# Informasjonssikkerhetspolicy - sikkerhetsmål og sikkerhetsstrategi

## Omfang

Denne policyen for informasjonssikkerhet gjelder all informasjonsbehandling som skjer internt i *<virksomhet>* og som *<virksomhet>* har ansvaret for eksternt. Dette omfatter all behandling, lagring og kommunikasjon av informasjon både muntlig, på papir og digitalt. All bruk av IKT-verktøy er også inkludert.

## Formålet med vår informasjonsbehandling og informasjonssikkerhet

Formålet med informasjonsbehandling i *<virksomhet>* er å understøtte våre oppgaver og tjenester slik at vi kan nå våre mål og realisere vår visjon. Mål og prioriteringer finner dere i vår overordnede strategi og virksomhetsplan.

En informasjonsbehandling som er målorientert, effektiv, lovlig og til å stole på er avgjørende for at *<virksomhet>* skal lykkes. Tilstrekkelig og balansert informasjonssikkerhet er en kritisk faktor for å understøtte dette.

## Overordnede føringer

*<Beskriv her overordnede føringer med betydning for informasjonsbehandling og informasjonssikkerhet, for eksempel gitt av «Handlingsplan for informasjonssikkerhet i staten» og «Digitaliseringsrundskrivet». >*

## Sentrale lover og forskrifter

Informasjonssikkerheten i *<virksomhet>* er regulert av en rekke lover og regler. Dette er noen av de mest sentrale:
*<Eksempler. Stryk de lover nedenfor som ikke er relevante, og legg eventuelt til andre lover og forskrifter>*

* Lov om behandling av personopplysninger (personopplysningsloven)
* Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven)
* Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
* Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)
* Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven)
* Forskrift om informasjonssikkerhet (forskrift til sikkerhetsloven)
* Forskrift om sikkerhetsadministrasjon (forskrift til sikkerhetsloven)
* Arbeidsmiljøloven
* Straffeloven
* Arkivloven
* Helseregisterloven
* Verdipapirhandelloven
* Forskrift om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (Internkontrollforskriften)

## Sikkerhetsmål

*<Virksomhet>s* behandling av informasjon skal være i samsvar med regulatoriske, interne og avtalerettslige krav til informasjonssikkerhet. Personopplysninger og annen beskyttelsesverdig informasjon skal sikres på en betryggende måte gjennom fysiske, tekniske og organisatoriske tiltak.

### Konfidensialitet

Personopplysninger og annen beskyttelsesverdig informasjon som behandles i *<virksomhet>* skal være beskyttet mot uautorisert tilgang.

Personopplysninger behandles konfidensielt og kan bare deles med andre medarbeidere i den grad det er tjenstlige behov.

Personopplysninger om egne arbeidstakere kan kun behandles av den som har tjenstlig behov.

### Integritet

Informasjon som *<virksomhet>* har ansvaret for blir bare produsert og endret av ansatte, eller av eksterne som har fullmakt til dette.

Informasjon skal ikke endres utilsiktet.

### Tilgjengelighet

Informasjonssystemet er tilgjengelig for autoriserte brukere ved behov.

### Robusthet

Virksomheten og informasjonssystemet er motstandsdyktig og robust.

Når uønskede fysiske eller tekniske hendelser inntreffer, bidrar beredskapstiltak til å begrense skaden og at *<virksomhet>* raskt kommer tilbake til normal drift. Dette inkluderer å gjenopprette tilgjengelighet og tilgang til personopplysninger i rett tid.

## Sikkerhetsstrategi

Informasjonssikkerhetsarbeidet skal:

* være forankret i linjen og utføres systematisk
* gjennomføres for å nå målene for informasjonssikkerhet
* være risikobasert og følge anerkjente standarder
* følge prinsippene for læring og kontinuerlig forbedring

Det innebærer at:

* risikovurderinger gjennomføres systematisk, periodisk og ved vesentlige endringer i oppgaver eller omgivelsene
* tiltak for å redusere risiko er basert på risikovurderinger og ledelsens føringer for risikohåndtering og akseptabel risiko
* hendelser som ut fra risiko kan påvirke informasjonssikkerhetsmålene negativt, meldes og følges på en systematisk måte
* ledelsen systematisk styrer og følger opp informasjonssikkerhetsarbeidet
* ledelsen systematisk følger opp måloppnåelse, etterlevelse, kompetanse og kultur.

For å lykkes med dette skal alle ansatte:

* ha et bevisst forhold til virksomhetens sikkerhetsmål og målenes viktighet
* vite hvilke typer av informasjon de behandler og hvilke krav som stilles til deres egen informasjonsbehandling og bruk av IKT
* etterleve krav, retningslinjer, prosedyrer, rutiner m.v. som gjelder for dem og det arbeidet de utfører.

Strategiene implementeres gjennom ledelsesforankrede sikkerhetsvalg.

## Sikkerhetsvalg

### Systemteknisk sikkerhet – nødvendig sikkerhetsnivå

Avhengig av det aktuelle system og informasjonen som behandles, vil de ulike aspektene ved sikkerhet (konfidensialitet, integritet, tilgjengelighet og robusthet) ha ulik betydning. Følgende kategorisering benyttes for beskyttelsesbehov:

* **Høy** – gis bare system og informasjon med virksomhetskritisk beskyttelsesbehov
* **Middels** – gis system og informasjon med beskyttelsesbehov
* **Lav** (lave krav til sikkerhet) – kan gjelde alle system og informasjon med lite eller ingen beskyttelsesbehov.

Ulike delsystem kan ha ulike beskyttelsesbehov.

