

Krav til sikkerhet

Innholdsfortegnelse

1. Formål	2
2. Personellsikkerhet	2
2.1. Screening	2
2.2. Konfidensialitet	2
2.3. Sikkerhetsopplæring og bevisstgjøring	2
2.4. Fjernarbeid	2
2.5. Sikkerhetsloven	3
3. Tilgangsstyring	3
3.1. Tilgang til Selskapet infrastruktur (remote)	4
3.2. Retningslinje og rutine for passord	4
4. Informasjonshåndtering	4
4.1. Klassifisering av informasjon	4
4.2. Sikringsforskriftens krav til informasjonshåndtering	6
4.3. Skjermingsverdig informasjon - Sikkerhetsloven	6
4.4. Persondata	6
4.5. Kryptering av data	6
4.6. Lagring av informasjon	7
4.7. Overføring av informasjon	7
4.8. Bruk av verdier	7
4.9. Tilbakelevering av verdier	7
5. Håndtering av (lagrings)medier	7
6. Fysisk sikkerhet	7
7. Hendelseshåndtering	7
7.1. Klassifisering av sikkerhetshendelser	7
7.2. Etablert prosess for hendelseshåndtering	9
7.3. Varsling av sikkerhetshendelser	10
8. Sikkerhet i egen IKT	10
8.1. Utvikle sikkerhet i egen IKT	10
9. Sikkerhet hos Underleverandører	10
10. Bruk av skytjenester i leveranser til Selskapet	11
11. Rapportering	11
12. Sikkerhetsrevisjon, -tilsyn og -inspeksjon	11
13. Lov- og regulatoriske krav	12

1. Formål

Sikkerhet i egne leveranser er viktig for Selskapet. Selskapet er underlagt flere regulatoriske krav som, i tillegg til eget Ledelsessystem for Informasjonssikkerhet, stiller krav til forsvarlig sikkerhet i og sikring av informasjon, informasjons- og kommunikasjonssystemer. Sikringsforskriften legger premiss om at Selskapet skal systematisk forebygge og håndtere uønskede handlinger og begrense konsekvensen av disse.

Dette sikkerhetsannekset ivaretar Selskapets minimumsnivå for forsvarlig Informasjonssikkerhet. Sikkerhetsannekset skal regulere Informasjonssikkerhet i Kontrakten nr. XXXXXX inngått mellom Selskapet og Leverandøren. Dette annekset regulerer digital Informasjonssikkerhet hos Leverandøren.

Er sikkerhetskrav beskrevet flere steder skal dette sikkerhetsannekset ha forrang ved tvister, hvis ikke annet er skriftlig avtalt.

2. Personellsikkerhet

2.1. Screening

Ved ansettelse skal Leverandøren ha en prosess for å verifisere den ansattes identitet før arbeidsavtalen signeres. Leverandøren skal verifisere at den ansatte har riktig faglig og praktisk kompetanse til å løse de oppgavene vedkommende er ansatt for å løse.

For særlig kritiske funksjoner, eksempelvis beslutningstaking eller funksjoner med utvidede tilgangrettigheter, skal Leverandøren vurdere den ansattes skikkethet for den tiltenkte rollen.

Tilganger til deler av Selskapets Informasjon, informasjonssystemer, infrastruktur og fysiske objekter vil kunne kreve autorisasjon og sikkerhetsklarering av personell, se kapittel 2.5.

2.2. Konfidensialitet

Leverandøren har ansvar for sine ansatte, deres handlinger og leveranser. Leverandøren skal ha etablert skriftlige arbeidsavtaler med sine ansatte som inkluderer konfidensialitetsklausuler om konfidensialitet om Selskapets informasjon, informasjonssystemer og øvrige verdier.

Konfidensialitetskravet om Selskapets informasjon, informasjonssystemer og øvrige verdier skal også gjelde etter at arbeidsforhold er terminert. Det er definert i taushetsplikterklæringen som signeres at denne gjelder uten tidsbegrensning, og hva som faller inn under denne.

2.3. Sikkerhetsopplæring og bevisstgjøring

Leverandøren skal ha et etablert program for sikkerhetsopplæring for ansatte og kontraktører i relevante sikkerhetspolicyer og -prosedyrer. Sikkerhetsopplæringen bør gjennomføres kontinuerlig og minimum årlig.

