Risikovurdering av et fagsystem

Alle som behandler Personopplysninger har lovpålagt plikt til å sørge for at per­sonopplysninger som behandles elektronisk, eller oppbevares i arkivskap, er tilfredsstillende sikret. Dette følger av personopp­lysningsloven § 13 og personopplysningsforskriften kapittel to, og omtales som informasjonssikkerhet. Formålet med reglene om informasjonssikkerhet er å unngå krenkelser av personver­net til ansatte, kunder eller klienter. Det vil si å ivareta behovet for personlig integritet og privatlivets fred. Målet med denne veile­deren er å hjelpe fagansvarlig for er fagsystem i Kristiansand Kommune å gjennomføre risikovurderingen av sine system.

Veilederen inneholder en rekke eksempler på hendelser som kan føre til brudd på informasjonssikkerheten, og inkluderer sikker­hetstiltak som kan iverksettes for å unngå dette. Den dekker likevel ikke alle uønskede hendelser eller aktuelle sikkerhetstil­tak.

Personopplysningsloven § 13 krever at behandlingen av per­sonopplysninger er tilfredsstillende sikret. Verdt å merke seg er at dette betyr at personopplysninger skal være tilfredsstil­lende sikret uavhengig av om de er sensitive eller alminne­lige. Datatilsynet stiller likevel ekstra strenge krav til sikring av sensitive personopplysninger.

# Definisjoner

Før vi går videre vil vi avklare noen definisjoner:

## Konfidensialitet

Med ”konfidensialitet” menes det at informasjon må være sikret mot at uvedkommende får kjennskap til opplysningene.

## Integritet

Med ”integritet” menes det at informasjon må være sikret mot utilsiktet eller uautorisert endring eller sletting.

## Tilgjengelighet

Med ”tilgjengelighet” menes det at informasjon som skal behandles, er tilgjengelig til den tid og på det sted det er behov for opplysningene.

## Uønsket hendelse

Datatilsynet definerer en uønsket hendelse på følgende måte: «*En trussel er en mulig uønsket hendelse som kan inntreffe. En hendelse er en handling eller tilstands­endring som kan utsette verdier for risiko – i form av mangelfull konfidensialitet, integritet eller tilgjenge­lighet*».

# Risikovurdering

Når man skal gjennomføre en risikoanalyse for et fagsystem, er det flere spørsmål man vil stille seg selv:

* Hva kan skje?
* Hvilke uønskede hendelse kan inntreffe?
* Hvordan er trusselbildet for vårt fagsystem?

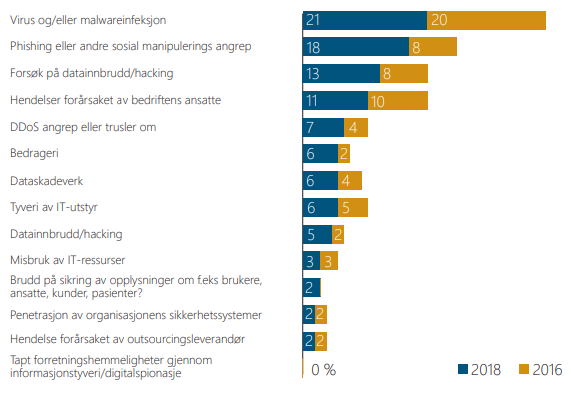
Innsikt i slike spørsmål kan skaffes på forskjellige måter. Vi kan ha opplevd hendelser som vi ikke vil skal gjenta seg, vi kan ha kontakt med andre firma som ligner på vårt og fått vite hva de har opplevd. Vi kan støtte oss på eksperter som har erfaring og kompetanse om informasjonssikkerhet og trusselbildet. Internett er også en kilde til å lære om trusler og farer som kan ramme oss. NorSIS- Norsk senter for informasjonssikring som er opprettet på oppdrag fra Nærings- og handelsdepartementet utgir regelmessig en rapport om IKT-trusselbildet for Norge. I kortversjonen av denne rapporten har de diskutert mulige uønskede hendelser innen følgende overskrifter:

