Riktlinjer för säkerhet i telenät och teletjänster

Riktlinjer för utformningen av åtgärder för att säkerställa ett arbetssätt samt metoder och verktyg för att etablera en relevant säkerhet av telenät och tillhandahållna teletjänster.

Ver. 1.2

TLP:CLEAR

STADSNÄTS FÖRENINGEN

Innehåll

1 Inledning och bakgrund

1.1 Inledning

Dessa riktlinjer avser införandet av cybersäkerhetslagen i verksamheter som redan omfattas av lagen om elektronisk kommunikation. Kraven i dessa regelverk ska därför tillämpas samordnat.

Kommentar:
Enligt Lagen om elektronisk kommunikation (2003:389) (LEK) är man skyldig att anmäla en verksamhet till Post- och telestyrelsen (PTS) innan man börjar tillhandahålla:

- *ett allmänt elektroniskt kommunikationsnät, eller*
- *en allmänt tillgänglig elektronisk kommunikationstjänst.*

Anmälningsskyldigheten gäller när verksamheten riktar sig till allmänheten (dvs. inte enbart internt inom en organisation).

I förarbetena till cybersäkerhetslagen diskuteras samordning med lagen om elektronisk kommunikation. Den antagna cybersäkerhetslagen innebär dock inga materiella ändringar av lagen om elektronisk kommunikation. Krav enligt lagen om elektronisk kommunikation gäller därmed oförändrat och tillämpas parallellt med de kompletterande krav som följer av cybersäkerhetslagen.

Definitioner och dokumentförteckningar framgår av Bilaga Definitioner, dokumentförteckning och standarder.

1.2 Vad är cybersäkerhetslagen

Detta avsnitt ger en översiktlig beskrivning av cybersäkerhetslagen, vilka verksamheter som omfattas av lagen samt vilka skyldigheter och konsekvenser som följer av lagstiftningen. Beskrivningen syftar till att ge en bakgrund till de riktlinjer och arbetssätt som beskrivs i detta dokument.

Cybersäkerhetslagen (CSL) är en svensk lag som trädde i kraft den 15 januari 2026. Lagen syftar till att uppnå en hög gemensam nivå av cybersäkerhet i samhället genom att ställa krav på hur organisationer ska skydda sina nätverk, informationssystem och digitala tjänster mot cyberhot.

Lagen är Sveriges nationella genomförande av EU:s NIS2-direktiv (Network and Information Security Directive 2), som utgör ett gemensamt regelverk inom EU för cybersäkerhet. Genom lagen införs bindande krav på riskhantering, säkerhetsåtgärder, incidenthantering och incidentrapportering för verksamheter som är av betydelse för samhällsviktiga funktioner och ekonomin.

Lagens syfte

Syftet med cybersäkerhetslagen är att uppnå en hög nivå av cybersäkerhet i samhället. Det sker genom att:

- stärka motståndskraften i samhällsviktiga och digitala infrastrukturer,
- minska risken för allvarliga cyberincidenter, samt
- säkerställa att incidenter hanteras och rapporteras på ett strukturerat och samordnat sätt.

Lagen bygger på ett riskbaserat och proportionerligt angreppssätt, där kraven anpassas efter verksamhetens art, omfattning och betydelse för samhället.

Tillämpning – vilka verksamheter omfattas
Cybersäkerhetslagen gäller för både offentliga och privata verksamhetsutövare inom ett antal särskilt utpekade samhällssektorer. Dessa omfattar bland annat energi, transporter, hälso- och sjukvård, bank- och finansverksamhet, dricksvatten och avloppsvatten, offentlig förvaltning, rymdverksamhet samt digital infrastruktur.

Området digital infrastruktur omfattar:

- internetknutpunkter (IXP),
- DNS-tjänsteleverantörer,
- toppdomänregister (TLD),
- datacenter,
- leverantörer av innehållsleveransnät (CDN), samt
- allmänt tillgängliga elektroniska kommunikationsnät och elektroniska kommunikationstjänster.

Verksamhetsutövare som i Sverige tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster omfattas av cybersäkerhetslagen enligt 1 kap. 6 §.

Väsentliga och viktiga verksamhetsutövare (bantad)

Cybersäkerhetslagen skiljer mellan väsentliga och viktiga verksamhetsutövare. Indelningen avgör bland annat:

- kravnivån på säkerhetsåtgärder,
- tillsynens omfattning, samt
- nivån på eventuella sanktionsavgifter vid bristande efterlevnad.

Klassningen baseras på verksamhetens betydelse för samhället, de risker som en incident kan medföra samt verksamhetens storlek.

Kommentar MCF: När det gäller klassning enligt Cybersäkerhetslagen är utgångspunkten följande.
Stadsnät och andra tillhandahållare av allmänna elektroniska kommunikationsnät omfattas av regleringen oavsett geografisk räckvidd. De klassas som väsentliga verksamhetsutövare enligt lagen, och detta påverkas inte av att verksamheten är lokal eller av hur personalen är organiserad mellan bolag i koncernen.

När verksamhet är klassad som väsentligt företag gäller samma rättsliga skyldigheter oavsett vilken omsättning eller storlek företaget har.

Verksamhetsutövarens skyldighet och ansvar

Verksamhetsutövaren har det samlade och yttersta ansvaret för att kraven enligt cybersäkerhetslagen uppfylls i den egna verksamheten. Ansvaret omfattar styrning, organisation, resurssättning, genomförande, uppföljning och förbättring av säkerhetsarbetet.

Ansvaret kan inte överlåtas till leverantör, samarbetspartner eller annan extern part, även om delar av verksamheten är outsourcad eller upphandlad.

Säkerhetsarbetet ska bedrivas på ett sätt som är:

- Ledningsstyrt
- Riskbaserat
- Dokumenterat
- Proportionerligt
- Kvalitetssäkrat

Verksamhetsutövarens skyldigheter omfattar minst följande områden:

Lagen anger att en verksamhetsutövare har följande skyldighet:

- Anmälningsskyldighet
- Säkerhetsåtgärder, minst:
  1. strategier för riskanalys och för nätverks- och informationssystemens säkerhet,
  2. incidenthantering,
  3. kontinuitetshantering och krishantering,
  4. säkerhet i leveranskedjan,
  5. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem,
  6. strategier och förfaranden för att bedöma effektiviteten i säkerhetsåtgärderna,
  7. grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,
  8. strategier och förfaranden för användning av kryptografi samt, vid behov, kryptering,
  9. personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning, och
  10. vid behov användning av lösningar för autentisering, säkrade kommunikationer och säkrade nödkommunikationssystem.
- Utbildning i riskhantering
- Incidentrapportering och informationsskyldighet

Tillsyn och påföljder
Tillsyn enligt lagen utövas av Myndigheten för civilt försvar (MCF) samt av sektorsansvariga tillsynsmyndigheter. För elektroniska kommunikationsnät och -tjänster är Post- och telestyrelsen (PTS) tillsynsmyndighet.

En väsentlig verksamhetsutövare står under proaktiv tillsyn vilket innebär att tillsynsmyndigheten har rätt att begära in upplysningar och handlingar, genomföra inspektioner samt besluta om förelägganden. Förelägganden kan förenas med vite.

Vid allvarlig eller upprepad bristande efterlevnad får tillsynsmyndigheten besluta om sanktionsavgift. För en väsentlig verksamhetsutövare får sanktionsavgiften uppgå till högst:

- 10 miljoner euro, eller
- 2 procent av det beräkningsunderlag som enligt cybersäkerhetslagen ska läggas till grund för avgiften,

varvid det lägsta beloppen gäller.

För offentliga verksamhetsutövare fastställs beräkningsunderlaget enligt cybersäkerhetslagens bestämmelser och med beaktande av verksamhetens art och omfattning. Den slutliga avgiften bestäms av tillsynsmyndigheten efter en proportionalitetsbedömning i det enskilda fallet.

1.3 Dokumentets tillämpning och omfattning

Mot bakgrund av de skyldigheter som följer av cybersäkerhetslagen och lagen om elektronisk kommunikation anger detta dokument riktlinjer för säkerhetsarbetet avseende telenät och tillhandahållna teletjänster. Dokumentet omfattar de organisatoriska, tekniska och administrativa åtgärder som krävs för att säkerställa driftsäkerhet, informationssäkerhet och robusthet i telenät och teletjänster.

Riktlinjerna ska stödja verksamheten i att uppfylla krav enligt:

- cybersäkerhetslagen och cybersäkerhetsförordningen,
- lagen om elektronisk kommunikation med tillhörande föreskrifter,
- samt kompletterande krav som följer av styrelsens och ledningens styrning av säkerhetsarbetet.

Verksamheten är i detta sammanhang både verksamhetsutövare enligt cybersäkerhetslagen och tillhandahållare av allmänt tillgängliga elektroniska kommunikationsnät och/eller elektroniska kommunikationstjänster enligt lagen om elektronisk kommunikation.

I detta dokument används begreppet verksamhetsutövare som ett gemensamt begrepp för den organisation som ansvarar för drift, förvaltning och säkerhet i telenät och teletjänster. Begreppet används även i avsnitt som behandlar krav enligt lagen om elektronisk kommunikation, även om lagstiftningen där använder begreppet tillhandahållare.

Riktlinjernas omfattning och huvudsakliga tillämpningsområden illustreras i nedanstående figur.

