1898 pasientar fekk feil diagnose i journalen: – Det er forferdeleg ugreitt

Nær 2000 sjukehuspasientar i Noreg har fått ført opp feil diagnose i journalen sin. Dette kunne i verste fall ha ført til feilbehandling, ifølge Helsetilsynet.

Dokumenterer 8

Nytt datasystem til 4 milliarder ble aldri testet. Førte til kaos på landets fjerde største sykehus.

5.4 Sikker IT-drift

- Konfigurasjonskontroll
  - Det er en forutsetning at virksomheten har **oversikt** over dataflyt, datakommunikasjon og integrasjoner og kontroll på alt eget utstyr og programvare som benyttes i behandlingen av helse- og personopplysninger
  - Se også Kap. 3.3 oversikt over IKT-systemer, infrastruktur m.m

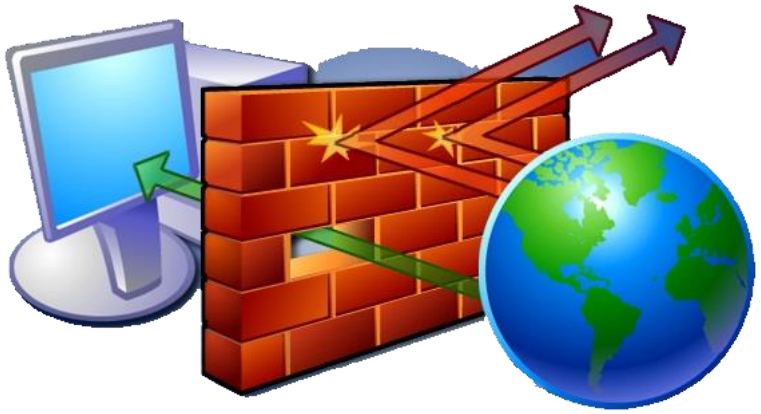
- Endringsstyring
  - Alle **endringer** med betydning for informasjonssikkerheten i organisasjon, informasjonssystem og infrastruktur skal **forankres** på relevant ledernivå

- Sikkerhetskopiering

- Styring og håndtering av tekniske sårbarheter
  - Virksomheten skal ha rutine for å **skaffe seg informasjon om tekniske sårbarheter** i utstyr og programvare.
  - Også rutiner for bl.a. hvordan virksomheten skal **reagere og varsle** om sårbarheter

5.5 Kommunikasjonssikkerhet

- Krav for nettverkssikkerheten skal defineres og dokumenteres
  - Tiltakene skal være basert på risikovurdering
- Ved tilkobling til eksterne nett skal tiltak sikre at eksplisitt angitt tillatt trafikk kan passere utenfra og inn eller motsatt, og at annen trafikk stoppes
  - Det skal være minst to uavhengige tekniske tiltak slik at personer utenfor virksomheten ikke skal kunne få uautorisert tilgang, endre eller slette opplysninger
- Det skal avtales klare ansvarsforhold mellom avsender, mottaker og eventuell meldingsformidler
  - Alle avtaler skal være skriftlige



5.4.6 Sikkerhetsrevisjon
5.8 Håndtering av informasjonssikkerhetsbrudd

- Formålet med sikkerhetsrevisjon er å gjennomføre kontrollaktiviteter og kvalitetssikring av etablerte tiltak og fastsatte rutiner
- Det skal foreligge en godkjent plan for sikkerhetsrevisjoner
- Virksomhetens ledelse skal følge opp at sikkerheten ivaretas ved jevnlige og **minimum årlige sikkerhetsrevisjoner**
- Uønskede hendelser (f.eks. brudd på rutiner, personvernet eller informasjonssikkerheten) skal behandles som **avvik**.
  Avvik skal behandles for å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse
- Dersom avviket er et **brudd på personopplysningssikkerheten** og har eller vil føre til middels eller høy risiko for den registrerte, skal avviket rapporteres til **Datatilsynet** innen 72 timer, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter
- Dersom det er sannsynlig at avviket har eller vil føre til høy risiko for **den registrerte**, skal virksomheten underrette vedkommende
- **Alvorlig svikt i informasjonssystemer** kan være meldepliktige til **Statens Helsetilsyn**

Hackerne tok samtlige systemer som løsepengergissel

Angrepet av hackere – hele kommunen rammet

Dataangrepet på Østre Toten kommune har lammet nærmest hele kommunen. – Over på penn og papir, sier ordfører.

22

Arbeidsliv

Hvert fjerde helseforetak måtte stoppe driften etter løsepengevirusangrep

En undersøkelse viser at flertallet av helseforetakene innrømmer å ha blitt utsatt for løsepengevirus i løpet av de siste tre årene.

NORMEN

Nettverk var nede på Ålesund sjukehus

Ålesund sjukehus sette i verk nødrutinar og krisestab etter at alt av nettverk ved sjukehuset var nede måndag kveld.

Dagsavisen

Offentlig sektor er et lukrativt mål for digital mafia

Dagsavisen | 29. des. 2021 | side 29 | 580 ord

Ikke forberedt på langvarig IKT-STOPP

Bioingeniøren | 10. des. 2021 | side 14 - 17 | 1304 ord

5.9 Nødrutiner

- Nødvendige helse- og personopplysninger skal være tilgjengelige
- Konsekvenser av bortfall skal kartlegges
- Systemer skal klassifiseres
  - Inkludert hvilke andre systemer og hvilken infrastruktur de klassifiserte systemene er avhengige av
  - For hver klassifisering skal ledelsen beslutte akseptabel risiko for tilgjengelighet. Som minimum skal det fastsettes maksimal avbruddstid
- Virksomheten skal etablere nødrutiner
  - Alternativ drift uten bruk av informasjonssystemene
  - Alternativ drift med delvis støtte fra informasjonssystemene
- Nødrutinene skal øves, testes, revideres og oppdateres minst en gang i året

Spørsmål og refleksjoner