Sjå rettleiinga for trinn 3 i foranalysen for rettleiing i gjennomføringa.

|  |  |  |
| --- | --- | --- |
| Organisatorisk eining: | |  |
| Ansvarsområde: | |  |
| Oppdateringar | | |
| Dato | Deltakarar | |
|  |  | |
|  |  | |
|  |  | |

Innhald

[1. Trugsmål 2](#_Toc90489339)

[2. Farar 3](#_Toc90489340)

[3. Sårbarheiter 4](#_Toc90489341)

# Trugsmål

**Motivasjon, vilje og kapasitet og trugsmålsnivå:**

Bruk kodane SH=Svært høg, H=Høg; M=Moderat; L=Låg; IA=inga aning.

Bruk eige skjøn på kodevala ut frå kva de veit og trur om trugsmålsaktørane.

Fyll ut merknadsfeltet der de meiner trugsmålsaktørane har eit klart motiv.

Etter vurdering av alle aktørane: Merk, t.d. med gul farge, radene med dei høgaste trugsmålsnivåa. Dei blir då lettare å identifisere ved seinare bruk av vurderinga.

**Kunnskapsstyrke:**

Set kodane H=Høg; M=Moderat; L=Låg

|  | Grunnlag | | | Konklusjon | | Merknad |
| --- | --- | --- | --- | --- | --- | --- |
|  | Intensjon | | Kapa-sitet | Trugsmåls-nivå | Kunnskaps-styrke |
| Trugsmålsaktør | Motiv | Vilje |
| Utru tenarar internt i verksemda |  |  |  |  |  |  |
| Utru tenarar hos ekstern databehandlar |  |  |  |  |  |  |
| Forfølgjarar av trugsmålsutsette personar |  |  |  |  |  |  |
| Vinningskriminelle |  |  |  |  |  |  |
| Pøbel |  |  |  |  |  |  |
| Hacktivistar |  |  |  |  |  |  |
| Framand makt (land) |  |  |  |  |  |  |
| Terroristar |  |  |  |  |  |  |
| (Andre?) |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# Farar

**Innleiande sannsyn og forventa skadenivå:**

Bruk kodane SH=Svært høg, H=Høg; M=Moderat; L=Låg; IA=inga aning.

Bruk eige skjøn på kodevala ut frå kva de veit og trur om farekjeldene og stadene.

Fyll ut merknadsfeltet med eventuelle spesielle tilhøve de kjenner til som påverkar sannsyn og skadenivå.

Etter vurdering av aktuelle farekjelder og stader: Merk, t.d. med gul farge, radene med dei høgaste kombinasjonane av innleiande sannsyn og forventa skadenivå. Dei blir då lettare å identifisere ved seinare bruk av vurderinga.

**Kunnskapsstyrke:**

Set kodane H=Høg; M=Moderat; L=Låg

| Farekjelde | Stad | Innleiande sannsyn | Forventa skadenivå | Kunnskapsstyrke | Merknad |
| --- | --- | --- | --- | --- | --- |
| Brann | Hos ekstern databehandlar |  |  |  |  |
| Brann | I eige sørvarrom |  |  |  |  |
| Brann | I arbeidslokale |  |  |  |  |
| Vasslekkasje | Hos ekstern databehandlar |  |  |  |  |
| Vasslekkasje | I eige sørvarrom |  |  |  |  |
| Vasslekkasje | I arbeidslokale |  |  |  |  |
| Anna naturhending | Hos ekstern databehandlar |  |  |  |  |
| Anna naturhending | I eige sørvarrom |  |  |  |  |
| Anna naturhending | I arbeidslokale |  |  |  |  |
| Anna hending | I nærområdet |  |  |  |  |
| (Andre?) | (Andre?) |  |  |  |  |
|  |  |  |  |  |  |

# Sårbarheiter

Sjå på dei av områda under som de veit eller burde vite noko om, eller som de elles har synspunkt på.

**Sårbarheitsnivå:**

Bruk kodane SH=Svært høg, H=Høg; M=Moderat; L=Låg; IA=inga aning.

