# Avvikshåndtering

|  |
| --- |
| Veiledning om håndtering av avvik med melding til Datatilsynet og informasjon til de berørte finnes på Datatilsynets nettsider: <https://www.datatilsynet.no/>avvik |

Et avvik er en uheldig hendelse eller et regelbrudd, og er noe som skjer i alle virksomheter. Brudd på disse reglene, og internkontrollen for øvrig, skal rapporteres til sikkerhetsansvarlig som avvik.

Avvik kan være:

* Brudd på gjeldende rutiner eller regelverk
* Hendelser som kan ha konsekvenser for informasjonssikkerheten vår
* Utført av ansatte, som brudd på sikkerhetsbestemmelser (bevisst eller ubevisst)
* Utført av eksterne, som fysisk innbrudd eller elektroniske angrep

Personvernforordningen artikkel 32 og 33 stiller krav om at vi håndterer hendelser og brudd på personopplysningssikkerheten. Vi må behandle avvikene for å:

* Lære av feil og hendelser
* Håndtere hendelser og gjenopprette normaltilstand
* Forbedre systemer og rutiner

Feil i programvare og maskinvare regnes ikke som avvik i denne sammenhengen, og rapporteres til IT-drift.

## Rapportering

Alle ansatte er ansvarlig for å rapportere avvik til den sikkerhetsansvarlige. Det skal være en lav terskel for å rapportere avvik. Meld også fra om situasjoner hvor noe kunne gått galt, slik at vi kan forbedre oss.

Avvik kan meldes enten på e-post til *<egen e-postadresse>* (dersom innholdet ikke er kritisk mht. konfidensialitet), eller leveres på eget skjema.

Dersom det er grunn til å anta at det haster med å håndtere avviket, skal den sikkerhetsansvarlige i tillegg orienteres direkte.

Dersom den sikkerhetsansvarlige ikke er tilgjengelig, og den ansatte vurderer at det haster med å melde fra, varsles *<avdelingsdirektør>*, dernest *<daglig leder>.*

## Behandling av rapporterte avvik

Den sikkerhetsansvarlige er ansvarlig for oppfølgingen av meldte avvik, og skal:

* Arkivere mottatte avvik
* Varsle *<direktør/avdelingsdirektør>* ved behov.
* Vurdere det meldte avviket og om nødvendig ta initiativ til korrigerende tiltak
* Dersom det har skjedd et brudd på personopplysningssikkerheten, vurdere hvilken risiko det er for de berørtes rettigheter og friheter:
  + Dersom det er ingen eller lav risiko, er det ikke behov for å melde fra til Datatilsynet eller til de berørte
  + Dersom det er middels risiko, er det nødvendig å melde fra til Datatilsynet, men ikke informere de berørte
  + Dersom det er høy risiko, er det nødvendig å melde fra til Datatilsynet og informere de berørte
* Føre en løpende oppdatert oversikt over meldte avvik. Oversikten skal minimum inneholde:
  + Dato
  + Beskrivelse
  + Melder
  + Type
  + Alvorlighet
  + Status
  + Gjennomførte og planlagte tiltak
  + Frist for neste oppfølgingspunkt
  + Kommentarer

### Korrigerende tiltak

Dersom den sikkerhetsansvarlige vurderer det som nødvendig, skal det iverksettes korrigerende tiltak. Slike tiltak kan primært bestå i ett eller flere av følgende elementer:

* Oppfølging av den ansatte som har forårsaket avviket
* Bedre informasjon til alle
* Vurdering og eventuell utbedring av rutiner
* Tekniske sårbarheter utbedres / begrenses
* Varsling av eksterne parter

Dersom lukking av avviket kan påvirke *<Virksomhet>s* omdømme, relasjon til eksterne parter, økonomiske situasjon eller lignende, skal *<direktør/avdelingsdirektør>* godkjenne dette før tiltak iverksettes.

### Oppfølging av medarbeider som har forårsaket avvik

Noen avvik må følges opp overfor ansatte som har forårsaket avviket, utover informasjon/opplæring av nærmeste leder.

Følgende avvik skal følges opp overfor den ansatte av nærmeste leder:

* Brudd på taushetsplikt
* Bevisste sikkerhetsbrudd:
  + Misbruk av virksomhetens IKT-systemer
  + Tyveri av virksomhetens eiendom
  + Tilsiktet spredning av ondsinnet programvare
  + Forsøk på å sende sensitive personopplysninger i e-post/vedlegg

Reaksjonsformen må konkret vurderes, blant annet med hensyn til:

* Om avviket har resultert i uønskede hendelser, eventuelt i hvilket omfang
* Om avviket er eller kan bli til skade for virksomheten
* Om avviket har vært gjentatt
* Om overtredelsen synes å være uaktsom eller forsettlig

Mulig reaksjonsformer:

* Den sikkerhetsansvarlige tar avviket opp med vedkommende.
* Avviket tas opp av nærmeste overordnet med den eller de som er årsak til avviket.
* Avviket tas opp av nærmeste overordnet med den eller de som er årsak til avviket. Avdelingsdirektør og direktør informeres.

Avviket medfører en skriftlig advarsel til den eller de som er årsak til avviket. Advarselen gis etter at den eller disse har fått gitt en redegjørelse for avvik

### Utført av eksterne

Alle innbrudd og forsøk på innbrudd skal politianmeldes.

Alle elektroniske angrep som medfører økonomiske konsekvenser for virksomhet, skal vurderes anmeldt til Politiet.

## Beredskapshendelser

IT-drift skal håndtere alle beredskapshendelser og rapportere dette på eget skjema.