### Tekniske sikkerhetstiltak

* Tiltak som forhindrer at arbeidstakere uaktsomt eller med forsett skal kunne skade informasjonssystemet eller informasjon som her er lagret.
* Tiltak som sørger for å gi tilgang til informasjonssystemet for de brukere som er autorisert, og som forhindrer at uvedkommende gis tilgang til informasjon.
* Det er etablert sikkerhetslogging som gjør at sikkerhetsbrudd kan avdekkes.
* Tiltak for å forhindre at skadelig programvare kommer inn i virksomhetens informasjonssystem.
* Jevnlig sikkerhetskopiering av lagringsmedium.
* Tapt informasjon skal kunne gjøres tilgjengelig igjen senest innen tre virkedager. I den grad tap av informasjon skyldes brann eller annen alvorlig skade skal informasjonen kunne gjøres tilgjengelig senest innen to uker. For informasjonssystemet gjelder at alvorlig systemfeil (for eksempel svikt i vitale komponenter) ikke skal føre til driftsstans mer enn 72 timer.
* Telefonsystem tillates ikke å ha en driftsstans som overstiger 24 timer for driftsfeil. Ved alvorlige systemfeil skal feilretting startes uten ugrunnet opphold.

*<Kort beskrivelse av sikkerhetsarkitektur, for eksempel at det etableres to soner i virksomhetens informasjonssystem, hvorav en defineres som sikker sone og en som intern sone. Det tillates logisk forbindelse mellom de to sonene, men tilfredsstillende beskyttelse skal være etablert. Beskrivelse av hvilke system som ligger i sikker sone og hvorfor.>*

### Organisatoriske tiltak

* Rutiner for håndtering av tilgang til virksomhetens informasjonssystem. I dette ligger kontroll av passord, rettigheter, applikasjoner mv. Vanskelighetsgraden for passord skal håndteres av systemet og ligge på et høyt nivå. *<Passordråd finnes her:* [*https://nettvett.no/passord/*](https://nettvett.no/passord/) *>*
* Rutiner med hensyn til ansattes håndtering av transportable lagringsmedium, slik som bærbare datamaskiner, for å unngå at informasjon havner på avveier.
* Rutiner for låsing av lokalene, håndtering av gjester og bruk av alarm utenom arbeidstid.
* Prosedyrer for plassering og sikring av komponenter, lagringsmedium, dokumenter eller øvrige bestanddeler som er vitale for virksomhetens drift.

### Fysiske tiltak

* *<Virksomhet>*s lokaler sikres mot blant annet innbrudd, brann, vannskade mv.
* Forhindre at uvedkommende gis tilgang til lokaler hvor beskyttelsesverdig informasjon oppbevares.
* Maskinpark, lagringsmedium og sentrale nettverkskomponenter er fysisk sikret, slik at uvedkommende ikke kan bringe dette med seg ut av etatens lokaler.
* Bærbare enheter som er ment å bringes utenfor virksomhetens lokaler skal sikres med kryptering.
* System for destruksjon av sensitive opplysninger. Det finnes egen deponeringskasse som er tilstrekkelig beskyttet slik at ikke dokumenter kan fjernes etter deponering. Likeledes finnes det et tilfredsstillende system for håndtering av elektroniske lagringsmedium.

### *<Virksomhet>s* spesifikke applikasjoner

For virksomhetens spesifikke applikasjoner, det vil si applikasjoner som utvikles spesielt for *<Virksomhet>*, gjelder følgende:

* Ansvaret for håndtering av sikkerhetsbehov i *<Virksomhet>s* spesifikke applikasjoner ligger hos systemeieren. Utøvende ansvar kan delegeres til prosjektleder eller andre navngitte personer.
* All programvare skal utvikles på bakgrunn av detaljerte kravspesifikasjoner der også krav til innebygd personvern, personvern som standardinnstilling og sikkerhet inngår (se Datatilsynets veileder for programvareutvikling med innebygd personvern og sjekklister <https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/programvareutvikling-med-innebygd-personvern/> )
* Innebygd personvern, personvern som standardinnstilling og teknisk sikkerhetsnivå skal verifiseres i alle prosjektets faser ved utvikling.
* Før programvaren/systemer settes i produksjon, skal teknisk sikkerhetsnivå, innebygd personvern og personvern som standardinnstilling verifiseres. Ved feil eller mangler skal retting av eventuelle feil/mangler gjennomføres før systemet settes i produksjon. Rettelser av feil og mangler skal verifiseres.
* Før programmer eller systemer settes i produksjon skal rutiner for drift, proaktiv overvåkning og beredskap være iverksatt.
* Verifikasjon av sikkerhet og personvern gjennom test skal utføres av andre personer enn de som har vært med på å utvikle systemet eller personer som drifter systemer. Sikkerhetsansvarlig har ansvaret for selve gjennomføringen av testen og formidler resultatene tilbake til prosjektet.

## Bruk av databehandlere og underleverandører

*<Virksomhet>s* bruk av databehandlere og leverandører skal reguleres i kontrakter, hvor også bestemmelser om informasjonssikkerhet inngår. Alle avtaler hvor en ekstern virksomhet påtar seg oppdrag for *<virksomhet>* som også omfatter informasjonssikkerhet, skal baseres på avtaler som minst samsvarer med kravene som er gitt i personvernforordningen artikkel 28 og 29.

Verdieier kan ikke engasjere nye leverandører uten at dette avklares med *<daglig leder / avdelingsdirektør>*. Eksterne virksomheter eller personer kan ikke gis tilgang til virksomhetens informasjonssystem med mindre dette skjer som ledd i en godkjent avtale.

## Oppbevaring og behandling av gradert informasjon

*<Dersom virksomheten oppbevarer og behandler informasjon som faller inn under lov om forebyggende sikkerhet, beskrives det her.>*