Bruk eige skjøn på kodevala ut frå kva de veit og trur om status under dei ulike områda.

Oppsummer ved å **anslå** eit samla sårbarheitsnivå for området.

Fyll ut merknadsfeltet med eventuelle spesielle tilhøve de kjenner til som påverkar dykkar vurdering av status og sårbarheitsnivå.

Etter den samla vurderinga: Merk, t.d. med gul farge, radene med sårbarheitsnivå Svært høg (SH) eller høg (H). Dei blir då lettare å identifisere ved seinare bruk av vurderinga.

**Kunnskapsstyrke:**

Set kodane H=Høg; M=Moderat; L=Låg

| Område /  Sentrale målsetjingar for området | Sårbarheits-nivå | Kunnskaps-styrke | Merknad |
| --- | --- | --- | --- |
| 1) Eiga organisatoriske eining |  |  |  |
| Leiarane har og følgjer gode rutinar for å gje, endre og fjerne brukarane sine tilgangar og rettar til IKT-system. |  |  |  |
| Klare prosedyrar og rutinar for arbeidet generelt og bruken av ulike IKT-løysingar spesielt |  |  |  |
| Tilsette rapporterer alltid sikkerheitsbrot og andre uønskte hendingar |  |  |  |
| Leiarane har systematisk oppfølging av rapporterte sikkerheitsbrot og uønskte hendingar |  |  |  |
| God kompetanse blant leiarane og tilsette med tanke på info.sikkerheit generelt og gjeldande rutinar spesielt |  |  |  |
| God kultur blant leiarane og tilsette med tanke på at det viktige med informasjonssikkerheit og etterleving av gjeldande tryggingstiltak/krav |  |  |  |
| Anna? |  |  |  |
| 2) Viktige IKT-system der ein sjølv er systemeigar |  |  |  |
| God brukarinvolvering i anskaffingar, forbetringar og risikovurderingar |  |  |  |
| Systema er godt tilpassa arbeidsoppgåvene og gjev ikkje behov for å finne personlege omvegar |  |  |  |
| Små moglegheiter for å gjere feil med vesentlege konsekvensar |  |  |  |
| Profesjonelt utvikla |  |  |  |
| God oppfølging av feil og svakheiter, frå identifisering til innrapportering og forbetring. |  |  |  |
| Systematisk vedlikehalde og oppdatert |  |  |  |
| Tilfredsstillande oppetider (tilgjenge) |  |  |  |
| Gode løysingar og rutinar for pålogging, tilgangsstyring og styring av rettar |  |  |  |
| Gode løysingar og rutinar for administratortilgang til systemet sjølv, databasar mv. |  |  |  |
| Kryptering der det er naudsynt |  |  |  |
| Systematisk overvaking der det er naudsynt |  |  |  |
| Tilfredsstillande loggar som enkelt kan følgjast opp |  |  |  |
| Systematisk oppfølging av loggar der det er naudsynt |  |  |  |
| Anna? |  |  |  |
| 3) Viktige IKT-system der andre er systemeigarar |  |  |  |
| God brukarinvolvering i anskaffingar, forbetringar og risikovurderingar |  |  |  |
| Systema er godt tilpassa arbeidsoppgåvene og gjev ikkje behov for å finne personlege omvegar |  |  |  |
| Små moglegheiter for å gjere feil med vesentlege konsekvensar |  |  |  |
| Profesjonelt utvikla |  |  |  |
| God oppfølging av feil og svakheiter, frå identifisering til innrapportering og forbetring. |  |  |  |
| Systematisk vedlikehalde og oppdatert |  |  |  |
| Tilfredsstillande oppetider (tilgjenge) |  |  |  |
| Gode løysingar og rutinar for pålogging, tilgangsstyring og styring av rettar |  |  |  |
| Gode løysingar og rutinar for administratortilgang til systemet sjølv, databasar mv. |  |  |  |
| Kryptering der det er naudsynt |  |  |  |
| Systematisk overvaking der det er naudsynt |  |  |  |
| Tilfredsstillande loggar som enkelt kan følgjast opp |  |  |  |
