Se veiledningen for foranalysens trinn 3 for veiledning i gjennomføringen.

|  |  |  |
| --- | --- | --- |
| Organisatorisk enhet: | |  |
| Ansvarsområde: | |  |
| Oppdateringer | | |
| Dato | Deltakere | |
|  |  | |
|  |  | |
|  |  | |

Innhold

[1. Trusler 2](#_Toc90488873)

[2. Farer 3](#_Toc90488874)

[3. Sårbarheter 4](#_Toc90488875)

# Trusler

**Motivasjon, vilje og kapasitet og trusselnivå:**

Bruk kodene SH=Svært høy; H=Høy; M=Moderat; L=Lav; IA=ingen aning.

Bruk eget skjønn på kodevalgene ut fra hva dere vet og tror om trusselaktørene.

Fyll ut merknadsfeltet der dere mener trusselaktørene har et klart motiv.

Etter vurdering av alle aktørene: Merk, f.eks. med gul farge, radene med de høyeste trusselnivåene. De blir da lettere å identifisere ved senere bruk av vurderingen.

**Kunnskapsstyrke:**

Sett kodene H=Høy; M=Moderat; L=Lav

|  | Grunnlag | | | Konklusjon | | Merknad |
| --- | --- | --- | --- | --- | --- | --- |
|  | Intensjon | | Kapa­sitet | Trussel­nivå | Kunnskaps­styrke |
| Trusselaktør | Motiv | Vilje |
| Utro tjenere internt i virksomheten |  |  |  |  |  |  |
| Utro tjenere hos ekstern databehandler |  |  |  |  |  |  |
| Forfølgere av trusselutsatte personer |  |  |  |  |  |  |
| Vinningskriminelle |  |  |  |  |  |  |
| Pøbel |  |  |  |  |  |  |
| Hacktivister |  |  |  |  |  |  |
| Fremmed makt (land) |  |  |  |  |  |  |
| Terrorister |  |  |  |  |  |  |
| (Andre?) |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# Farer

**Innledende sannsynlighet og forventet skadenivå:**

Bruk kodene SH=Svært høy; H=Høy; M=Moderat; L=Lav; IA=ingen aning.

Bruk eget skjønn på kodevalgene ut fra hva dere vet og tror om farekildene og stedene.

Fyll ut merknadsfeltet med eventuelle spesielle forhold dere kjenner til som påvirker sannsynlighet og skadenivå.

Etter vurdering av aktuelle farekilder og steder: Merk, f.eks. med gul farge, radene med de høyeste kombinasjonene av innledende sannsynlighet og forventet skadenivå. De blir da lettere å identifisere ved senere bruk av vurderingen.

**Kunnskapsstyrke:**

Sett kodene H=Høy; M=Moderat; L=Lav

| Farekilde | Sted | Innledende sannsynlighet | Forventet skadenivå | Kunnskaps­styrke | Merknad |
| --- | --- | --- | --- | --- | --- |
| Brann | Hos ekstern databehandler |  |  |  |  |
| Brann | I eget serverrom |  |  |  |  |
| Brann | I arbeidslokaler |  |  |  |  |
| Vannlekkasje | Hos ekstern databehandler |  |  |  |  |
| Vannlekkasje | I eget serverrom |  |  |  |  |
| Vannlekkasje | I arbeidslokaler |  |  |  |  |
| Annen naturhendelse | Hos ekstern databehandler |  |  |  |  |
| Annen naturhendelse | I eget serverrom |  |  |  |  |
| Annen naturhendelse | I arbeidslokaler |  |  |  |  |
| Annen hendelse | I nærområdet |  |  |  |  |
| (Andre?) | (Andre?) |  |  |  |  |
|  |  |  |  |  |  |

# Sårbarheter

Se på de av områdene under som dere vet eller burde vite noe om, eller som dere ellers har synspunkter på.

**Sårbarhetsnivå:**

Bruk kodene SH=Svært høy; H=Høy; M=Moderat; L=Lav; IA=ingen aning.