* [Spam](https://nettvett.no/spam/), Lotterigevinster, «nigeriabrev» og [phishing](https://nettvett.no/phishing/)
  + Gamle, klassiske "Nigeria scams" har flyttet seg fra telefax til e-post, og stadig flere later til å la seg lure av lovnader om lettjente penger ved hvitvasking av millioner. Lovlydige borgere kan på den annen side bli lurt med på "phisketur", hvor de kan bli lurt til å oppgi kontoinformasjon, koder og passord på websider som til forveksling likner nettbanken o.l.
* [Falske Eposter](https://nettvett.no/falske-e-poster/)
  + E-post er en vanlig og nødvendig del av den digitale hverdagen. Dessverre kan e-poster enkelt forfalskes til å fremstå som noe annet enn de er, og det utnytter svindlere og kriminelle daglig. I denne veiledningen forklarer vi hvordan du kan avsløre en falsk e-post, og hvordan du kan håndtere den.
* [Falske trusler og utpressingskrav](https://nettvett.no/falske-trusler-og-utpressingskrav/)
  + Fra 2018 og utover har e-poster med usanne påstander om at du er hacket, og har blitt filmet mens du har sett på pornografi, blitt veldig vanlig.
* Spywear
  + Skjulte elementer i e-postmeldinger og websider (web bugs) og programvare som er laget for overvåkning (spyware) er svært utbredt og kan samle opplysninger om alt fra surfevaner på Internett til nettbankpassord.
* [Virus](https://nettvett.no/virus/) og ormer
  + De siste par årene har Norge vært rammet av flere virus og ormer (Netsky, Bagle/Beagle, Sasser) som har hatt store konsekvenser for norske bedrifter. Bruk av antivirus-programvare er utbredt i Norge, men man ser at tiden fra en sårbarhet oppdages til det dukker opp et virus eller en orm som utnytter denne, blir stadig kortere. Det er derfor en stor utfordring å sørge for å holde sine systemer oppdatert med siste sikkerhetspatch og ha oppdaterte virusfiltre.
* [Direktørsvindel](https://nettvett.no/direktor-svindel/)
  + Denne typen svindel innebærer for eksempel at noen som jobber i økonomiavdelingen mottar en e-post eller en SMS fra en leder i virksomheten, gjerne administrerende direktør (derav navnet direktørsvindel, og det engelske navnet *CEO fraud*). Lederen ber den ansatte om å overføre et større beløp, og det presiseres gjerne at det haster, noe som gir den ansatte lite tid til å tenke seg om eller følge vanlige rutiner og prosedyrer.
* [Trådløs forbindelse](https://infosec.sintef.no/informasjonssikkerhet/2018/10/sikkerhet-uten-en-trad/)
  + Trådløs nettverking involverer typisk kringkastingskommunikasjon, som er svært mye mer utsatt for avlytting og jamming enn trådbundne nettverk. Trådløse nettverk er også mer sårbare for aktive angrep som utnytter sårbarheter i kommunikasjonsprotokoller.
* [Tjenestenekt eller DDOS angrep](https://www.nsm.stat.no/blogg/tjenestenektangrep/)
  + Tjenestenekting oppstår når en tjeneste blir utilgjengelig uten at dette er planlagt, for eksempel som følge av et målrettet angrep i form av store mengder nettverkstrafikk. Tjenestenekting er ofte et resultat av virus-/orm-angrep. Vi har også sett eksempler der virksomheter har tatt ned sin nettforbindelse, og dermed gjort sine nettbaserte tjenester utilgjengelige, fordi de forventer at et angrep vil komme.
* [Single-point of failure](https://en.wikipedia.org/wiki/Single_point_of_failure)
  + Etter hvert som bruk av Internett og nettbaserte tjenester blir en stadig større del av norske arbeidstakeres jobbhverdag, blir også konsekvensene ved bortfall av disse tjenestene større. Norske virksomheter bør være bevisst dette i langt større grad enn hva de er i dag, og vurdere kostnadene ved bortfall av nettilgang mot kostnadene ved å forsikre seg på best mulig måte mot at dette kan skje.
* [Utilsiktede menneskelige feil](https://www.ibas.com/no/blogg/hva-menes-med-datahavari/)
  + Mennesker er som kjent ikke alltid logiske og forutsigbare, og det er derfor vanskelig å forutse og kontrollere deres oppførsel. Brukerne av IKT-systemer, og de som bygger, drifter og vedlikeholder systemene, er mennesker; den menneskelige faktor er derfor noe man må ta hensyn til ved design av systemer og utforming av regler og rutiner for bruk. Det har de siste årene vært flere eksempler på store sikkerhetshendelser i Norge som skyldes menneskelige feil.
* [Utro tjenere](https://juristen.no/nyheter/2019/08/nesten-%C3%A9n-av-tre-virksomheter-avdekket-utro-tjenere-blant-egne-ansatte-%C2%A0)
  + Mørketallsundersøkelsen 2003 om datakriminalitet og IT-sikkerhet, utført av ØKOKRIM, NSR og SIS, viser at en av to gjerningsmenn som blir tatt er en av virksomhetens egne ansatte. Norske bedrifter har fortsatt en utfordring forbundet med å begynne å fokusere også på angrep som kommer innenfra.
* Misbruk av virksomhetens ressurser
  + Det har vært flere store saker fremme i media som har dreid seg om at ansatte i virksomheter har benyttet virksomhetens dataressurser til privat og ulovlig bruk. Vi ser et behov for klarere retningslinjer for hva som er tillatt bruk av virksomhetens ressurser.
* [Tyveri av mobil enhet](http://intranett/tjenester/Tema/IT-tjenester/)
  + Mobile enheter, som bærbare PC-er, PDA-er, mobiltelefoner og MP3-spillere, er i stand til å lagre store mengder informasjon. Tyveri av mobile enheter fra ansatte på reise utgjør en stor sikkerhetsrisiko for norske virksomheter da store mengder informasjon kan komme på avveie på en gang.
* [Identitetstyveri](https://nettvett.no/id-tyveri/)
  + Identitetstyveri oppstår når noen anskaffer, overfører, besitter eller fremstår som rette innehaver av personlige opplysninger tilhørende en privatperson eller selskap på en uautorisert måte, med den hensikt å begå bedrageri eller annen kriminalitet.
* [Datainnbrudd og datakriminalitet](https://nettvett.no/skjema-anmeldelse-datakriminalitet/)
  + Anmeldelse av datakriminalitet er svært viktig for bekjempelse av denne type kriminalitet. Kriminaliteten rammer mange forskjellige typer ofre på mange forskjellige steder og på forskjellige tider. Det kan være avgjørende for oppklaringen av en sak å kunne se sammenhengen mellom hendelser og gjerningspersoner. Kripos anbefaler alle å anmelde både kriminalitet og forsøk på kriminalitet.