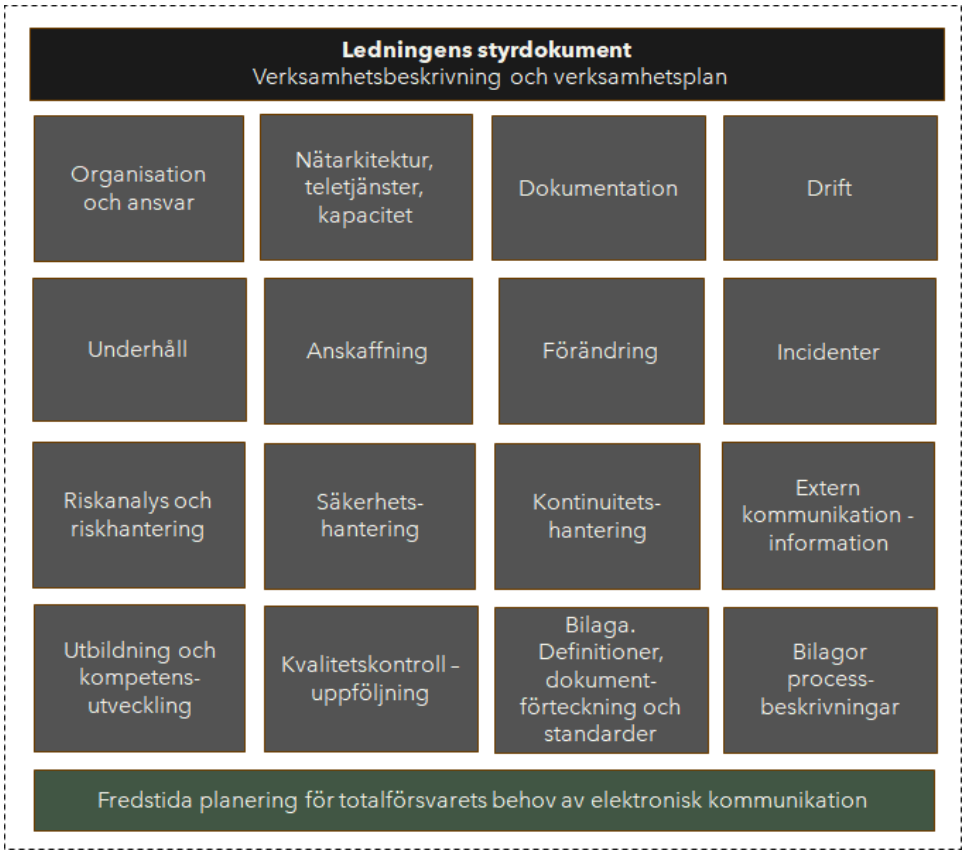

Bild Riktlinjernas omfattning

Genom att tillämpa de komponenter som framgår av bilden ges verksamhetsutövaren förutsättningar att etablera ett sammanhållet arbetssätt samt metoder och verktyg för att hantera säkerheten i telenät och tillhandahållna teletjänster.

Hur verksamhetsutövarens skyldigheter enligt cybersäkerhetslagen och lagen om elektronisk kommunikation omsätts i praktiken beskrivs i kapitel 2–19 i detta dokument.

- Kapitel 3 och 4 beskriver verksamhetens förutsättningar och planering.
- Kapitel 5 beskriver organisation, ansvar och styrning av säkerhetsarbetet.
- Kapitel 6–16 beskriver de operativa processer och åtgärder som krävs för att säkerställa driftsäkerhet och cybersäkerhet i telenät och teletjänster.
- Kapitel 17-18 beskriver uppföljning, kvalitetssäkring och relaterade styrdokument.

2 Syfte och Mål

Detta kapitel beskriver syftet med riktlinjerna samt de övergripande mål som ska styra verksamhetsutövarens säkerhetsarbete avseende telenät och tillhandahållna teletjänster.

Målen ska ge en gemensam inriktning för säkerhetsarbetet och utgöra grund för planering, genomförande, uppföljning och kontinuerlig förbättring av verksamhetens arbete med driftsäkerhet och cybersäkerhet.

2.1 Syftet med dokumentet

Syftet med detta dokument är att etablera ett sammanhållet och styrande ramverk för verksamhetsutövarens säkerhetsarbete avseende telenät och tillhandahållna teletjänster.

Riktlinjerna ska säkerställa att säkerhetsarbetet bedrivs på ett systematiskt, riskbaserat och proportionerligt sätt samt att verksamheten uppfyller tillämpliga krav enligt:

- lagen om elektronisk kommunikation med tillhörande föreskrifter
- cybersäkerhetslagen och cybersäkerhetsförordningen
- kompletterande krav som ställs av styrelse, ledning, ägare och kunder.

Anm:
Krav och åtgärder avseende Informationssäkerhet enligt Säkerhetsskyddslagen (2018:585) hanteras inte i detta dokument.

Krav och åtgärder enligt CER-direktivet 2022/2557 hanteras inte i detta dokument.

2.2 Målet för riktlinjerna

Målet med riktlinjerna är att säkerställa att verksamhetsutövaren har ett fungerande och långsiktigt säkerhetsarbete som:

- säkerställer tillgänglighet, riktighet, konfidentialitet och autenticitet i telenät och teletjänster
- upprätthåller förmåga att förebygga, upptäcka, hantera och rapportera incidenter
- stärker organisationens resiliens och förmåga att hantera störningar och kriser.

För att uppnå detta ska verksamhetsutövaren fastställa konkreta och uppföljningsbara mål för säkerhetsarbetet. Dessa mål ska vara anpassade till verksamhetens risker, omfattning och betydelse.

De specifika målen fastställs inom ramen för verksamhetsplaneringen (kapitel 4) och följs upp inom ramen för kvalitetsuppföljningen (kapitel 18).

2.3 Övergripande mål för säkerhetsarbetet

Det övergripande målet är att verksamhetsutövaren ska ha en ändamålsenlig, riskbaserad och dokumenterad säkerhetsförmåga som säkerställer att tillämpliga krav enligt cybersäkerhetslagen, lagen om elektronisk kommunikation, tillhörande föreskrifter och andra relevanta krav uppfylls.

Säkerhetsarbetet ska omfatta verksamhetens nätverks- och informationssystem, elektroniska kommunikationsnät, teletjänster, tillhörande tillgångar och fysisk miljö. Arbetet ska säkerställa funktion, tillgänglighet, driftsäkerhet, tillförlitlighet, riktighet, konfidentialitet och autenticitet samt förebygga, begränsa och hantera störningar, incidenter och avbrott.

För att uppnå detta ska verksamhetsutövaren fastställa mål, styra, genomföra, följa upp och utveckla säkerhetsarbetet inom följande områden utan ordningsföljd:

- tydlig och dokumenterad rollfördelning med särskilt utpekade ansvariga för arbetet,
- strategier för riskanalys och för nätverks- och informationssystemens säkerhet,
- incidenthantering,
- kontinuitetshantering och krishantering,
- säkerhet i leveranskedjan,
- säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem,
- strategier och förfaranden för att bedöma säkerhetsåtgärdernas effektivitet,
- grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,
- strategier och förfaranden för användning av kryptografi samt, vid behov, kryptering,
- personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning,
- vid behov användning av lösningar för autentisering, säkrade kommunikationer och säkrade nödkommunikationssystem,
- utbildning i riskhantering och hantering av behandlade uppgifter,
- incidentrapportering och informationsskyldighet.

Förslag till mål och aktiviteter för måluppfyllnad redovisas i kapitel 5–19.

3 Verksamhetsbeskrivning

En dokumenterad och aktuell verksamhetsbeskrivning utgör en grundläggande del av verksamhetsutövarens Ledningssystem (se *bilaga Definitioner*) för säkerhetsarbetet. Verksamhetsbeskrivningen ska ge underlag för riskanalyser, verksamhetsplanering, prioritering av säkerhetsåtgärder samt uppföljning av efterlevnad enligt cybersäkerhetslagen, lagen om elektronisk kommunikation och tillhörande föreskrifter.

Tillsammans med verksamhetsplanen (kapitel 4) utgör verksamhetsbeskrivningen den strategiska grund som säkerställer att krav i efterföljande kapitel avseende styrning, organisation, drift, incidenthantering, risk- och kontinuitetshantering kan uppfyllas på ett systematiskt, proportionerligt och dokumenterat sätt.

Verksamhetsbeskrivningen ska beskriva verksamhetens omfattning, kritiska funktioner, tillgångar, beroenden, organisation, nät och tjänster samt de förutsättningar som påverkar verksamhetens säkerhetsarbete och förmåga att upprätthålla driftsäkerhet och kontinuitet.

En uppdaterad verksamhetsbeskrivning är en förutsättning för att kunna visa att säkerhetsåtgärder är lämpliga och proportionerliga enligt tillämplig lagstiftning.

Verksamhetsutövarens kärnverksamhet

- Beskrivning av verksamhetsutövarens kärnverksamhet samt tillhandahållna telenät och teletjänster.
- Beskrivning av verksamhetens betydelse för användare, kunder och samhällsviktiga funktioner.
- Beskrivning av eventuella beredskapsfunktioner och samhällsviktiga beroenden.

Målgrupp och geografisk omfattning

- Beskrivning av de kundsegment och användargrupper verksamheten riktar sig mot.
- Beskrivning av verksamhetens geografiska omfattning och kritiska geografiska områden.