Dersom Selskapet krever en mer omfattende sikkerhetsopplæring enn Leverandøren tilbyr, skal Leverandøren sørge for at ansatte og kontraktører blir informert om, får opplæring og kjenner til sikkerhetskrav som er avtalt med Selskapet.

2.4. Fjernarbeid

Dersom Leverandørens ansatte har mulighet til å aksessere Selskapets infrastruktur og systemer gjennom Leverandørens egen infrastruktur fra andre steder enn egne kontorlokasjoner, skal Leverandøren ha etablert prosess for denne type fjernarbeid. Prosessen bør som minimum inneholde følgende krav til leverandørenes ansatte:

- En ansatt skal arbeide slik at man unngår at informasjon tilfaller uvedkommende eksempelvis ved «shoulder surfing».

- En ansatt skal ikke oppbevare/lagre informasjon som berører Selskapet på annen måte enn den som er avtalt.
- Det er påkrevd at ansatte skal benytte seg av VPN eller lignende når de utfører oppgaver på vegne av Selskapet.

Selskapet har begrensninger på hvor tilgang til Selskapets infrastruktur og systemer kan gjøres fra, disse begrensningene vil også gjelde for Leverandøren.

2.5. Sikkerhetsloven

Selskapet er underlagt sikkerhetsloven. Jernbanen er definert som en grunnleggende nasjonal funksjon (GNF), med underfunksjon jernbanedrift og trafikkstyring. Systemer, informasjonssystemer, infrastruktur og fysiske objekter som er avgjørende for å understøtte drift av jernbanen og styring av togtrafikk er omfattet og vil kunne bli utpekt som skjermingsverdig etter sikkerhetsloven. Det er gjennomført en kartlegging av systemer som er avgjørende for drift og styring av jernbanen og togtrafikken. Informasjonen er oversendt til Samferdselsdepartementet, som vil foreta en endelig utpeking og kategorisering av systemer, infrastruktur og fysiske objekter som skal omfattes.

For Informasjon, informasjonssystemer, infrastruktur og fysiske objekter som er skjermingsverdig vil følgende krav til Leverandørens personell (herunder Underleverandørers personell) gjelde:

- **Logisk tilgang** til et utpekt system vil kunne utløse krav om autorisasjon eller klarering og autorisasjon avhengig av kategoriseringen av systemet.
- **Fysisk adgang** til teknisk rom hvor systemet er innplassert vil kunne utløse krav om adgangsklarering eller klarering og autorisasjon avhengig av klassifiseringen til det tekniske rommet.
- **Skjermingsverdig informasjon** skal beskyttes iht. Sikkerhetsloven, se kapittel 4.3.
- Myndighetene har hjemmel i lov til å gjennomføre **tilsyn og revisjon** på virksomheter som er underlagt sikkerhetsloven. Selskapet må kontraktsfeste tilsvarende tilsyns- og revisjonskrav med sine leverandører som har tilgang og/eller adgang til utpekte systemer, infrastruktur og fysiske objekter, samt logisk og fysisk tilgang til skjermingsverdig informasjon.

Får Leverandøren tilgang til sikkerhetsgradert informasjon eller skjermingsverdig objekt eller infrastruktur, må Leverandøren inngå en sikkerhetsavtale iht. standard definert av Norske myndigheter¹.

3. Tilgangsstyring

Leverandøren skal ha etablert prosess for tilgangsstyring til systemer eller tjenester hvor Leverandøren behandler og lagrer Selskapets informasjon eller informasjon om Selskapet. Etablert prosess bør som minimum inkludere;

- Begrenset antall ledere som kan godkjenne og tildele (nye) brukere
- Tilganger skal kun tildeles brukere med tjenstlig behov
- Tilganger med privilegerte rettigheter skal begrenses til et minimum
- En oversikt over alle brukertilganger Leverandøren har hos Selskapet
- Selskapet skal, på forespørsel, få tilgang til oversikt over brukertilganger
- Tilganger skal revideres med en jevnlig frekvens (minimum hvert kvartal)
- Tilganger er personlig og skal ikke deles
- Tilganger skal termineres ved opphør av ansettelsesforhold

¹ Mal for sikkerhetsavtaler: <https://nsm.no/sok/?q=sikkerhetsavtale>

Leverandøren skal på forespørsel fra Selskapet fremlegge og dokumentere prosedyre for tilgangsstyring.

