# Sikkerhetsrevisjon

|  |
| --- |
| For mer detaljer om sikkerhetsrevisjon vil vi anbefale at man leser Nasjonal Sikkerhetsmyndighets (NSM) veileder om sikkerhetsrevisjon: <https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/2017_veilederisikkerhetsrevisjonv02.pdf>  |

I denne dokumentet beskrives egenkontroller, internrevisjon og revisjoner av sikkerhetsparter og databehandlere.

I tillegg inngår daglig oppfølging av sikkerhetslogger i *<Virksomhet>*s sikkerhetsrevisjoner. Funn fra loggkontroll håndteres som øvrige avvik. Egenkontroll, internrevisjon og revisjon med sikkerhetsparter og databehandlere rapporteres eksplisitt.

## Egenkontroll

### Plan

Den sikkerhetsansvarlige har ansvar for å opprette og vedlikeholde en plan over egenkontrollaktiviteter. Planen skal inneholde aktiviteter for å kontrollere at rutiner blir fulgt, og vil utarbeides med bakgrunn i relevante kontrolltiltak i ISO/IEC 27002.

*<Planen bør dekke et tidsrom på minimum ett år men kan løpe over flere år. Det kan være ønskelig å gjøre en grundig kontroll av noen områder eller avdelinger i virksomheten sjeldnere enn en gang pr. år men det skal fremgå av planen at alle aktuelle områder eller avdelinger dekkes i løpet av 2 - 5 år.>*

*Eksempel:*

| **Egenkontrolltiltak** | **Eier av aktivitet** | **Frekvens** | **Resultat** |
| --- | --- | --- | --- |
| Test av uautorisert fysisk adgang til virksomhets lokaler og kontorer | Eiendom og Sikkerhet | Årlig |   |
| Brukeres tilgangsrettigheter. Avdelingsleder sjekker liste tilsendt fra IT-avdeling og kvitterer denne. IT-drift gjør nødvendige oppdateringer | IT-drift | Halvårlig |   |
| Gjennomgang av privilegerte brukeres tilgangsrettigheter – administrator rettigheter | IT-drift, telefoni og system | Halvårlig |   |
| Bekrefte skifte av administratorpassord. | IT-drift, telefoni og system | Årlig / når driftspersonell slutter |   |
| Verifikasjon og evt. oppdatering av konfigurasjonskart - Nettverk | IT-drift | Halvårlig/ved endringer |   |
| Kontroll av liste over IT-utstyr og lagringsmedia | IT-drift | Årlig / ved endringer |   |
| Gjennomgå status på oppdatering av antivirusprogram på hver enkelt PC/server | IT-drift | Kvartal/ stikkprøver |   |
| Gjennomføring av sikkerhetstester (virksomhetskritiske applikasjoner og infrastruktur) | Sikkerhetsansvarlig | Ved endringer  |   |
| Sikkerhetsovervåking IDP (Intrusion Detection Prevention) av kritiske servere samt eksterne forbindelser. | IT-drift | Kontinuerlig |   |
| Bekrefte regelsett i IDP | IT-drift | Årlig /ved endringer |   |
| Periodisk måling av oppetid på viktige og prioriterte systemer. | IT-drift og telefoni | Periodisk |   |
| Bekrefte herding av nettverksenheter, inklusiv sjekk av sikkerhetskopi av svitsjer/ruterkonfigurasjon  | IT-drift | Årlig |   |
| Bekrefte herding av servere  | IT-drift | Årlig / ved endringer |   |
| Bekreftelse av fungerende sikkerhetskopi. For de systemer der dette er gjort som en del av vanlig drift, kreves ikke egen separat egenkontroll aktivitet | IT-drift og telefoni | Årlig / ved endringer |  |
| Bekreftelse av kjennskap -håndteringsrutiner | sikkerhetsansvarlig | Årlig |  |
| Verifikasjon av etterlevelse -håndteringsrutiner | sikkerhetsansvarlig | Årlig |   |

### Rutine

Egenkontroll gjennomføres i henhold til dokumentert plan av enheten som eier aktiviteten. Den sikkerhetsansvarlige har ansvar for å følge opp at planlagte aktiviteter blir gjennomført.

### Rapportering

Resultater fra egenkontrollaktiviteter skal dokumenteres og rapporteres til den sikkerhetsansvarlige. Avvik som avdekkes i egenkontrollen varsles som beskrevet i avvikshåndtering.

Den sikkerhetsansvarlige har ansvar for at det utarbeides en årlig rapport fra egenkontroll til ledelsens gjennomgang.

## Internrevisjon

I årsplanen for internkontrollarbeidet skal det fastsettes områder for internrevisjon. Personell og tidfesting tas inn i *<Virksomhet>s* virksomhetsplan.

Revisjonspersonellet er normalt internt ansatte i *<virksomhet>*, men skal ha en armlengdes avstand til det sentrale arbeidet med internkontroll, informasjonssikkerhet og IKT.

Den sikkerhetsansvarlige representerer *<virksomhet>* i møtet med internrevisjonen. Ledelse og øvrige ansatte involveres ved behov.

Funn fra internrevisjonen skal sammenfattes i en rapport. Rapporten bør være kortfattet, og punktbasert. Det skal skilles mellom konstaterte avvik og anbefalinger. Avvik og anbefalinger skal nummereres i rapporten for å lette oppfølgingen etter revisjonen.

Den sikkerhetsansvarlige skal lage en tiltaksplan for lukking av avvik og oppfølging av anbefalinger etter internrevisjonen.

Rapporten fra internrevisjonen sammen med tiltaksplanen legges frem for ledelsen senest ved ledelsen gjennomgang.

Rapporten fra internrevisjonen er unntatt offentlighet, jf. offentlighetsloven § 14

## Revisjon av sikkerhetsparter og databehandlere

Det skal gjennomføres regelmessig revisjon med våre leverandører, og enhver leverandør skal revideres minst hvert tredje år.

Revisjoner gjennomføres i samsvar med årsplan for internkontrollarbeidet, samt når den sikkerhetsansvarlige finner behov for det.

Det skal lages en rapport etter revisjoner, og det skal legges en plan for oppfølging av avvik og forbedringspunkter både hos leverandøren og *<virksomhet>*. Rapporten og plan for oppfølging av avvik skal oppsummeres til ledelsens gjennomgang, og rapporten skal være tilgjengelig for ledelsen.

Revisjonen skal planlegges innen rammene av avtalen med leverandøren. Revisjoner skal gjennomføres på en måte som bygger opp under et ryddig forhold mellom leverandøren og *<virksomhet>* som kunde.

Dersom det er avtalt mellom <virksomhet> og leverandøren kan tredjeparter gjennomføre revisjonen.

### Revisjonen skal minimum omfatte

* Kontroll om avtalene med parten er oppdaterte og tilstrekkelige
	+ Endringer hos *<virksomhet>*
	+ Endringer hos leverandøren
	+ Endringer i tjenesten
* Gjennomgang av avvik hos leverandøren som er relevant for oppdraget og forholdet til *<virksomhet>*

*<Revisjonen kan også omfatte andre tema som*

* *Leverandørens rutiner opp mot krav i regelverk og avtale*
* *Fysisk sikkerhet hos leverandøren*
* *Leverandørens autorisasjonssystem og medarbeidernes faktiske tilgang til <virksomhet>s informasjonsverdier eller sikkerhetstiltak*
* *Leverandørens logger over tilgang til <virksomhet>s informasjonsverdier eller sikkerhetstiltak*
* *Leverandørens gjennomførte revisjoner eller tredjepartsrevisjoner>*