### Undersøkelse fra Næringslivets sikkerhetsråd NRS - [mørketallundersøkelsen](https://www.nsr-org.no/getfile.php/1311303-1537281687/Bilder/M%c3%b8rketallsunders%c3%b8kelsen/M%c3%b8rketallsunders%c3%b8kelsen%202018%20low.pdf) 2018 viser:

* 82 prosent (offentlig administrasjon) og 88 prosent (helse) sier at de har rammeverk for informasjonssikkerhet og at rutinene etterleves.
* Samtidig sier 25 prosent at manglende sikkerhetsprosesser førte til sikkerhetsbrudd og at 40 prosent innen offentlig administrasjon rapporerer at virksomheten har opplevd sikkerhetsbrudd grunnet manglende oppfølging av prosesser.
* Siden en tredjedel av offentlig virksomhet oppdager sikkerhetsbrudd ved en tilfeldighet så kan en godt stille spørsmål om hvor effektiv etterlevelsen av rammeverk for informasjonssikkerhet er i praksis, samt hvilken effekt eksisterende prosesser eller etterlevelse av rutiner har påå sikkerhetsarbeidet.
* I undersøkelsen er phishing og sosial manipulering de vanligste informasjonssikkerhetshendelsene, og det er mer enn en dobling av antallet siden 2016. Nå en spør om årsakene til at hendelser skjer, er de fire mest vanlige årsakene tilfeldigheter og uflaks, menneskelige feil, mangel på sikkerhetsbevissthet hos de ansatte og at eksisterende prosesser ikke blir fulgt. NorSIS anbefaler at grundig opplæring og trening i digital sikkerhet vil både forebygge slike hendelser og sørge for at konsekvensene blir mindre når hendelsen er et faktum.

Hvilke informasjonssikkerhetshendelser var virksomhetene utsatt for i 2016 og 2018

 Når vi skal gjøre vår risikovurdering vil denne listen, sammen med våre egne erfaringer, kunne være et godt utgangspunkt for systematisk å ta for seg området «Informasjonssystem».