3.1. Tilgang til Selskapets infrastruktur (remote)

Har Leverandøren behov for tilgang til Selskapets systemer eller infrastruktur må Leverandøren godta Selskapets til enhver tid gjeldende policyer, prosesser og retningslinjer for slik tilgang:

- Leverandørens personell skal følge Selskapets instruks for sikker bruk for eksterne partnere
- Privilegerte brukere skal i tillegg til ovennevnt punkt følge Selskapets prosedyre for tilgangsstyring for privilegerte brukere
- Fjerntilgang skal kun tillates via Selskapets standard plattform for fjerntilgang.
- Fjerntilgang til Selskapets interne tjenester, systemer og infrastruktur i alle miljøer skal sikres ved bruk av multifaktorautentisering.
- Tilganger gis generelt med tidsbegrensning
- Tilganger gjennomgås med en frekvens / periodisk
- Leverandøren skal uten ugrunnet opphold varsle Selskapet ved mistanke om eller bekreftet uautorisert tilgang, passord eller brukernavn på avveie, m.m.

3.2. Retningslinje og rutine for passord

Leverandøren skal ha etablert retningslinjer og rutiner for passord og passordhåndtering. Selskapet følger anbefalingene til Nasjonale Sikkerhetsmyndighet (NSM) for passord og passordhåndtering, Leverandøren skal ha retningslinjer og rutiner for passord og passordhåndtering som et minimum møter disse anbefalingene ².

Retningslinjer og rutiner for passord og passordhåndtering skal også inneholde rutine for endring eller sletting av kompromitterte passord.

4. Informasjonshåndtering

4.1. Klassifisering av informasjon

Selskapet har definert 3 nivåer for klassifisering av informasjon, åpen, intern og sensitiv, se tabell 1 nedenfor. Leverandøren skal håndtere informasjon på tilsvarende måter som angitt i tabell 2 eller bedre enn Selskapet.

Tabell 1.

Nivå	Beskrivelse/Definisjoner	Eksempler
Åpen	Dette er informasjon som kan være tilgjengelig for lesing for offentligheten, inkludert presse og publikum. Hvis informasjonen kommer på avveier, vil det ikke forårsake skade for Selskapet, samarbeidspartnere og/eller publikum.	• Produktbeskrivelser • Regelverk og bestemmelser • Trasévalg etter beslutning • Kantinemenyen
Intern	Intern er standardklassifisering. Dette er informasjon som kan være tilgjengelig for alle i	• Organisasjonskart med navn

² Råd og anbefalinger om passord: <https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/rad-og-anbefalinger-om-passord>

Nivå	Beskrivelse/Definisjoner	Eksempler
	Selskapet inkludert ansatte, innleide og samarbeidspartnere. Intern kan også begrenses til f.eks. divisjoner, avdelinger og prosjekter. Hvis informasjonen kommer på avveier, kan det forårsake noe skade for Selskapet, partnere og/eller publikum.	• Prosedyrer og rutinebeskrivelser • Informasjon fra ledelsen til alle medarbeidere
Sensitiv	Dette er informasjon som kun skal være tilgjengelig for en begrenset gruppe autoriserte ansatte, innleide og samarbeidspartnere med tjenstlig behov. Dette kan være en spesiell avdeling, et program, et prosjekt, deler av et prosjekt, ledergrupper etc. Informasjonseier avgjør hvem som skal ha tilgang. Hvis informasjonen kommer på avveier, kan dette kunne føre til skade for Selskapet, medarbeidere, samarbeidspartnere og/eller publikum.	• Møtereferater fra konsernledelsen • Risiko og sårbarhet om våre digitale løsninger, objekter og infrastruktur • Konkurransemessige forhold • Særlige kategorier av personopplysninger • Dokumentasjon tilhørende prosjektleveranser • Skjermingsverdig informasjon iht. Sikringsforskriften

Tabell 2.