Teknologi och infrastruktur

- Övergripande beskrivning av nätarkitektur, telenät, teletjänster och tekniska huvudkomponenter.
- Beskrivning av principer för nät- och tjänsteutveckling.
- Beskrivning av principer för kapacitetsplanering, redundans och robusthet.
- Beskrivning av kritiska beroenden till elförsörjning, externa operatörer, leverantörer och verksamhetssystem.

Skyddsvärda funktioner och tillgångar

- Identifiering och beskrivning av skyddsvärda funktioner, nät, tjänster, informationstillgångar och informationsbehandlingstillgångar.
- Identifiering av kritiska beroenden och externa tjänster som är nödvändiga för verksamhetens funktion.
- Beskrivning av hur skyddsvärda funktioner och tillgångar klassificeras och används som underlag för riskanalys, kontinuitetsplanering och incidenthantering.

Organisation och ansvar

- Övergripande beskrivning av verksamhetens organisation, styrning och ansvarsfördelning.
- Beskrivning av verksamhetens funktionsområden, roller och rapporteringsvägar.
- Beskrivning av hur säkerhetsarbetet integreras i verksamhetens ordinarie styrning och uppföljning.

Regelverk och säkerhet

- Beskrivning av tillämpliga lagar, föreskrifter och externa krav som verksamheten omfattas av.
- Beskrivning av verksamhetens övergripande principer för säkerhet, informationshantering och skydd av nät, tjänster och uppgifter.
- Beskrivning av hur verksamheten arbetar med regelefterlevnad, riskhantering och uppföljning.

Kompetens och utbildning

- Beskrivning av verksamhetens övergripande arbete med utbildning, kompetensutveckling och medvetandegörande inom säkerhet, riskhantering och kontinuitetshantering.

Strategisk utveckling och framtidsplanering

- Beskrivning av verksamhetens strategiska mål och utvecklingsinriktning.
- Beskrivning av processer för omvärldsanalys och teknikutveckling.
- Beskrivning av planerade investeringar, förändringar och utvecklingsprojekt.

Finansiering och resurser

- Beskrivning av principer för finansiering, resursfördelning och långsiktig förvaltning av nät, tjänster och säkerhetsarbete.

4 Verksamhetsplan

Verksamhetsplanen konkretiserar verksamhetsbeskrivningen genom att omsätta beslut avseende riskhantering, lagkrav, beroenden och strategiska prioriteringar till planerade aktiviteter, resursfördelning och uppföljningsbara mål.

Verksamhetsplanen utgör verksamhetsutövarens övergripande plan för hur mål, riskhantering, säkerhetsåtgärder, resurser och uppföljning ska omsättas i praktisk verksamhet. Planen ska vara riskbaserad och utgå från verksamhetsbeskrivningen, genomförda riskanalyser, identifierade beroenden samt fastställda säkerhetsmål.

Verksamhetsplanen utgör därmed ett centralt styrinstrument för hur verksamhetsutövaren praktiskt säkerställer efterlevnad, driftsäkerhet, kontinuitet och cybersäkerhet enligt cybersäkerhetslagen, lagen om elektronisk kommunikation och tillhörande föreskrifter.

Planen ska säkerställa att krav i efterföljande kapitel avseende organisation, drift, underhåll, incidenthantering, riskhantering, kontinuitetshantering och uppföljning genomförs samordnat, prioriterat och uppföljningsbart inom ramen för verksamhetens ordinarie styrning och uppföljning.

Följande punkter rekommenderas ingå:

- **Mål:** Fastställda och uppföljningsbara mål för säkerhetsarbetet baserade på verksamhetens riskbild, skyddsbehov, lagkrav och strategiska prioriteringar.
- **Aktiviteter:** Riskbaserade åtgärder, projekt och förbättringsinsatser som ska genomföras för att uppnå fastställda mål och hantera identifierade risker och beroenden.
- **Resurser:** Planering och prioritering av resurser, kompetens, budget och tekniska förutsättningar som krävs för att genomföra säkerhetsarbetet.
- **Tidsplan:** Planering och prioritering av aktiviteter, förändringar och åtgärder inklusive ansvariga funktioner och tidpunkter för genomförande.
- **Utbildning och kompetens:** Planering av utbildning, övning och medvetandegörande för ledning, personal, konsulter och uppdragstagare.
- **Riskhantering och uppföljning:** Planering för uppföljning och utvärdering av mål, åtgärder, risknivåer, incidenter, kontinuitetsförmåga och genomförda säkerhetsåtgärder.
- **Ledningens fastställande och uppföljning:**
    - Verksamhetsplanen ska fastställas av verksamhetsutövarens ledning.
    - Uppföljning av genomförande, risker och måluppfyllelse ska ske regelbundet och minst årligen eller vid väsentliga förändringar.
    - Identifierade brister, avvikelser och risker ska rapporteras till ledningen och hanteras inom ramen för verksamhetens styr- och uppföljningsprocesser.

Tillsammans med verksamhetsbeskrivningen, organisationen, riskhanteringen, uppföljningen och övriga styrande dokument utgör verksamhetsplanen verksamhetsutövarens sammanhållna ledningssystem för säkerhetsarbetet enligt cybersäkerhetslagen, lagen om elektronisk kommunikation och tillhörande föreskrifter. Verksamhetsplanen kompletteras med processer, rutiner och anvisningar enligt kapitel 5 och framåt.

5 Organisation och ansvar

Detta kapitel beskriver hur verksamhetsutövaren ska organisera, styra och fördela ansvar för att säkerställa driftsäkerhet, kontinuitet och säkerhet i telenät och tillhandahållna teletjänster.

Organisation, ansvar och styrning ska vara anpassade till verksamhetens art, omfattning och riskbild samt säkerställa efterlevnad av gällande lagstiftning, i synnerhet lagen om elektronisk kommunikation och cybersäkerhetslagen.

Verksamhetsutövaren ska säkerställa att:

- ansvar, roller och rapporteringsvägar är tydligt definierade och dokumenterade,
- styrning och intern kontroll är ändamålsenliga,
- verksamheten har tillräcklig förmåga att uppfylla krav på driftsäkerhet, kontinuitet och säkerhet över tid,
- efterlevnad kan följas upp och visas vid tillsyn.

Organisationen ska möjliggöra att krav enligt lagstiftningen uppfylls såväl vid normal drift som vid störningar, incidenter och förändringar i verksamheten.

Tillämpliga lagar och föreskrifter

Organisation och ansvar enligt detta kapitel utgår bland annat från följande regelverk:

Cybersäkerhetslagen (CSL)
Ställer krav på att verksamhetsutövare etablerar en tydlig styrning, organisation och ansvarsfördelning för cybersäkerhetsarbetet samt att ledningen godkänner och följer upp riskhanteringsåtgärder.

Cybersäkerhetsförordningen (CSF)
Reglerar anmälningsskyldighet, tillsyn och rapportering till ansvarig myndighet.

Lagen om elektronisk kommunikation (LEK)
Ställer krav på att tillhandahållare av elektroniska kommunikationsnät och -tjänster säkerställer driftsäkerhet och kontinuitet.

PTS kompletterande föreskrifter avseende LEK
Bestämmelser om särskilda tekniska och organisatoriska åtgärder.

Lagen om extraordinära händelser i fredstid och höjd beredskap (LEH)
Ställer krav på krisberedskap och organisation för hantering av störningar i samhällsviktig verksamhet.

5.1 Styrelsens och Ledningens ansvar

5.1.1 Övergripande krav

Styrelse och verkställande ledning ska, inom ramen för verksamhetens interna styrning och kontroll, säkerställa att verksamhetsutövaren har organisation, resurser, ansvarsfördelning, processer och uppföljning för att uppfylla tillämpliga krav enligt cybersäkerhetslagen, lagen om elektronisk kommunikation, tillhörande föreskrifter och andra relevanta krav.

Styrelse och verkställande ledning ska säkerställa att säkerhetsarbetet är ledningsstyrt, riskbaserat, dokumenterat, proportionerligt och föremål för regelbunden uppföljning och förbättring. Detta omfattar ansvar för att fastställa mål, prioriteringar och ramar för säkerhetsarbetet samt att följa upp verksamhetens säkerhetsförmåga, risknivåer, incidenter, kontinuitetsförmåga och efterlevnad.

Styrelse och verkställande ledning ska även säkerställa att verksamhetsutövaren har förmåga att fastställa mål, styra, genomföra, följa upp och utveckla säkerhetsarbetet för de mål som redovisas i kapitel 2.3 Övergripande mål för säkerhetsarbetet.

Verksamhetsbeskrivningen enligt kapitel 3 utgör tillsammans med verksamhetsplanen, organisationen, riskhanteringen, uppföljningen och övriga styrande dokument verksamhetsutövarens sammanhållna ledningssystem för säkerhetsarbetet enligt cybersäkerhetslagen, lagen om elektronisk kommunikation och tillhörande föreskrifter.

Ledningen ska säkerställa att ett ledningssystem tillämpas och integreras i verksamhetens ordinarie styrning, planering, drift och uppföljning. Säkerhetsarbetet ska baseras på riskanalyser, identifierade beroenden, verksamhetens skyddsbehov samt tillämpliga lagar, föreskrifter och interna krav.

Styrelse och verkställande ledning ska säkerställa att verksamhetsutövaren:

- fastställer mål, krav och ansvar för respektive område,
- omsätter krav och mål i styrande dokument, processer och tekniska skyddsåtgärder,
- säkerställer att ansvariga funktioner har tillräckliga resurser, befogenheter och kompetens,
- genomför regelbundna riskanalyser, uppföljningar och kontroller,
- identifierar och hanterar brister, avvikelser och förbättringsbehov,
- följer upp incidenter, störningar och genomförda åtgärder,
- säkerställer utbildning, övning och medvetandegörande,
- samt regelbundet följer upp och förbättrar säkerhetsförmågan.