## Eksempel på uønskede hendelser

La oss se på noen eksempler av uønskede hendelser for et kontorstøttesystem. Her har vi også forsøkt å angi om hendelsen medfører brudd på konfidensialitet, tilgjengelighet eller integritet.

|  |  |  |
| --- | --- | --- |
| Uønsket hendelse | Årsak | Brudd på: K – konfidensialitet, I – integritet, T – tilgjengelighet |
| Uautorisert tilgang til data | Tilsatte går fra åpen/pålogget pc  Utskrifter på avveie  Ukorrekte filrettigheter | K- Konfidensialitet |
| Utlevering av sensitiv informasjon | Uvitenhet  Manglende kompetanse  Lagrer feil  Utskrifter på avveie | K- Konfidensialitet |
| Informasjon sendt til feil adressat | Feil epostadresse  Dårlig adresseliste  Slurv/stress  Doble adresser  Bruker kortnavn som epost(initialer)  Nesten identiske navn i kontakter | K- Konfidensialitet |
| Utilsiktet og tilsiktet endring/sletting av data | Manglende kunnskap  Lagring på fellesområder  Egen vinning  Manglende rutiner  Tilsatte går fra åpen pc  Manglende sikring av pc  Slurv | «I-Intigritet, T-Tilgjengeligehet |
| Ødelagte eller endrede data | Virusangrep  Feil eller manglende installasjon av Antivirus  Virus via epost  Nedlastning av program fra Internett | «I-Intigritet, T-Tilgjengeligehet |
| Uautorisert bruker endrer dokumentet | Feil i definisjon av tilgang  Feil i lagring  Ikke utlogget arbeidsstasjon  Bruk av andres id og passord  Lett tilgjengelig passord  Tilsatte går fra åpen pc  Manglende sikring av pc | «I-Intigritet, |
| Brudd i tilgang til informasjon | Systemfeil og -stopp  Feil på maskinvare  Strømstans  Nettverksfeil  Sabotasje | T- Tilgjengelighet |
| Ødelagte/slettede/endrede data | Ingen sikkerhetskopi  Feil/ødelagt media  Virus | T- Tilgjengelighet |

## Sannsynlighet og konsekvens

Hvordan beregner vi sannsynligheten for at en hendelse skal inntreffe? I Kristiansand Kommune har vi valgt å ha tre graderinger. Det er vanskelig å forutse noe som ikke har skjedd enda, og vi kan ikke gjøre stort annet enn å være på vakt og gjenta risikoanalysen med jevne mellomrom. Det er derfor krav til systemeier og fagansvarlig at vurderingen gjøres på årlig basis.

Sannsynlighet - Vurdering av hvor ofte en uønsket situasjon vil kunne oppstå.

|  |  |
| --- | --- |
| Sannsynlighetsgrad | Forklaring |
| 1 | Vil kunne skje hvert femte år eller sjeldnere |
| 2 | Vil kunne skje 1 gang pr år eller sjeldnere |
| 3 | vil kunne skje 1 gang i måneden |
| 4 | Vil kunne skje ukentlig |
| 5 | Vil kunne skje ukentlig/daglig |

Vurdering av konsekvens av en hendelse skal gjøres uavhengig av hvor sannsynlig det er at den inntreffer.

Konsekvens - Vurdere hvor alvorlige konsekvensene/skaden vil være. Kan være til hjelp i graderingen å tenke på hva som skal til for å rette opp skaden igjen.

|  |  |
| --- | --- |
| Konsekvensgrad | Forklaring |
| 1. Lite alvorlig | Lite alvorlig  Hendelsen medfører ingen økonomiske tap. Kan gjenopprettes, fører ikke til tap av anseelse eller integritet. |
| 2 - Lav | Hendelsen kan medføre økonomiske tap - men som kan gjenopprettes, eller kan føre til tap av anseesle eller integritet (eksempelvis komprommitering av opplysninger den registrerte oppfattes som følsomme). Avvik vurderes sendes til datatilsynet |
| 3 - Moderat | Hendelsen kan medføre betydelig økonomisk tap - men som kan gjenopprettes, eller kan føre til tap av anseelse eller integritet (eksempelvis kompromittering av opplysninger deg registrerte oppfatter som krenkende, eller som andre kan gjøre nytte av). Avvik sendes datatilsynet |
| 4 - Høy | Hendelsen kan føre til tap av helse, eller kan medføre uopprettelig økonomiske tap, eller kan føre til alvorlig tap av anseelse og integritet. Avvik sendes datatilsynet |
| 5 - Kritisk | Hendelsen kan føre til tap av liv eller vedvarende helsetap, eller kan medføre betydelig og uopprettelig økonomisk tap, eller kan føre til alvorlig tap av anseelse eller integritet som påvirker liv eller helse. Avvik sendes datatilsynet. |