Nivå	Merking	Lagring	Behandling	Sletting/ Makulering
Åpen	Nei	Ingen begrensninger på lagring.	Ingen begrensninger på behandling.	Ingen krav til sletting/ makulering.
Intern	Dokumenter merkes på forsiden og alle sider. Elektronisk informasjon skal merkes.	Kan lagres på Selskapets godkjente løsninger. Ikke krav om kryptering ved lagring. Kan lagres ukryptert på eksterne lagringsmedier. Informasjonen skal ikke lagres på eksterne tjenester som ikke er forhåndsgodkjente av Selskapet.	Ikke krav om å kryptere ved sending av e-post internt og eksternt. Fysiske dokumenter kan sendes med vanlig post i lukket konvolutt.	Informasjon slettes/makuleres når behandling er fullført og tjenstlig behov ikke tilsier fortsatt lagring.

Nivå	Merking	Lagring	Behandling	Sletting/ Makulering
		Fysiske dokumenter skal alltid oppbevares under kontroll.		
Sensitiv	Dokumenter merkes på forsiden og alle sider. Elektronisk informasjon skal merkes. Dokumenter/lagringsmedier med skjermingsverdig informasjon skal merkes med rød tekst "Skjernet iht Sikringsforskriften §§ 3-3, 3-4"	Informasjon skal krypteres og lagres på tilgangsbegrensede områder. Informasjonen skal ikke lagres på eksterne tjenester som ikke er forhåndsgodkjente av Selskapet. Fysiske dokumenter oppbevares under kontroll i autorisert personells varetekt eller i låst skap.	Tilgang til behandling av informasjon skal begrenses til tjenstlig behov inkl. innsyn på skjerm og sikring av informasjon i form av tale. Informasjonen skal ikke sendes til privat e-post adresse. Informasjonen skal krypteres ved sending. Fysiske dokumenter og lagringsmedier kan sendes med vanlig post i hhv. lukket og umerket konvolutt/emballasje.	Informasjon slettes/makuleres når behandling er fullført og tjenstlig behov ikke tilsier fortsatt lagring. Lagringsmedier med skjermingsverdig informasjon skal avhendes slik at informasjonen ikke kan gjenfinnes, eksempelvis ved destruksjon eller formatering

4.2. Sikringsforskriftens krav til informasjonshåndtering

Selskapet er, i forskrift om sikring på jernbane (sikringsforskriften), pålagt og arbeide systematisk for å forebygge og håndtere tilsiktede uønskede handlinger og begrense konsekvensene av dem. Dette betyr at all type informasjon som kan utnyttes til tilsiktede uønskede handlinger skal sikres slik at konfidensialitet, integritet og tilgjengelighet ivaretas.

Alle som får eller har hatt tilgang til informasjon underlagt sikringsforskriften har taushetsplikt.

4.3. Skjermingsverdig informasjon - Sikkerhetsloven

Informasjon er skjermingsverdig dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.

Skjermingsverdig informasjon skal beskyttes iht. Sikkerhetsloven og tilgang til dette, digitalt eller fysisk (papir), krever autorisasjon eller klarering og autorisasjon avhengig av informasjonsklassifisering.

4.4. Persondata

Før Leverandøren får tilgang til eller starter behandling av persondata skal det etableres og signeres en databehandlingsavtale (DPA).

4.5. Kryptering av data

Leverandøren skal ha etablert kryptografiske mekanismer, basert på beste praksis, for beskyttelse av informasjon, både i ro og i transitt.

Leverandøren skal på forespørsel fra Selskapet fremlegge beskrivelse av kryptografiske mekanismer etablert og innført.

4.6. Lagring av informasjon

Selskapets informasjon skal fortrinnsvis lagres i Norge, og ikke utenfor EU/EØS.

Regulatoriske krav, som sikkerhetsloven, krav om nasjonal autonomi, vil sette føringer for hvor data kan lagres.

4.7. Overføring av informasjon

Informasjon klassifisert som sensitiv skal krypteres ved overføring, se kapittel 5.1 Klassifisering av informasjon.