Säkerhetsarbetet ska vara dokumenterat och kunna verifieras genom uppföljning, revision och ledningens genomgång.

Gemensamma principer

Det yttersta ansvaret för efterlevnad av lagen om elektronisk kommunikation och cybersäkerhetslagen kan inte delegeras bort, även om arbetsuppgifter utförs av anställda, konsulter eller externa leverantörer.

Utbildning av styrelse och ledning

Styrelseledamöter och ledande befattningshavare ska regelbundet genomgå utbildning inom riskhantering och cybersäkerhet som är anpassad till verksamhetens art och riskbild.

Utbildningsinsatser ska dokumenteras.

5.1.2 Organisering av stadsnätsverksamheten

Stadsnätsverksamheten kan organiseras på olika sätt inom kommunal verksamhet, beroende på kommunens storlek, styrmodell och strategiska val. Vanliga organisationsformer är:

- Direkt under kommunstyrelsen. I mindre kommuner kan stadsnätsverksamheten bedrivas som förvaltningsverksamhet direkt under kommunstyrelsens ansvarsområde, särskilt om stadsnätet utgör en begränsad del av den totala verksamheten.
- Under teknisk nämnd eller motsvarande nämnd. Nämnden ansvarar då för styrning och uppföljning av stadsnätsverksamheten inom ramen för fullmäktiges beslut, medan den operativa verksamheten bedrivs av förvaltningen.
- I ett kommunalt bolag. Stadsnätsverksamheten bedrivs då i ett kommunalt aktiebolag, ofta som ett dotterbolag i en kommunal koncern. Detta är en ofta förekommande organisationsform för stadsnätsverksamhet.
- I ett gemensamt bolag eller kommunalförbund. Verksamheten bedrivs då gemensamt av flera kommuner, exempelvis genom ett samägt bolag eller ett kommunalförbund

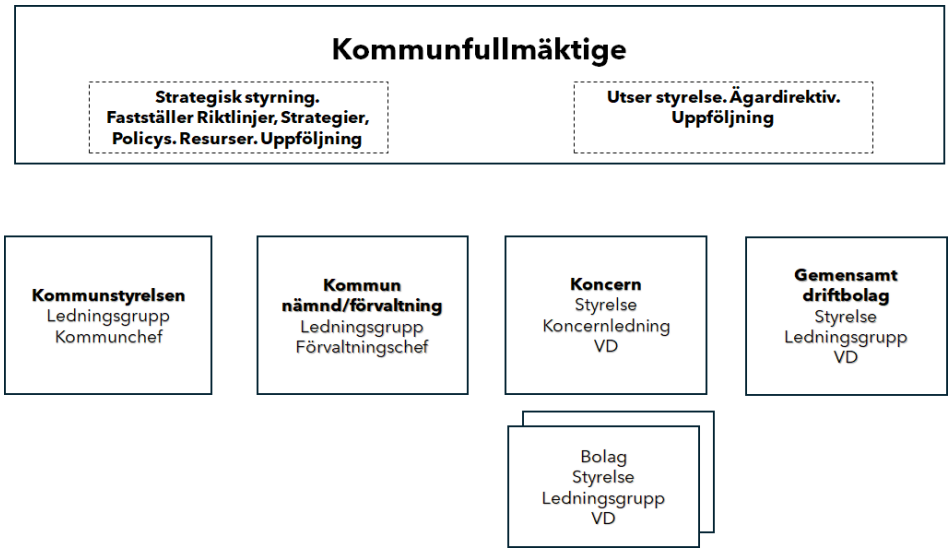

Bild. Organisationsalternativ kommunal verksamhet

Verksamhetsutövare och ansvar för arbetet med Cybersäkerhet

Hanteringen av ledningens och styrelsens ansvar för Telenät och Teletjänster (stadsnätsverksamheten) är beroende av organisationsform i enlighet med nedan.

5.1.3 Stadsnätsverksamheten bedrivs inom kommunal förvaltning

Formell verksamhetsutövare: Kommunen som juridisk person

- Kommunfullmäktige ansvarar för den strategiska styrningen genom att fastställa mål, riktlinjer, strategier och policys samt besluta om resurser och följa upp verksamheten.
- Kommunstyrelsen är kommunens verkställande organ och ansvarar för att leda och samordna kommunens verksamhet samt utöva uppsikt över nämnder och kommunala verksamheter. Kommunstyrelsen ansvarar för att kommunen har en ändamålsenlig organisation för att hantera cybersäkerhetsarbete, intern kontroll och efterlevnad av cybersäkerhetslagen.
- Ansvarig nämnd, i de fall stadsnätsverksamheten är organiserad under en nämnd, har det verksamhetsansvar som följer av nämndens uppdrag och ansvarar för att stadsnätsverksamheten uppfyller krav på cybersäkerhet, intern kontroll och Cybersäkerhetslagens efterlevnad.
- Ledningen (kommunchef/förvaltningschef eller motsvarande samt ansvarig för stadsnätsverksamheten) ansvarar för det operativa genomförandet av cybersäkerhetsarbetet i enlighet med politiska beslut och fastställda styrdokument.

5.1.4 Stadsnätsverksamheten bedrivs i ett kommunalt bolag inom en koncern

Formell verksamhetsutövare: Det kommunala stadsnätsbolaget (juridisk person)

- Kommunfullmäktige ansvarar för ägardirektiv till koncernstyrelsen samt för uppföljning av dessa.
- Koncernstyrelsen har det övergripande ansvaret för koncernens säkerhetsarbete, internkontroll och efterlevnad av cybersäkerhetslagen och rapporterar till kommunen som ägare.
- Styrelsen för stadsnätsbolaget har det yttersta ansvaret för bolagets organisation, säkerhetsarbete, internkontroll och Cybersäkerhetslagens efterlevnad.
- Bolagets VD ansvarar för det operativa genomförandet av cybersäkerhetsarbetet och rapporterar till bolagsstyrelsen.

5.1.5 Stadsnätsverksamheten bedrivs i ett gemensamt bolag eller kommunalförbund

Formell verksamhetsutövare: Det gemensamma bolaget eller kommunalförbundet (juridisk person)

- Ägarna (exempelvis kommuner, regional nätverksorganisation eller kommunalförbund) ansvarar för ägardirektiv eller förbundsordning samt för uppföljning av verksamheten.
- Styrelsen för det gemensamma bolaget eller kommunalförbundet har det yttersta ansvaret för säkerhetsarbete, internkontroll och efterlevnad av cybersäkerhetslagen.
- Verkställande ledning ansvarar för det operativa genomförandet av cybersäkerhetsarbetet och rapporterar till styrelsen.

5.1.6 Privat verksamhet

Formell verksamhetsutövare: Den juridiska person som driver verksamheten

I privat verksamhet enligt cybersäkerhetslagen/NIS2 gäller att:

- Styrelsen har det yttersta ansvaret för cybersäkerhet och intern kontroll,
- VD har det operativa ansvaret,
- ansvaret kan inte delegeras bort, endast arbetsuppgifter,
- bolagsform saknar betydelse – det är den juridiska person som driver verksamheten som är verksamhetsutövare

5.2 Funktionsområden

För att säkerställa ett strukturerat, sammanhållet och riskbaserat säkerhetsarbete kan verksamhetsutövaren strukturera arbetet i funktionsområden.

Funktionsområdena beskriver ansvar och styrning för säkerhetsarbetet samt hur krav enligt lagen om elektronisk kommunikation och cybersäkerhetslagen ska hanteras inom verksamheten. De avser funktionella ansvarsnivåer och utgör inte beskrivningar av operativt utförande.

Funktionsområdena innebär inte krav på separata organisatoriska enheter. I mindre organisationer kan samma person, funktion eller extern leverantör ansvara för flera funktionsområden.

Det avgörande är att ansvar, mandat, rapporteringsvägar och uppföljning är tydligt definierade och dokumenterade.

Bild. Funktionsområden

I verksamhetsbeskrivningen ska Stadsnätet beskriva hur arbetet är organiserat och med tydliga rollfördelningar.

Verksamhetsskydd för Telenät och Teletjänster

Verksamhetsskydd är den ledningsstyrda och riskbaserade styrningen av verksamhetens samlade säkerhetsarbete i syfte att säkerställa kontinuitet, robusthet och skydd mot störningar, intrång och andra hot.

Verksamhetsskydd omfattar den övergripande styrningen, kravställningen och uppföljningen av verksamhetens säkerhetsåtgärder för att skydda verksamheten som helhet mot störningar, intrång, sabotage och andra hot som kan påverka driften av telenät och leveransen av teletjänster.

Verksamhetsskydd ska säkerställa att säkerhetsarbetet bedrivs ledningsstyrt, riskbaserat och proportionerligt samt är anpassat till verksamhetens art, omfattning och betydelse.

Verksamhetsskydd omfattar inte teknisk implementation eller operativ drift av säkerhetsåtgärder, men ska ange krav, principer och uppföljning för dessa.

