Sikkerhetsledelse

Virksomhetens leder har det endelige ansvar for utøvelse av forebyggende sikkerhetstjeneste. Ansvaret omfatter også sikkerhetsoppgaver utført av andre for virksomheten, og forebyggende sikkerhetstjeneste i underlagte virksomheter. Ansvaret oppfylles gjennom:

- **Kunnskap om sikkerhetsloven**
  Virksomhetsledelsen må kjenne til sikkerhetslovens formål og virkeområde, og herunder vite hvem som kan behandle skjermingsverdig informasjon.

- **Forståelse for risiko**
  Virksomhetsledelsen må kjenne til hvilken skjermingsverdig informasjon og hvilke skjermingsverdige objekter virksomheten håndterer, og kjenne til mulige trusler mot disse.

- **Etablering av forebyggende sikkerhetstjeneste**
  Virksomhetsledelsen må etablere en tilfredsstillende forebyggende sikkerhetstjeneste med en sikkerhetsorganisasjon av tilstrekkelig omfang. Virksomhetens personell må ha nødvendig kompetanse slik at arbeidsoppgaver utføres sikkert.

- **Oppfølging av forebyggende sikkerhetstjeneste**
  Virksomhetsledelsen må kjenne til hvordan den forebyggende sikkerhetstjenesten utøves og fungerer i virksomheten og sørge for nødvendige forbedringer.

Nasjonal sikkerhetsmyndighet
Telefon 67 86 40 00
post@nsm.stat.no
Postboks 14
1306 Bærum Postterminal
www.nsm.stat.no

NSM

foto: Pål Rødal, Håvar Haug, COLORBOX og NSM

Sikkerhet - et lederansvar

NSM

Ledelsens rolle i forebyggende sikkerhetstjeneste

Samfunnsverdier må beskyttes

Skjermingsverdig informasjon og objekt skal beskyttes mot sikkerhetstruende virksomhet. Virksomhetens leder har, som forvalter av disse verdiene, det endelige ansvaret for beskyttelsen.

Skjermingsverdig informasjon

… er informasjon som må beskyttes for å hindre at Norges eller alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser skades.

Skjermingsverdige objekter

… er objekter der redusert funksjonalitet, skade, ødeleggelse eller overtagelse av andre, kan skade Norges selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser.

Planlagt og systematisk sikkerhetsarbeid

Plikten til å beskytte skjermingsverdig informasjon og objekt oppfylles gjennom forebyggende sikkerhetstjeneste i virksomheten.
Sikkerhetstjenesten skal utøves gjennom planlagt og systematisk sikkerhetsstyring. Tilstrekkelig og effektiv forebyggende sikkerhetstjeneste er kun mulig med en ledelse som er: **ansvarlig, systematisk og engasjert**

Forebyggende sikkerhetstjeneste

Forebyggende sikkerhetstjeneste er alle tiltak som bidrar til å beskytte skjermingsverdig informasjon og objekt mot sikkerhetstruende virksomhet. Forebyggende sikkerhetstjeneste må utøves planlagt og systematisk gjennom et sikkerhetsstyringssystem som omfatter elementene:

- Sikkerhetsledelse
- Sikkerhetsorganisering
- Sikkerhetstiltak og –prosedyrer
- Forholdet til andre virksomheter
- Sikkerhetsoppfølging
- Sikkerhetsdokumentasjon
- Risikovurdering og -håndtering

organisert slik at den forebyggende sikkerhetstjenesten:

planlegges, gjennomføres, kontrolleres og kontinuerlig forbedres



Spørsmål og svar

Hvordan sikkerhetsgraderes skjermingsverdig informasjon ?

Skjermingsverdig informasjon skal sikkerhetsgraderes BEGRENSET, KONFIDENSIELT, HEMMELIG eller STRENGT HEMMELIG, avhengig av den skade det kan medføre om informasjonen blir kjent for uvedkommende. Den som tilvirker informasjonen bestemmer sikkerhetsgraderingen, og kun tilvirker kan omgradere eller avgradere informasjonen.

Hvilke virksomheter kan behandle sikkerhetsgradert informasjon ?

Kun virksomheter som er organ for stat eller kommune, som er leverandør i en sikkerhetsgradert anskaffelse eller som er underlagt sikkerhetsloven gjennom enkeltvedtak, kan behandle sikkerhetsgradert informasjon.

Hvem i virksomheten kan behandle sikkerhetsgradert informasjon?

Personell som har tjenstlig behov, og som er autorisert, kan gis tilgang til sikkerhetsgradert informasjon. Personell må være sikkerhetsklarert før de autoriseres for tilgang til informasjon sikkerhetsgradert KONFIDENSIELT eller høyere.

Kan sikkerhetsgradert informasjon behandles elektronisk ?

Sikkerhetsgradert informasjon kan kun behandles i informasjonssystem som er sikkerhetsgodkjent.