4.8. Bruk av verdier

Leverandøren skal ikke benytte tilgang til Selskapets IKT-verdier (systemer, fysisk IKT-objekter, IKT-infrastruktur og IKT-utstyr) og informasjon på andre måter enn det som er avtalt.

4.9. Tilbakelevering av verdier

Når avtalen utløper eller termineres skal Leverandøren levere tilbake Selskapets informasjon, inkludert konfigurasjon og dokumentasjon som naturlig hører til leveransen, på et format som Selskapet bestemmer, slik at leveransen kan videreføres enten hos Selskapet selv eller ved valg av ny Leverandør.

5. Håndtering av (lagrings)medier

Leverandøren skal ha etablert og innført prosedyrer for forvaltning av medier, harddisker, minnepinner, andre lagringsmedier osv., som ivaretar konfidensialiteten og integriteten til lagring av Selskapets informasjon. Prosedyren skal inkludere beskrivelse av sikker avhending av medier.

IKT-utstyr som tilhører Selskapet, skal leveres tilbake til Selskapet for sletting av informasjon og programvare når utstyret ikke lenger benyttes.

Leverandøren skal på forespørsel fremlegge prosedyre for håndtering av medier.

6. Fysisk sikkerhet

Leverandøren skal påse at fysisk sikkerhet og adgangskontroll knyttet til fysiske objekter som brukes til aktiviteter for Selskapet, er tilstrekkelig sikret. Selskapets informasjon og systemer skal være sikret mot miljørelaterte (brann, oversvømmelse, høye temperaturer, osv.) og menneskerelaterte (innbrudd, sabotasje, tyveri, brann, uhell osv.) skader og påvirkninger. Adgangskontroll skal sikre at kun autorisert personell har adgang til Leverandørens fysiske områder.

Leverandøren skal på forespørsel fremlegge oversikt over fysiske sikringstiltak som er implementert.

7. Hendelseshåndtering

En digital sikkerhetshendelse er definert som en hendelse som kompromitterer konfidensialiteten, integriteten eller tilgjengeligheten til et system, eller informasjon.

Digitale sikkerhetshendelser inkluderer;

- Brudd på lovverk
- Hendelser som kompromitterer fysisk sikkerhet
- IKT-sikkerhetshendelser, eks. brudd på bruk av Selskapets identitet i digitale angrepskampanjer
- Brudd på avtale/kontrakt med Selskapet

7.1. Klassifisering av sikkerhetshendelser

Selskapet klassifiserer sikkerhetshendelser i følgende kategorier;

- **Svært alvorlig**

- Brudd på systemets tilgjengelighet får umiddelbar konsekvens for Selskapets samfunnskritiske funksjon:
 - Systemet har direkte betydning for togframføring - Systemstans medfører stans i togframføring innen 24 timer (som definert av Selskapets grunnleggende nasjonale funksjoner - GNF)
- Brudd på konfidensialitet kan få alvorlige konsekvenser for Selskapet eller samarbeidspartneres måloppnåelse, evne til å etterkomme lover og myndighetsgitte pålegg eller for Selskapets offentlige omdømme:
 - Systemet behandler dokumentasjon/informasjon om samfunnskritiske systemer (som definert av Selskapets grunnleggende nasjonale funksjoner - GNF)
 - Systemet behandler dokumentasjon/informasjon om samfunnskritiske systemers underliggende infrastruktur
 - Systemet er en infrastrukturtjeneste som behandler (lagrer, transporterer eller prosesserer) informasjon tilhørende andre systemer
 - Systemet inneholder beskrivelser av risiko, sårbarheter eller tilhørende tiltak
 - Brudd på konfidensialitet kan være konkurransevridende for Selskapets leverandører og samarbeidspartnere
 - Systemet inneholder informasjon om bosted for personer med fortrolig eller strengt fortrolig adresse
 - Systemet behandler informasjon klassifisert som 'Sensitiv'
- Brudd på integritet kan medføre feilvurderinger som gir alvorlige konsekvenser for Selskapet eller samarbeidspartneres måloppnåelse, evne til å etterkomme lover og myndighetsgitte pålegg eller for Selskapets offentlige omdømme:
 - Systemet inneholder informasjon som benyttes i trafikkavvikling
 - Systemet er en infrastrukturtjeneste som behandler (genererer, lagrer, transporterer eller prosesserer) informasjon som avleveres til andre systemer
 - Systemet ivaretar sikkerhetslogging
 - Systemet er et regnskapssystem
 - Systemet håndterer tilgangsstyring for flere andre Selskapet systemer
- Brudd på personvern kan medføre alvorlig skade for Selskapet eller den registrerte:
 - Systemet behandler personopplysninger om mer enn 10.000 registrerte
 - Systemet behandler særlige kategorier av personopplysninger eller opplysninger om straffedommer/ lovovertridelser om mer enn 100 registrerte
 - Systemet lagrer bilde- eller videoopptak av identifiserbare personer
 - Systemet utfører analyse av personopplysninger for å avdekke adferd, preferanser, evner eller behov for mer enn 100 registrerte