Ser vi på eksempelet ovenfor og gjør en vurdering av sannsynlighet og konsekvens, samt setter på forslag til tiltak for hver av de mulige hendelsene, kan resultatet se slik ut.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Uønsket hendelse | Årsak | Mulige konsekvenser | Brudd | S | K | Forslag til tiltak |
| Uautorisert tilgang til data | Tilsatte går fra åpen/pålogget pc  Utskrifter på avveie  Ukorrekte filrettigheter | Eksterne personer ser informasjon på skjerm til tilsatt.  Kan risikere at opplysninger kommer på avveie.  Truer klientens personvern | K | 1 | 3 | Pålegge alle å låse pc når man forlater den  Vurdere tidsintervall |
| Utlevering av sensitiv informasjon | Uvitenhet  Manglende kompetanse  Lagrer feil  Utskrifter på avveie | Personvern er truet  Negativ medieomtale  Feil saksbehandling  Økonomiske tap  Mottar ikke informasjon om sak  Konsekvens for ansettelsesforhold  Eksterne får informasjon | K | 1 | 4 | Opplæring av ansatte  Låsbare printerrom  Vurdere personlig kode for utskrift  Begrense tilganger til antall skrivere |
| Informasjon sendt til feil adressat | Feil epostadresse  Dårlig adresseliste  Slurv/stress  Doble adresser  Bruker kortnavn som epost(initialer)  Nesten identiske navn i kontakter | Feil person får se informasjon  Riktig person får ikke informasjon  Feil beslutningsgrunnlag  Informasjon på avveier  Uautorisert får tilgang til data som er sendt feil på epost | K | 2 | 2 | Opplæring/bevisstgjøring  Rettningslinjer |
| Utilsiktet og tilsiktet endring/sletting av data | Manglende kunnskap  Lagring på fellesområder  Egen vinning  Manglende rutiner  Tilsatte går fra åpen pc  Manglende sikring av pc  Slurv | Feil beslutning/vedtak  Tap av data  Merarbeid  Negativ medieomtale  Tap av tillit  Tap av data  Feil informasjon | I, T | 2 | 2 | Obligatorisk kurs i bruk av PC  Lage rettningslinjer for bruk av felles lagringsområder |
| Ødelagte eller endrede data | Virusangrep  Feil eller manglende installasjon av Antivirus  Virus via epost  Nedlastning av program fra Internett | Tap av data  Feil informasjon  Ukontrollert endring av data | I, T | 3 | 3 | Virussjekk på inngående epost  Obligatorsik opplæring og info om virusangrep  Riktig konfigurasjon av brannmur |
| Uautorisert bruker endrer dokumentet | Feil i definisjon av tilgang  Feil i lagring  Ikke utlogget arbeidsstasjon  Bruk av andres id og passord  Lett tilgjengelig passord  Tilsatte går fra åpen pc  Manglende sikring av pc | Tap av data  Feil informasjon  Ukontrollert endring av data | I | 1 | 3 | Konsekvente retningslinjer for skjerming av egen bruker-id og passord  Konsekvent bruk av skjermsparer m/passord  Bedre kvalitetssikring ved tildeling av rettigheter  Rutiner for endring av passord |
| Brudd i tilgang til informasjon | Systemfeil og -stopp  Feil på maskinvare  Strømstans  Nettverksfeil  Sabotasje | Tap av data  Feil informasjon  Ukontrollert endring av data | T | 3 | 1 | Bedre sikring for å hindre at bruker «klusser» i eget oppsett  Sjekk/kontroll av UPS |
| Ødelagte/slettede/endrede data | Ingen sikkerhetskopi  Feil/ødelagt media  Virus | Data ikke tilgjengelig for en kort studn  Tap av data  Tap av tid/ressurser | T | 2 | 2 | Obligatorisk, jevnlig test av backup/restore |