Bruk eget skjønn på kodevalgene ut fra hva dere vet og tror om status under de ulike områdene.

Oppsummer ved å anslå et **samlet** sårbarhetsnivå for området.

Fyll ut merknadsfeltet med eventuelle spesielle forhold dere kjenner til som påvirker deres vurdering av status og sårbarhetsnivå.

Etter den samlede vurderingen: Merk, f.eks. med gul farge, radene med sårbarhetsnivå Svært høy (SH) eller høy (H). De blir da lettere å identifisere ved senere bruk av vurderingen.

**Kunnskapsstyrke:**

Sett kodene H=Høy; M=Moderat; L=Lav

| Område /  Sentrale målsetninger for området | Sårbarhets-nivå | Kunnskaps­­styrke | Merknad |
| --- | --- | --- | --- |
| 1) Egen organisatoriske enhet |  |  |  |
| Lederne har og følger gode rutiner for å gi, endre og fjerne brukernes tilgang og rettigheter til IKT-system |  |  |  |
| Klare prosedyrer og rutiner for arbeidet generelt og bruken av ulike IKT-løsninger spesielt |  |  |  |
| Ansatte rapporterer alltid sikkerhetsbrudd og andre uønskede hendelser |  |  |  |
| Lederne har systematisk oppfølging av rapporterte sikkerhetsbrudd og uønskede hendelser |  |  |  |
| God kompetanse blant lederne og ansatte mht. info.sikkerhet generelt og gjeldende rutiner spesielt |  |  |  |
| God kultur blant lederne og ansatte mht. viktighet av informasjonssikkerhet og etterlevelse av gjeldende sikkerhetstiltak/krav |  |  |  |
| Annet? |  |  |  |
| 2) Viktige IKT-system der man selv er systemeier |  |  |  |
| God brukerinvolvering i anskaffelser, forbedringer og risikovurderinger |  |  |  |
| Systemene er godt tilpasset arbeidsoppgavene og gir ikke behov for å finne personlige omveier |  |  |  |
| Små muligheter for å gjøre feil med vesentlige konsekvenser |  |  |  |
| Profesjonelt utviklede |  |  |  |
| God oppfølging av feil og svakheter, fra identifisering til innrapportering og forbedring. |  |  |  |
| Systematisk vedlikeholdt og oppdatert |  |  |  |
| Tilfredsstillende oppetider (tilgjengelighet) |  |  |  |
| Gode løsninger og rutiner for pålogging, tilgangs- og rettighetsstyring |  |  |  |
| Gode løsninger og rutiner for administratortilgang til systemet selv, databaser mv. |  |  |  |
| Kryptering der det er nødvendig |  |  |  |
| Systematisk overvåking der det er nødvendig |  |  |  |
| Tilfredsstillende logger som enkelt kan følges opp |  |  |  |
| Systematisk oppfølging av logger der det er nødvendig |  |  |  |
| Annet? |  |  |  |
| 3) Viktige IKT-system der andre er systemeiere |  |  |  |
| God brukerinvolvering i anskaffelser, forbedringer og risikovurderinger |  |  |  |
| Systemene er godt tilpasset arbeidsoppgavene og gir ikke behov for å finne personlige omveier |  |  |  |
| Små muligheter for å gjøre feil med vesentlige konsekvenser |  |  |  |
| Profesjonelt utviklede |  |  |  |
| God oppfølging av feil og svakheter, fra identifisering til innrapportering og forbedring. |  |  |  |
| Systematisk vedlikeholdt og oppdatert |  |  |  |
| Tilfredsstillende oppetider (tilgjengelighet) |  |  |  |
| Gode løsninger og rutiner for pålogging, tilgangs- og rettighetsstyring |  |  |  |
| Gode løsninger og rutiner for administratortilgang til systemet selv, databaser mv. |  |  |  |
| Kryptering der det er nødvendig |  |  |  |
| Systematisk overvåking der det er nødvendig |  |  |  |
| Tilfredsstillende logger som enkelt kan følges opp |  |  |  |