- **Alvorlig**

- Brudd på systemets tilgjengelighet kan få konsekvens for Selskapets samfunnskritiske funksjon eller andre virksomhetskritiske funksjoner:
 - Systemet har indirekte betydning for togframføring - Systemstans kan medføre stans i togframføring etter mer enn 24 timer (som definert av Selskapets grunnleggende nasjonale funksjoner - GNF)
- Systemstans kan medføre stans i Selskapets virksomhetskritiske funksjoner:
 - Systemstans kan gi økonomiske tap over 100 mill. NOK

- Systemet er et primært arbeidsverktøy, eller understøtter primære arbeidsverktøy, for mer enn 200 ansatte
 - Systemet er viktig for Selskapets evne til å håndtere en krise eller sikkerhetstruende hendelse
 - Systemet utfører myndighetspålagt rapportering
- Brudd på konfidensialitet kan få konsekvenser for Selskapet eller samarbeidspartneres måloppnåelse, evne til å etterkomme lover og myndighetsgitte pålegg eller for Selskapets offentlige omdømme:
 - Brudd på konfidensialitet kan medføre foretraksstraff, overtredelsesgebyr, pålegg eller skriftlig advarsel fra tilsynsmyndighet
 - Systemet behandler informasjon unntatt offentlighet
 - Systemet behandler informasjon klassifisert som 'Intern'
- Brudd på integritet kan medføre feilvurderinger som gir konsekvenser for Selskapet eller samarbeidspartneres måloppnåelse, evne til å etterkomme lover og myndighetsgitte pålegg eller for Selskapets offentlige omdømme:
 - Brudd på integritet kan medføre foretraksstraff, pålegg eller skriftlig advarsel fra tilsynsmyndighet
 - Alle systemer som leverer data til eksterne partnere eller til publikum
- Brudd på personvern kan medføre skade for Selskapet eller den registrerte:
 - Systemet behandler særlige kategorier av personopplysninger eller opplysninger om straffedommer/lovovertridelser om mindre enn 100 registrerte
- **Lav**
 - Brudd på systemets tilgjengelighet får ikke konsekvens for Selskapets samfunnskritiske funksjon eller virksomhetskritiske funksjoner
 - Brudd på konfidensialitet vil i liten til ingen grad få konsekvenser for Selskapets måloppnåelse, evne til å etterkomme lover og myndighetsgitte pålegg eller for Selskapets offentlige omdømme:
 - Systemet behandler informasjon klassifisert som Åpen
 - Systemet behandler informasjon hvor brudd på konfidensialitet vil få ingen eller ubetydelige konsekvenser
 - Brudd på integritet vil i liten til ingen grad få konsekvenser for Selskapets måloppnåelse, evne til å etterkomme lover og myndighetsgitte pålegg eller for Selskapets offentlige omdømme
 - Brudd på personvern vil i liten til ingen grad medføre skade, eller systemet behandler ikke personopplysninger utover følgende kategorier:
 - Brukernavn, navn, e-post og evt. tilhørende passord, (og systemets logg oppfyller følgende: logg om enkeltpersoner er ren operatørlogg som kun viser operatørens interaksjon med systemet)
 - Navn og kontaktinformasjon (e-post, telefon) til kunder eller Leverandørers representanter i kundeforholdet

7.2. Etablert prosess for hendelseshåndtering

Leverandøren skal ha etablert prosess for hendelseshåndtering for raskt og effektivt kunne håndtere sikkerhetshendelser på en konsistent og strukturert måte. Prosess for hendelseshåndtering skal inkludere løpende kommunikasjon og oppdatering til Selskapet. Prosedyren bør også inkludere krav til registrering, vurdering, rapportering og læring av sikkerhetshendelser.