Verksamhetsskydd omfattar minst följande områden:

- **Fysisk säkerhet:** Fastställande av krav på skydd av kritisk infrastruktur, byggnader och anläggningar, inklusive krav på tillträdeskontroll, larm, övervakning och skydd mot intrång och sabotage.
- **Informationssäkerhet:** Säkerställande av att information är klassificerad och att krav på konfidentialitet, riktighet och tillgänglighet är fastställda och tillämpbara oavsett informationsform, lagringsplats eller behandlingssätt.
- **Personalsäkerhet:** Fastställande av krav och rutiner för att säkerställa att rätt personer anställs och ges åtkomst till verksamheten, inklusive hantering av insiderhot, säkerhetsmedvetenhet, utbildning samt skydd av personal.
- **IT- säkerhet och nätsäkerhet:** Fastställande av övergripande krav, principer och skyddsnivåer för IT- och nätsäkerhet. Kraven ska vara riskbaserade och verksamhetsanpassade samt omsättas i tekniska och operativa krav för verksamhetssystem och nät.
- **Kontinuitetsplanering och krishantering:** Fastställande av krav och planer för att säkerställa verksamhetens förmåga att förebygga, hantera och återhämta sig från störningar, incidenter och kriser.

- **Regelefterlevnad och juridiskt skydd:** Säkerställande av att tillämpliga lagar, föreskrifter och externa krav identifieras, efterlevs och kan visas vid uppföljning och tillsyn.

Som stöd för det systematiska säkerhetsarbetet kan verksamhetsutövaren använda etablerade standarder, metodstöd och vägledningar. Exempel på sådant stöd är MCF:s metodstöd för systematiskt säkerhetsarbete samt tillhörande vägledningar, såsom *Vägledning – säkerhetsåtgärder i informationssystem*.

Dessa stöd är ofta funktionsspecifika men bygger på vedertagna principer för systematiskt, riskbaserat och ledningsstyrt säkerhetsarbete.

Informationssäkerhetsfrågor som innefattas av säkerhetsskyddslagen hanteras inte i detta dokument.

Teknisk säkerhet

Omfattar det strategiska förvaltningsansvaret för utveckling och teknisk säkerhet för Telenät och Teletjänster, verksamhetssystem, relevanta IT -system och information.

Teknisk säkerhet ska:

- omsätta krav från Verksamhetsskydd till tekniska arkitekturer, standarder och säkerhetsprinciper,
- samordna teknikval och säkerhetslösningar mellan nät, tjänster och verksamhetssystem,
- fastställa och följa upp tekniska riktlinjer, processer och anvisningar för säker teknisk förvaltning,
- utvärdera att tekniska säkerhetsåtgärder är ändamålsenliga och långsiktigt hållbara.

Teknisk säkerhet ansvarar inte för operativ drift.

Driftfunktioner

Verksamhetsutövarens tekniska drift är uppdelad i två huvudsakliga funktionsområden, Drift Nät och tjänster och Drift Verksamhetssystem.

Funktionsområdena beskriver ansvarsfördelningen för drift, teknisk förvaltning, övervakning, incidenthantering, underhåll och förändringshantering. De operativa processerna för drift, övervakning, incidenthantering, underhåll och förändringshantering beskrivs i kapitel 8-11.

Indelningen i funktionsområden innebär inte krav på att ansvaret ska organiseras i särskilda organisatoriska enheter. Uppgifter inom funktionsområdena kan utföras av interna funktioner, systemleverantörer eller externa driftleverantörer, under förutsättning att ansvar, krav, gränssnitt, eskalering, informationssäkerhet och uppföljning är tydligt reglerade.

Drift Nät och tjänster

Funktionsområdet *Drift Nät och tjänster* ansvarar för operativ drift och teknisk förvaltning av verksamhetsutövarens telenät och de teletjänster som tillhandahålls genom nätet.

Funktionen ska säkerställa att nätinfrastruktur, förbindelser och tjänsteplattformar drivs, övervakas och underhålls på ett driftsäkert och tillförlitligt sätt i enlighet med krav enligt lagen om elektronisk kommunikation och cybersäkerhetslagen.

Drift Nät och tjänster omfattar drift av nätkomponenter såsom routrar, switchar, accessutrustning och transmissionssystem samt drift av tjänsteplattformar som används för att leverera elektroniska kommunikationstjänster.

Funktionsområdet ansvarar för operativ drift, övervakning, incidenthantering, underhåll och teknisk förvaltning av telenät och teletjänster samt för samordning av driftrelaterade aktiviteter och uppföljning av tjänsternas funktion och tillgänglighet.

Funktionsområdet omfattar bland annat följande aktiviteter:

- övervakning av nät och tjänster samt hantering av larm
- felsökning och åtgärd av driftstörningar
- incidenthantering och samordning vid driftstörningar
- planerat underhåll och uppgraderingar av nätinfrastruktur
- teknisk förvaltning av nätkomponenter och tjänsteplattformar
- hantering av förändringar i nät och tjänster
- uppföljning av drift, kapacitet och tjänstekvalitet
- rapportering och uppföljning av driftrelaterade händelser
- samverkan med leverantörer och andra aktörer vid drift och felavhjälpning

Drift Verksamhetssystem

Funktionsområdet *Drift Verksamhetssystem* ansvarar för operativ drift och teknisk förvaltning av verksamhetsutövarens verksamhetssystem.

Med verksamhetssystem avses IT-baserade system, applikationer, databaser, register, integrationer och stödsystem som används för att stödja, styra, administrera, övervaka, dokumentera eller följa upp verksamhetsutövarens nät- och tjänstedrift.

Verksamhetssystemen kan exempelvis omfatta system för nätövervakning, larmhantering, ärendehantering, kund- och abonnemangsadministration, dokumentation, inventarie- och konfigurationshantering, kapacitetsuppföljning, analys, identitets- och behörighetshantering samt system för loggning, säkerhetskopiering och rapportering.

Funktionen ska säkerställa att systemen drivs och underhålls på ett stabilt och säkert sätt samt att systemen har den tillgänglighet och funktion som krävs för att stödja driften av telenät och teletjänster.

Funktionsområdet ansvarar för verksamhetssystemens funktion, säkerhet, tekniska förvaltning och återställningsförmåga. Den operativa driften kan utföras av en intern IT-funktion, systemleverantörer eller externa driftleverantörer, men verksamhetsutövaren ansvarar för kravställning, styrning, uppföljning och tydliga gränssnitt.

Funktionsområdet omfattar bland annat följande aktiviteter:

- drift och övervakning av verksamhetssystem, applikationer, databaser, integrationer och systemplattformar
- hantering av systemlarm och driftstörningar
- incidenthantering och felsökning i systemmiljöer
- planerat underhåll och uppgraderingar av system och databaser
- teknisk förvaltning av applikationer och systemplattformar
- hantering av förändringar i system och konfigurationer
- behörighetsstyrning, loggning, säkerhetskopiering och skydd av information i verksamhetssystem
- uppföljning av systemens funktion, kapacitet och tillgänglighet
- rapportering och uppföljning av driftrelaterade händelser
- samverkan med systemleverantörer och externa driftleverantörer

5.3 Roller och ansvarsområden

Detta avsnitt beskriver hanteringen av roller och ansvarsområden för drift och förvaltning av Telenät, Teletjänster och Verksamhetssystem samt cybersäkerhetsarbetet hos Verksamhetsutövaren.

Mål: Att tydliggöra roller och ansvarsområden för drift och förvaltning av Telenät, Teletjänster, Verksamhetssystem samt cybersäkerhetsarbetet i Verksamhetsutövarens organisation.

Åtgärder:

- Identifiera och dokumentera roller och ansvar avseende drift och förvaltning av Telenät, Teletjänster, Verksamhetssystem samt cybersäkerhetsarbetet hos Verksamhetsutövaren i verktyget *HUKI* (Huvudansvarig/Beslutsfattare, Utförare/Uppdrags- och underlagsansvarig, Konsulteras, Informeras)*

  ***Anm.** HUKI är ett exempel på projektverktyg för att beskriva vilka roller som är ansvariga, ansvarstagande, rådgivande och informerade för varje specifik uppgift eller process inom driftsäkerhetsarbetet.

5.3.1 Roller för hantering av funktionsområden

Roller beskriver **vem som utför uppgifter**, inte vem som bär det yttersta ansvaret. Det yttersta ansvaret för efterlevnad av lagen om elektronisk kommunikation och cybersäkerhetslagen ligger alltid hos verksamhetsutövaren genom styrelse och ledning och kan inte delegeras bort.

Roller kan kombineras eller innehas av samma person eller extern leverantör, förutsatt att ansvar, mandat och rapporteringsvägar är tydligt dokumenterade.

Exempel på roller:

- **Verksamhetsskydd**
  - Säkerhetschef**.** Samordnar och koordinerar arbetet med verksamhetsskydd enligt kapitel 4.2,

- **Teknisk säkerhet**
  - Teknisk chef med övergripande strategiskt förvaltningsansvar för utveckling och teknisk säkerhet för Telenät och Teletjänster samt relevanta verksamhetssystem.

- **Drift nät och tjänster**
  - Driftchef Nät med ansvar för teknisk förvaltning och operativ drift av Telenät och Teletjänster.

- **Drift Verksamhetssystem**
  - IT-chef med ansvar för teknisk förvaltning och operativ drift av verksamhetsutövarens IT-baserade verksamhetssystem, driftsystem, databaser, integrationer, informationsbehandlingstillgångar och interna stödsystem.

6 Nätarkitektur, Teletjänster och kapacitet

Syfte:

Syftet med detta kapitel är att säkerställa att nätarkitektur, kritiska funktioner, redundans och kapacitet planeras och dimensioneras utifrån verksamhetsutövarens riskanalys och identifierade beroenden.