| Systematisk oppfølging av loggar der det er naudsynt |  |  |  |
| Anna? |  |  |  |
| 4) Verksemda sitt utstyr, kommunikasjonsløysingar og andre datatenester |  |  |  |
| God brukarinvolvering i anskaffingar, forbetringar og risikovurderingar |  |  |  |
| Godt tilpassa arbeidsoppgåvene og gjev ikkje behov for å finne personlege omvegar |  |  |  |
| Små moglegheiter for å gjere feil med vesentlege konsekvensar |  |  |  |
| Profesjonelt utvikla |  |  |  |
| God oppfølging av feil og svakheiter, frå identifisering til innrapportering og forbetring. |  |  |  |
| Systematisk vedlikehalde og oppdatert |  |  |  |
| Tilfredsstillande oppetider (tilgjenge) |  |  |  |
| Gode løysingar og rutinar for pålogging, tilgangsstyring og styring av rettar |  |  |  |
| Gode løysingar og rutinar for administratortilgang |  |  |  |
| Kryptering der det er naudsynt |  |  |  |
| Systematisk overvaking der det er naudsynt |  |  |  |
| Tilfredsstillande loggar som enkelt kan følgjast opp |  |  |  |
| Systematisk oppfølging av loggar der det er naudsynt |  |  |  |
| Anna? |  |  |  |
| 6) Fysisk tilgang |  |  |  |
| God brukarinvolvering i bygningsmessig tilrettelegging |  |  |  |
| Dei bygningsmessige løysingane er godt tilpassa arbeidsoppgåvene |  |  |  |
| Gode løysingar og gode rutinar for tilgangskontroll |  |  |  |
| God oppfølging av feil og svakheiter, frå identifisering til innrapportering og forbetring. |  |  |  |
| Systematisk vedlikehalde og oppdatert |  |  |  |
| Systematisk overvaking der det er naudsynt |  |  |  |
| Tilfredsstillande loggar som enkelt kan følgjast opp |  |  |  |
| Systematisk oppfølging av loggar der det er naudsynt |  |  |  |
| Kontrollert tilgang til papir med spesielle krav til konfidensialitet, integritet eller tilgjenge |  |  |  |
| Kontroll på kven som høyrer konfidensielle samtalar |  |  |  |
| På kontoret: Kontrollert tilgang til utstyr som behandlar informasjon med spesielle krav til konfidensialitet, integritet eller tilgjenge |  |  |  |
| På reise/heime: Kontrollert tilgang til utstyr som behandlar informasjon med spesielle krav til konfidensialitet, integritet eller tilgjenge |  |  |  |
| Anna? |  |  |  |
| 7) Oppleving av internt IKT-drift |  |  |  |
| Klare tenestenivåavtalar som systematisk følgjast opp og der etterleving blir synleggjort |  |  |  |
| Profesjonell organisasjon med høg kompetanse og gode systematiske rutinar som blir etterlevde |  |  |  |
| Gjennomgåande profesjonell og god service |  |  |  |
| Systematisk overvaking der det er naudsynt |  |  |  |
| Systematisk oppfølging av loggar der det er naudsynt |  |  |  |
| Rask og god oppfølging og tilbakemelding på rapporterte sikkerheitsbrot og andre hendingar |  |  |  |
| Anna? |  |  |  |
| 8) Oppleving av andre leverandørar av IKT-tenester vi brukar i oppgåvene våre |  |  |  |
| Klare tenestenivåavtalar som systematisk følgjast opp og der etterleving blir synleggjort |  |  |  |
| Profesjonell organisasjon med høg kompetanse og gode systematiske rutinar som blir etterlevde |  |  |  |
| Gjennomgåande profesjonell og god service |  |  |  |
| Systematisk overvaking der det er naudsynt |  |  |  |
| Systematisk oppfølging av loggar der det er naudsynt |  |  |  |
| Rask og god oppfølging og tilbakemelding på rapporterte sikkerheitsbrot og andre hendingar |  |  |  |
| Anna? |  |  |  |