Leverandøren skal på forespørsel fremlegge dokumentasjon av prosess for hendelseshåndtering.

7.3. Varsling av sikkerhetshendelser

Leverandøren skal ha en etablert prosess for varsling av sikkerhetshendelser. Dersom det oppstår en svært alvorlig eller alvorlig sikkerhetshendelse som påvirker eller kan påvirke sikkerheten til Selskapet skal Leverandøren uten ugrunnet opphold og senest 6 timer etter hendelsen er oppdaget varsle Selskapet.

Leverandøren skal, etter at sikkerhetshendelse er varslet, rapportere skriftlig til Selskapet status på sikkerhetshendelsen. En slik rapportering skal inneholde;

- Beskrivelse av hendelsen
- Når hendelsen inntraff
- Hva som forårsaket hendelsen
- Hvilke tiltak som iverksettes for å minimere konsekvens av hendelsen
- Beskrivelse hvordan hendelsen skal løses
- Når løsning av hendelsen foreligger

8. Sikkerhet i egen IKT

Leverandøren er ansvarlig for implementering av relevante sikkerhetsmekanismer i egen IKT for å ivareta konfidensialitet, integritet og tilgjengelighet for Selskapets verdier (informasjon, informasjonssystemer og objekter).

Leverandøren skal som et minimum ha etablert sikkerhetsmekanismer for;

- Beskyttelse av endepunkter, inkludert PC, nettbrett, servere m.m., som jevnlig oppdateres automatisk
- Prosedyre og rutine for sikkerhetsheding
- Prosedyre og rutine for sikkerhetsoppdateringer
- Etablert IDS med anomalideteksjon
- Etablert IPS
- Etablert brannmur (Next Generation FW) med lag 7 overvåking

8.1. Utvikle sikkerhet i egen IKT

Leverandøren er ansvarlig for sikkerhet i eget IKT-miljø og en ansvarlige for å påse at de følger med på endring i trusselbilde og gjør endringer, slik at sikkerheten i egen IKT ikke forringes/forvitres over tid

Leverandøren skal på forespørsel fra Selskapet presentere en overordnet oversikt over sine tiltak for sikkerhet i sine IKT-miljøer.

Leverandøren bør ha tilstrekkelige kapabiliteter og kompetanse for analyse av sikkerhetslogger og alarmer.

9. Sikkerhet hos Underleverandører

Leverandøren er ansvarlig for sine Underleverandører og plikter å speile sikkerhetskravene eller tilsvarende sikkerhetskrav inngått i denne avtalen med Underleverandører. Selskapet skal ha rett til å se etablerte sikkerhetskrav mellom Leverandøren og underleverandør.

Leverandøren skal presentere oversikt over Underleverandører som har delleveranser eller har vesentlig leveranser i leveransen(e) til Selskapet. Selskapet forbeholder seg retten til å nekte bruk av Underleverandører i leveransen(e) til Selskapet hvis bruk av disse Underleverandørene medfører en økt risiko for Selskapet, brudd på Selskapets policyer, retningslinjer, prosedyre eller lovbrudd.

Leverandøren skal varsle Selskapet ved endringer i bruk av Underleverandører.

10. Bruk av skytjenester i leveranser til Selskapet

Dersom Leverandøren benytter seg av skytjenester i leveransene til Selskapet, skal bruken og sikringen av disse som et minimum være i henhold til Selskapets prinsipper og krav for bruk av skytjenester. Det skal kun benyttes skytjenester/-leverandører som er forhåndsgodkjent av Selskapet.