6.1 Telenät- och Teletjänster

6.1.1 Nulägesbeskrivning

Mål: Att nuläget för Telenätet och Teletjänster är beskrivet och dokumenterat.

Åtgärder:

- Ta fram en nulägesbeskrivning över nätarkitektur, anläggnings- och informationsbehandlingstillgångar, förbindelser och tillhandhållna tjänster. dokumenteras i Verksamhetsbeskrivningen eller i tillhörande teknisk dokumentation.
- Dokumentera tillgångar i enlighet med kap 8 Dokumentation
- Klassificera nätets komponenter, förbindelser och tjänster utifrån deras kritiska påverkan för verksamheten, samhällsfunktioner och användare.
- Klassningen ska användas som underlag för riskanalys, redundans, reservkraft och kapacitetsplanering.

6.1.2 Redundanta förbindelser

Mål: Att de åtgärder som krävs för hantering av redundans för förbindelser är beskrivet och dokumenterat.

Åtgärder:

- Identifiera och dokumentera behovet av redundans baserat på verksamhetsutövarens riskanalys. Tidigare gällande föreskrifter kan användas som vägledning i den mån de är förenliga med kraven på lämpliga och proportionerliga säkerhetsåtgärder enligt cybersäkerhetslagen.
- Utveckla och upprätthålla en *Åtgärdsplan för hantering av redundans avseende förbindelser för kritiska tillgångar.*

6.1.3 Reservkraft

Mål: Att de åtgärder som krävs för hantering av redundans för reservkraft är beskrivet och dokumenterat.

Åtgärder:

- Identifiera och dokumentera behovet av redundans baserat på verksamhetsutövarens riskanalys. Tidigare gällande föreskrifter kan användas som vägledning i den mån de är förenliga med kraven på lämpliga och proportionerliga säkerhetsåtgärder enligt cybersäkerhetslagen.

- Utveckla och upprätthålla en *Åtgärdsplan för hantering av reservkraft för kritiska tillgångar*.

6.2 Nät- och tjänsteutveckling

Mål: Säkerställa att utveckling och förändring av Telenät och Teletjänster sker strukturerat, dokumenterat och riskbaserat samt att tekniska val, arkitekturförändringar och nya tjänster dimensioneras i enlighet med genomförd riskanalys och identifierade kritiska funktioner och beroenden.

Åtgärder:

- Genomföra omvärldsanalys avseende tjänsteutveckling och samhällstrender.
- Genomföra omvärldsanalys avseende teknikutveckling gällande infrastruktur och tjänsteplattformar.
- Genomföra omvärldsanalys avseende teknikutveckling för informationsbehandlingstillgångar.
- Ta fram ett förslag till tekniska och funktionella förändringar inklusive påverkan på:
    - kritiska funktioner
    - redundans och reservkraft
    - kapacitet och tillgänglighet
    - beroenden till externa leverantörer, operatörer och elförsörjning
- Genomför en dokumenterad riskanalys innan beslut om genomförande fattas.
- Ta fram en implementeringsplan som inkluderar tidsplan, resurser, testning, återställningsplan och uppföljning
- Säkerställ att förändringar hanteras inom ramen för fastställd förändringsprocess.
- Dokumentera alla beslut avseende förändringar i Verksamhetsbeskrivningen eller i tillhörande teknisk dokumentation.

6.3 Kapacitetsplanering

Mål: Att behovet av framtida kapacitetsförändringar är analyserat och planerat för att undvika överbelastning och säkerställa optimal prestanda.

Åtgärder:

- Analysera nuvarande användning och trafikmönster.
- Utvärdera och planera kapacitetsbehoven för planerad tjänsteutveckling
- Säkerställa att tjänsterna kan levereras utan avbrott även under hög belastning.
- Dokumentera kapacitetsplanerna i Verksamhetsbeskrivningen eller i tillhörande teknisk dokumentation.”.
- Beakta identifierade risker och beroenden vid kapacitetsplanering, inklusive beroenden till elförsörjning, externa operatörer, leverantörer och verksamhetssystem.

Genom att följa dessa riktlinjer kan Verksamhetsutövaren säkerställa en planerad utveckling av Telenätet och Teletjänster som är säkra och hanterar nuvarande och framtida krav.

7 Dokumentation

Syfte: Säkerställa att samtliga anläggningstillgångar, informationsbehandlingstillgångar, förbindelser och uppdragshållare är dokumenterade och hålls uppdaterade för att effektivisera förändringsarbete, incidenthantering samt drift och underhåll.

Mål: Att samtliga anläggningstillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare är identifierade, dokumenterade och klassificerade utifrån risk, betydelse och påverkan för verksamheten, samhällsfunktioner och användare. Dokumentationen ska hållas uppdaterad och stödja förändringsarbete, incidenthantering, drift och underhåll.

Åtgärder:

- Dokumentera alla nätanläggningstillgångar.
  Tillhandahållaren ska för respektive anläggningstillgång åtminstone dokumentera:
  - en unik beteckning,
  - dess funktion,
  - geografisk placering, om sådan finns,
  - en hänvisning till aktuell riskanalys,
  - tillverkare.

- Dokumentera alla förbindelser. Redundans ska framgå.
  Tillhandahållaren ska för respektive förbindelse åtminstone dokumentera:
  - en unik beteckning,
  - dess funktion,
  - geografisk placering, om sådan finns,
  - en hänvisning till aktuell riskanalys,
  - tillverkare.

- Dokumentera informationsbehandlingstillgångar.
  Tillhandahållaren ska för respektive informationsbehandlingstillgång åtminstone dokumentera:
  - en unik beteckning,
  - dess funktion,
  - geografisk placering, om sådan finns,
  - en hänvisning till aktuell riskanalys,
  - tillverkare.

- Dokumentera uppdragstagare
  Tillhandahållaren ska för respektive uppdragstagare åtminstone dokumentera
  - uppdragstagarens namn,
  - organisationsnummer,
  - kontaktuppgifter,
  - en beskrivning av uppdraget.

Dokumentationen ska hållas uppdaterad och bevaras under sådan tid att efterlevnad, uppföljning, incidentutredning och tillsyn kan säkerställas, eller längre om detta följer av annan tillämplig lagstiftning.

8 Drift

Kapitlet konkretiserar hur fastställda krav på driftsäkerhet, tillgänglighet, kontinuitet och incidenthantering omsätts i praktiken genom övervakning, larmhantering, felsökning, avhjälpning, förebyggande åtgärder och uppföljning.

Begreppet Drift används i detta kapitel för att beskriva funktions- och ansvarsområden för operativ drift och teknisk förvaltning. Det innebär inte krav på en särskild organisatorisk enhet, utan beskriver hur arbetsuppgifter och ansvar kan organiseras.

Den operativa driften genomförs av två samverkande driftfunktioner i enlighet med ansvarsfördelningen i kapitel 5:

- Drift Nät och tjänster, som ansvarar för drift av telenätets infrastruktur och tjänsteplattformar
- Drift Verksamhetssystem, som ansvarar för drift av de IT baserade verksamhetssystemen och de informationsbehandlingstillgångar som används för att övervaka, konfigurera och administrera telenät och teletjänster.

Driftfunktionerna samverkar för att säkerställa stabil drift, effektiv incidenthantering och en samlad lägesbild av nätets och tjänsternas funktion.

Verksamhetens hantering av processer och rutiner baseras på etablerade driftprocesser, exempelvis enligt ITIL eller motsvarande metodstöd.

Syfte: Säkerställa att driften av nät, tjänster och verksamhetssystem fungerar stabilt, effektivt och utan avbrott genom att Verksamhetsutövarens driftorganisation kontinuerligt övervakar nät, tjänster och verksamhetssystem för att snabbt kunna identifiera och åtgärda tekniska fel eller avbrott.
Driftövervakning och incidenthantering ska även beakta beroenden till externa leverantörer, elförsörjning och gemensam infrastruktur.

8.1 Drift Nät- och tjänster

Detta avsnitt beskriver hur funktionsområdet Drift Nät och tjänster genomför den operativa driften av Telenät och Teletjänster.

Avsnittet fokuserar på det operativa genomförandet av drift, övervakning, incidenthantering och åtgärder i syfte att upprätthålla driftsäkerhet, tillgänglighet och kontinuitet i enlighet med gällande lagstiftning och fastställda krav.

Mål: Säkerställa att driften av Telenät och Teletjänster fungerar stabilt, effektivt och utan avbrott genom att Verksamhetsutövarens driftorganisation kontinuerligt övervakar Telenätet och Teletjänsterna för att snabbt kunna identifiera och åtgärda tekniska fel eller avbrott samt identifiera behov av förebyggande åtgärder.

Åtgärder:

- Upprätta en Servicedesk för hantering av felanmälan och supportärenden. Servicedesk kan vara internt organiserad eller tillhandahållas av extern leverantör, förutsatt att ansvar, tillgänglighet och eskaleringsrutiner är tydligt reglerade.
- Upprätta en funktion för 2:a-3:e Linjens support bemannad med drifttekniker och utbildade incidenthanteringsspecialister, som är tillgängliga dygnet runt.
- Implementera övervakningsverktyg och system som kan upptäcka avvikelser och potentiella hot i realtid.
- Implementera ett centralt driftstödsystem som integrerar larm och notifieringar från olika övervakningsverktyg.
- Konfigurera system för att övervaka nyckelparametrar som trafik i nätet, serverhälsa, applikationsprestanda och säkerhetsloggar.
- Implementera övervakningssystem för att kontinuerligt mäta och förbättra Teletjänsternas prestanda.
- Ställ in larmtrösklar baserat på definierade säkerhetspolicyer och bästa praxis för att minimera falsklarm och säkerställa snabb respons.
- Hot, störningar och driftavvikelser ska dokumenteras.
- Säkerställa att driftövervakning och larmhantering är riskbaserad och anpassad efter identifierade kritiska funktioner i telenätet och teletjänsterna.
- Säkerställa att driftavvikelser, larm och åtgärder dokumenteras och följs upp enligt fastställda rutiner.
- Säkerställa att driftavvikelser som kan utgöra säkerhetsincidenter eskaleras och hanteras enligt organisationens incidenthanteringsprocess.