| Systematisk oppfølging av logger der det er nødvendig |  |  |  |
| Annet? |  |  |  |
| 4) Virksomhetens utstyr, kommunikasjonsløsninger og datatjenester forøvrig |  |  |  |
| God brukerinvolvering i anskaffelser, forbedringer og risikovurderinger |  |  |  |
| Godt tilpasset arbeidsoppgavene og gir ikke behov for å finne personlige omveier |  |  |  |
| Små muligheter for å gjøre feil med vesentlige konsekvenser |  |  |  |
| Profesjonelt utviklede |  |  |  |
| God oppfølging av feil og svakheter, fra identifisering til innrapportering og forbedring. |  |  |  |
| Systematisk vedlikeholdt og oppdatert |  |  |  |
| Tilfredsstillende oppetider (tilgjengelighet) |  |  |  |
| Gode løsninger og rutiner for pålogging, tilgangs- og rettighetsstyring |  |  |  |
| Gode løsninger og rutiner for administratortilgang |  |  |  |
| Kryptering der det er nødvendig |  |  |  |
| Systematisk overvåking der det er nødvendig |  |  |  |
| Tilfredsstillende logger som enkelt kan følges opp |  |  |  |
| Systematisk oppfølging av logger der det er nødvendig |  |  |  |
| Annet? |  |  |  |
| 6) Fysisk adgang |  |  |  |
| God brukerinvolvering i bygningsmessig tilrettelegging |  |  |  |
| De bygningsmessig løsningene er godt tilpasset arbeidsoppgavene |  |  |  |
| Gode løsninger og rutiner for adgangskontroll |  |  |  |
| God oppfølging av feil og svakheter, fra identifisering til innrapportering og forbedring. |  |  |  |
| Systematisk vedlikeholdt og oppdatert |  |  |  |
| Systematisk overvåking der det er nødvendig |  |  |  |
| Tilfredsstillende logger som enkelt kan følges opp |  |  |  |
| Systematisk oppfølging av logger der det er nødvendig |  |  |  |
| Kontrollert tilgang til papirer med spesielle krav til konfidensialitet, integritet eller tilgjengelighet |  |  |  |
| Kontroll på hvem som hører konfidensielle samtaler |  |  |  |
| På kontoret: Kontrollert tilgang til utstyr som behandler informasjon med spesielle krav til konfidensialitet, integritet eller tilgjengelighet |  |  |  |
| På reise/hjemme: Kontrollert tilgang til utstyr som behandler informasjon med spesielle krav til konfidensialitet, integritet eller tilgjengelighet |  |  |  |
| Annet? |  |  |  |
| 7) Opplevelse av intern IKT-drift |  |  |  |
| Klare tjenestenivåavtaler som systematisk følges opp og der etterlevelse synliggjøres |  |  |  |
| Profesjonell organisasjon med høy kompetanse og gode systematiske rutiner som etterleves |  |  |  |
| Gjennomgående profesjonell og god service |  |  |  |
| Systematisk overvåking der det er nødvendig |  |  |  |
| Systematisk oppfølging av logger der det er nødvendig |  |  |  |
| Rask og god oppfølging av og tilbakemelding på rapporterte sikkerhetsbrudd og andre hendelser |  |  |  |
| Annet? |  |  |  |
| 8) Opplevelse av andre leverandører av IKT-tjenester vi benytter i våre oppgaver |  |  |  |
| Klare tjenestenivåavtaler som systematisk følges opp og der etterlevelse synliggjøres |  |  |  |
| Profesjonell organisasjon med høy kompetanse og gode systematiske rutiner som etterleves |  |  |  |
| Gjennomgående profesjonell og god service |  |  |  |
| Systematisk overvåking der det er nødvendig |  |  |  |
| Systematisk oppfølging av logger der det er nødvendig |  |  |  |
| Rask og god oppfølging av og tilbakemelding på rapporterte sikkerhetsbrudd og andre hendelser |  |  |  |
| Annet? |  |  |  |