Før bruk av skytjenester godkjennes, må det sammen med Selskapet gjøres en vurdering av om lover og reguleringer tillater at det benyttes skytjenester i det bestemte tilfellet. I vurderingen av om skytjenester kan benyttes vil det først og fremst være viktig å vurdere hvilke informasjonsverdier som kan inngå i systemet og hvilke konfidensialitets-, integritets- og tilgjengelighetskrav man har til disse. Det kan også være relevant å vurdere hvilke tilgjengelighetskrav man har til oppgavene eller funksjonene systemet støtter. Det kan for eksempel ikke benyttes skytjenester i tilfeller hvor det håndteres gradert informasjon etter sikkerhetsloven.

Det bør stilles krav til følgende områder (se tabell). Hvilke krav som stilles i de ulike kategoriene vil være situasjonsbetinget.

- Sikkerhetskopi
- Kryptering
- Segregering
- Portabilitet
- Tilgangsstyring
- Sletting
- Fysisk tilgangsstyring
- Logging
- Sikring mot dataangrep
- Monitorering

Dersom Leverandøren har Underleverandører som benytter skytjenester, skal også bruken og sikringen av disse være i henhold til Selskapets prinsipper og krav for bruk av skytjenester.

11. Rapportering

Selskapet vil i løpet av kontraktperioden sende én eller flere, men ikke oftere enn en gang i året, egenvurderinger av sikkerhetsstauts ut til Leverandørene. Leverandøren forplikter seg til å besvare egenvurderingene når dette blir forespurt. Disse vil inneholde vurderinger knyttet til regulerte og avtalte sikkerhetskrav i dette annekset.

12. Sikkerhetsrevisjon, -tilsyn og -inspeksjon

Selskapet har rett til å gjennomføre sikkerhetsrevisjon, -tilsyn og -inspeksjon av Leverandøren, herunder av tjenester og/eller funksjoner som er i sammenheng med tjenestene som leveres. Leverandøren kan ikke nekte Selskapet retten til å gjennomføre sikkerhetsrevisjon, -tilsyn og -inspeksjon.

Selskapet er underlagt flere regulatoriske krav, eksempelvis Jernbaneloven med forskrifter, Sikkerhetsloven, ekomloven m.fl. Disse regulatoriske krav gir jernbanemyndigheten rett til å gjennomføre sikkerhetsrevisjon, -tilsyn og -inspeksjon av Selskapet og Selskapets Leverandører. Leverandører må være forberedt på at krav om sikkerhetsrevisjon, -tilsyn og -inspeksjon fra jernbanemyndighetene kan forekomme.

Selskapets rett til å gjennomføre sikkerhetsrevisjon, -tilsyn og -inspeksjon vil være begrenset til en gang per kalenderår. Ved gjentatte sikkerhetshendelser, hos Leverandøren eller i leveransen til Selskapet, vil Selskapet ha rett til å gjennomføre sikkerhetsrevisjon, -tilsyn og -inspeksjon oftere enn en gang per kalenderår. Første mulighet til å gjennomføre revisjon er ett år etter signering av kontrakt.

Selskapet har rett til å benytte en tredjepart, valgt av Selskapet, til å gjennomføre sikkerhetsrevisjon, -tilsyn og -inspeksjon. Selskapet skal ikke velge en tredjepart til å gjennomføre sikkerhetsrevisjon, -tilsyn og -inspeksjon som er i direkte konkurranse med Leverandøren.

Leverandøren skal stille relevant dokumentasjon og personell tilgjengelig slik at sikkerhetsrevisjon, -tilsyn og -inspeksjon kan gjennomføres på en god og effektiv måte.

Leverandøren skal varsles og informeres om Selskapets behov for å gjennomføre sikkerhetsrevisjon, -tilsyn og -inspeksjon. Selskapet vil kalle inn til oppstartsmøte for å presentere behov, omfang og plan for sikkerhetsrevisjon, -tilsyn og -inspeksjon.

Leverandørene forplikter seg til å følge opp og rette identifiserte funn fra sikkerhetsrevisjon, -tilsyn og -inspeksjon. Leverandøren skal rapportere status på tiltak for å rette identifiserte funn til Selskapet.

13. Lov- og regulatoriske krav

Selskapet er underlagt flere lov- og regulatoriske krav, endringer i disse vil kunne medføre endringer og justeringer i sikkerhetskrav. Leverandøren forplikter seg til å implementere og etterleve lov- og regulatoriske endringer.