8.2 Drift Verksamhetssystem

Detta avsnitt beskriver hur funktionsområdet Drift Verksamhetssystem genomför den operativa driften av de verksamhetssystem och tillhörande informationsbehandlingstillgångar som stödjer drift och förvaltning av telenät och teletjänster.

Verksamhetssystemen omfattar exempelvis övervakningssystem, larm- och driftstödsystem, konfigurationssystem, ärendehanteringssystem, dokumentationssystem, kund- och abonnemangssystem, databaser, integrationer och andra IT-baserade stödsystem som används för att administrera, övervaka, analysera eller följa upp nät och tjänster.

Mål: Säkerställa att driften av Verksamhetssystemen fungerar stabilt, effektivt och utan avbrott genom att Verksamhetsutövarens driftorganisation kontinuerligt övervakar Verksamhetssystemen för att snabbt kunna identifiera och åtgärda tekniska fel eller avbrott samt identifiera behov av förebyggande åtgärder.

Åtgärder:

- Upprätta en Servicedesk för hantering av felanmälan och supportärenden
- Upprätta en funktion för 2:a–3:e Linjens support bemannad med drifttekniker och utbildade incidenthanteringsspecialister, som är tillgängliga dygnet runt.
- Implementera övervakningsverktyg och system som kan upptäcka avvikelser och potentiella hot i realtid.
- Implementera ett centralt driftstödsystem som integrerar larm och notifieringar från olika övervakningsverktyg.
- Konfigurera system för att övervaka nyckelparametrar som serverhälsa, applikationsprestanda och säkerhetsloggar.
- Säkerställ att loggar och driftrelaterad dokumentation bevaras under sådan tid att incidentutredning, uppföljning och efterlevnad kan säkerställas.
- Ställ in larmtrösklar baserat på definierade säkerhetspolicyer och bästa praxis för att minimera falsklarm och säkerställa snabb respons.
- Dokumentera hot, störningar och driftavvikelser.
- Säkerställa att skydd av information i verksamhetssystem beaktar krav på konfidentialitet, riktighet och tillgänglighet.
- Säkerställa att behörigheter, åtkomst, ändringar, patchning, säkerhetskopiering och återställning hanteras enligt fastställda rutiner.
- Säkerställa att driftavvikelser och säkerhetsrelaterade händelser i verksamhetssystem dokumenteras och följs upp enligt fastställda rutiner.
- Säkerställa att driftavvikelser i verksamhetssystem som kan utgöra säkerhetsincidenter eskaleras och hanteras enligt organisationens incidenthanteringsprocess.
- Säkerställa tydlig samverkan och eskalering mellan Drift Verksamhetssystem, Drift Nät och tjänster, systemleverantörer och externa driftleverantörer.

9 Underhåll

Syfte: Säkerställa att alla system och utrustningar i Telenätet fungerar optimalt genom att utföra regelbundet underhåll och att säkerställa tillgången på reservdelar.

Underhållsåtgärder ska prioriteras och dimensioneras utifrån verksamhetsutövarens riskanalys och identifierade kritiska funktioner.

9. 1 Förebyggande underhåll

9.1.1 Underhållsplaner

Mål: Att underhållet av alla relevanta komponenter i Telenätet är planlagt för att förebygga fel och förlänga utrustningarnas livslängd.

Åtgärder:

- Ta fram *Underhållsplan(*er)
- Dokumentera underhållsaktiviteter som specificerar vilka underhållsåtgärder som ska utföras, frekvensen av dessa åtgärder och vem som är ansvarig.
- Säkerställa att Underhållsplanen (er) uppdateras regelbundet baserat på utrustningarnas, tillverkarens rekommendationer och tidigare underhållshistorik.
- Av planen ska också framgå hur analys av underhållsdata och framtida behov ska utföras för att förutse behovet av korrigeringar av verkställande underhåll.

9.1.2 Dokumentation av Underhåll

Mål: Att allt förebyggande underhåll är dokumenterat för att säkerställa spårbarhet för att förbättra framtida underhållsaktiviteter.

Åtgärder:

- Dokumentera alla utförda underhållsåtgärder, inklusive datum, tid, åtgärder som utförts och ansvarig tekniker.
- Dokumentera och rapportera alla avsteg från planerade underhållsåtgärder, ursprunglig planerad åtgärdsdatum, åtgärd som inte utförts, ansvarig tekniker och förslag till åtgärd.

9.1.3 Utbildning av Personal

Mål: Att all underhållspersonal har den nödvändiga utbildningen och kompetensen som behövs för att utföra förebyggande underhåll.

Åtgärder:

- Genomföra regelbunden utbildning och vid behov certifieringsprogram för underhållspersonal.
- Uppdatera utbildningsmaterial och procedurer baserat på den senaste tekniken och bästa praxis inom förebyggande underhåll.

9.1.4 Användning av Tekniska hjälpmedel

Mål: Tekniska hjälpmedel och verktyg används för att förbättra effektiviteten och noggrannheten i förebyggande underhåll.

Åtgärder:

- Implementera system för tillståndsövervakning som kontinuerligt övervakar utrustningens prestanda och skick.
- Använda automatiserade verktyg för att schemalägga och utföra underhållsåtgärder baserat på utrustningens tillstånd och förutspådda behov.

9.1.5 Riskhantering

Mål: Att risker associerade med förebyggande underhåll för att minimera driftstörningar är identifierade och hanterade.

Åtgärder:

- I underhållsplanen(er) ska det finnas en beskrivning över hanteringen av riskbedömningar före och efter underhållsåtgärder för att identifiera potentiella problem samt metoder för hantera oförutsedda problem som kan uppstå under eller efter underhåll och som inte innebär en driftstörning.

9. 2 Reservdelshantering

9.2.1 Reservdelsregister

Mål: Att ett register över alla kritiska reservdelar som behövs för Telenätet är implementerat för att minimera driftstopp och säkerställa kontinuitet i verksamheten.

Åtgärder:

- Dokumentera alla reservdelar i registret med detaljer som artikelnummer, leverantör, kvantitet, lagringsplats och inköpsdatum.
- Regelbundet uppdatera registret för att säkerställa att det alltid är korrekt och aktuellt.

9.2.2 Lagerhållning och Förvaring

Mål: Att reservdelar lagras på ett sätt som skyddar dem från skador och gör dem lättillgängliga vid behov.

Åtgärder:

- Förvara reservdelar vid behov i kontrollerade miljöer som skyddar mot fukt, damm och temperaturförändringar.
- Märka alla lagringsplatser tydligt för att underlätta snabb åtkomst.

9.2.3 Påfyllning

Mål: Att kritiska reservdelar alltid finns tillgängliga.

Åtgärder:

- Definiera minimumnivåer i registret för lagerhållning av varje reservdel och en indikering för anskaffning när nivåerna når denna gräns.
- Samarbeta med pålitliga leverantörer för att säkerställa snabba leveranser vid behov.

9.2.4 Användning och utbyte

Mål: Att användning och utbyte av reservdelar är dokumenterat i registret för att säkerställa spårbarhet och underlätta framtida inköp.

Åtgärder:

- Registrera varje gång en reservdel används eller byts ut, inklusive detaljer om vilken del som användes, anledningen till bytet, och datumet.
- Genomföra regelbundna revisioner av reservdelshanteringen för att säkerställa att alla processer följs och att lagret är korrekt.

9.2.5 Planering och beredskap

Mål: Att tillgången till reservdelar baserat på förväntad livslängd och användning av utrustningen är säkerställd.

Åtgärder:

- Ta fram en *Underhållsplan(*er). Av planen ska också framgå hur analys av historiska data och framtida behov ska utföras för att förutse efterfrågan på reservdelar.
- Inkludera reservdelshantering i processerna för riskhantering och kontinuitetshantering.

9.2.6 Utbildning och medvetenhet

Mål: Att personalen är utbildad om vikten av korrekt reservdelshantering och rutiner för att säkerställa effektiv hantering.

Åtgärder:

- Genomföra regelbunden utbildning för teknisk personal om Verksamhetsutövarens planer för reservdelshanterings.
- Uppmuntra medarbetare att rapportera eventuella problem eller förbättringsförslag rörande reservdelshantering.

9.3 Uppdateringar av mjukvara

9.3.1 Uppdateringsrutin

Mål: Att hanteringen för uppdatering av mjukvara för alla system och komponenter är planerad och strukturerad.

Åtgärder:

- Ta fram en *Rutin för uppdatering mjukvara inkl. testprotokoll*
- Implementera en centraliserad lösning för att övervaka och hantera uppdateringsstatus för alla komponenter i Telenätet.
- Säkerhetsuppdateringar ska tillämpas skyndsamt utifrån risk och betydelse i enlighet med verksamhetsutövarens riskanalys.

9.3.2 Uppdateringsfrekvens

Mål: Att all programvara och firmware uppdateras regelbundet för att säkerställa att systemen har de senaste förbättringarna och säkerhetsfixarna.

Åtgärder:

- Genomföra månatliga uppdateringar för mindre kritiska system och komponenter.
- Genomföra kvartalsvisa djupgående uppdateringar för hela systemet.
- Omedelbart genomföra uppdateringar efter information från leverantörer.

9.3.3 Testning av Uppdateringar

Mål: Att alla uppdateringar är grundligt testade innan de distribueras till produktionsmiljön.

Åtgärder:

- Skapa en testmiljö som speglar produktionsmiljön för att verifiera uppdateringars effekt.
- Dokumentera och utvärdera resultaten av testning och genomföra nödvändiga justeringar innan fullständig distribution.

9.3.4 Dokumentation och Spårbarhet

Mål: Att alla uppdateringar är dokumenterade för att säkerställa spårbarhet och efterlevnad.

Åtgärder:

- Dokumentera varje tillämpad uppdatering med detaljer som datum, tid, ändringar och ansvarig person.
- Upprätta en revisionslogg för att kunna spåra historiken av alla uppdateringar som har applicerats.

9.3.5 Automatisering

Mål: Att automatiserade verktyg och processer används för att förbättra effektiviteten och noggrannheten i hanteringen av uppdateringar.

Åtgärder:

- Implementera automatiserade system för att skanna efter tillgängliga uppdateringar.
- Använda automatiserade distributionstekniker för att tillämpa uppdateringar med minimal manuell inblandning.

9.3.6 Riskhantering

Mål: Att risker associerade med uppdatering alltid bedöms och hanteras för att minimera driftstörningar.

Åtgärder:

- Ta fram en *Rutin för Riskbedömning och återställning mjukvara* som hanterar riskbedömningar före och efter uppdateringar samt metoder för att för att snabbt kunna rulla tillbaka uppdateringar om oväntade problem uppstår.

9.3.7 Kommunikation och Medvetenhet

Mål: Att alla relevanta parter är medvetna om planerade uppdateringar samt deras potentiella påverkan.

Åtgärder:

- Informera alla intressenter om kommande uppdateringar genom regelbundna meddelanden och statusrapporter.
- Utbilda personal om vikten av uppdatering samt hur de kan rapportera problem som kan uppstå.

9.4 Akut underhåll

Mål: Att säkerställa en snabb och effektiv hantering av akuta underhållsbehov för att minimera driftstörningar, genom att upprätthålla en hög reparationsberedskap med stöd av Stadsnätsföreningens MoU för Motståndskraft och Uthållighet.

Åtgärder:

- Säkerställa att personal som utför ensamarbete är utbildat på, och tillämpar, Svenska Stadsnätsföreingens *Anvisning för ensamarbete i optiska fibernät för situationer som är normala, kritiska samt vid höjd beredskap*.
- Säkerställa tillgängligheten av utrustning.
- Kontinuerligt genomföra beredskapsutbildningar för ny personal samt repetitionsutbildning.
- Att via CRISIS och SISG dela lägesbild samt samverka om resursförstärkning.
- Deltagande i gemensamma krisövningar.

10 Anskaffning

Syfte: Säkerställa att Verksamhetsutövaren har en strukturerad och kontrollerad hantering för anskaffning av materiel för Telenätet och anlitande av uppdragstagare för att stödja verksamhetens behov och säkerhetskrav. För hantering av leverantörer se *kap 15.3 Leverantörshantering*.

Anskaffning av produkter, tjänster och leverantörer ska ske riskbaserat. Bedömning av säkerhetskrav, leverantörsrisker och avtalsvillkor ska baseras på verksamhetsutövarens riskanalys och den betydelse som den aktuella anskaffningen har för telenätets och teletjänsternas funktion och säkerhet.

10.1 Anskaffningsrutin

Mål: Att alla anskaffningar sker enligt fastställda krav och riktlinjer.

Åtgärder:

- Ta fram en *Anskaffningsrutin* som inkluderar steg för behovsanalys, leverantörsutvärdering, riskbedömning och godkännande.
- Säkerställ att alla anskaffningar genomgår en riskanalys för att identifiera och hantera potentiella säkerhetsrisker.

10.2 Anskaffningskontroll och dokumentation

Anskaffningskontroll kan omfatta granskning av leverantörens säkerhetsförmåga, relevanta avtalsvillkor, krav på incidentrapportering, informationssäkerhet samt möjligheter till uppföljning och revision.

Mål: Att säkerställa att anskaffning av produkter, tjänster och leverantörer sker på ett riskbaserat sätt och att säkerhetskrav, leverantörsrisker och avtalsvillkor beaktas i syfte att skydda telenätets och teletjänsternas funktion och säkerhet.

Åtgärder:

- Säkerställa att anskaffning av produkter, tjänster och leverantörer föregås av en bedömning baserad på verksamhetsutövarens riskanalys och den betydelse som anskaffningen har för telenätet och tillhandahållna teletjänster.
- Identifiera anskaffningar som avser produkter, tjänster eller leverantörer av särskild betydelse för verksamheten och säkerställa att dessa omfattas av fördjupad säkerhetsbedömning.
- Säkerställa att säkerhetskrav beaktas i kravställning och upphandling, inklusive krav på informationssäkerhet, incidentrapportering, kontinuitet och skydd av information.
- Säkerställa att avtal och överenskommelser med leverantörer innehåller relevanta bestämmelser om säkerhet, rapportering av incidenter samt möjligheter till uppföljning.

- Dokumentera genomförda bedömningar, beslut och säkerhetskrav i samband med anskaffning på ett sätt som möjliggör uppföljning, revision och tillsyn.

10.3 Utbildning och medvetenhet

Mål: Att säkerställa att berörda roller har tillräcklig kunskap, hjälpmedel och medvetenhet för att beakta säkerhetsaspekter vid anskaffning av produkter, tjänster och leverantörer.

Åtgärder:

- Identifiera vilka roller som deltar i eller påverkar anskaffningsprocesser, exempelvis inom inköp, teknik, IT, säkerhet, juridik och ledning.
- Säkerställa att berörda roller har grundläggande kunskap om cybersäkerhetskrav, leverantörsrisker och anskaffningens betydelse för telenätets och teletjänsternas säkerhet.
- Genomföra riktad utbildning eller informationsinsatser för berörda roller i samband med införande av nya rutiner, förändrade säkerhetskrav eller uppdaterad lagstiftning.
- Säkerställa att utbildning och informationsinsatser dokumenteras och vid behov följs upp inom ramen för verksamhetens uppföljnings- och kvalitetsprocesser.

11 Förändringar

Förändringar i telenät, teletjänster och verksamhetssystem ska hanteras riskbaserat. Omfattning av krav på analys, testning, godkännande och uppföljning ska anpassas efter förändringens betydelse och påverkan på verksamheten, användare och samhällsfunktioner.

Syfte: Säkerställa att alla förändringar i Telenätet och Teletjänsterna är noggrant planerade, godkända och testade för att minimera risken för driftstörningar och säkerhetsincidenter.

11.1 Förändringsprocesser

Mål: Att allt förändringsarbete genomförs planerat och strukturerat för att hantera förändringar i Telenät och Teletjänster och verksamhetssystem.

Åtgärder:

- Ta fram *Process för förändring i Telenät och Teletjänster* med processer för Normala/Standard/Akuta förändringar.
- Komplettera processerna med erforderliga rutiner och anvisningar.
- Säkerställ att alla förändringar är föremål för riskbedömning och att nödvändiga säkerhetsåtgärder identifieras och implementeras.
- Säkerställa att förändringar klassificeras utifrån omfattning, risk, betydelse och påverkan för telenätets och teletjänsternas funktion, och att förändringsprocessen anpassas därefter.
- Genomförda säkerhetsåtgärder kompletteras med penetrationstester.

11.2 Testning av Förändringar

Mål: Att alla förändringar är noggrant testade innan de införs i produktionsmiljön.

Åtgärder:

- Implementera en testmiljö som speglar produktionsmiljön för att kunna utföra nödvändiga tester av förändringar.
- Säkerställa att testning omfattar bedömning av påverkan på säkerhet, driftsäkerhet, kontinuitet och incidenthantering i den utsträckning som är motiverad utifrån förändringens betydelse.
- Dokumentera testresultaten och genomför en utvärdering för att identifiera eventuella problem eller risker.

11.3 Godkännande av förändringar

Mål: Att alla förändringar är godkända av behöriga parter innan implementering.

Åtgärder:

- Säkerställa att ansvar för godkännande av förändringar är tydligt definierat och anpassat efter förändringens betydelse, exempelvis genom olika godkännandenivåer för mindre respektive mer omfattande förändringar.
- Beslut ska dokumenteras i enlighet med fastställda rutiner.

11.4 Kommunikation och medvetenhet

Mål: Att alla berörda parter är medvetna om planerade förändringar och deras potentiella påverkan.

Åtgärder:

- Informera anställda, kunder och andra intressenter om kommande förändringar enligt fastställda rutiner.
- Säkerställa att information om förändringar kommuniceras i god tid före införande, i den utsträckning det är möjligt.

11.5 Implementering och kontroll

Mål: Att förändringar implementeras på ett kontrollerat sätt och att de övervakas noggrant för att upptäcka och åtgärda problem snabbt.

Åtgärder:

- Innan implementering ska berörda tillgångar vara säkerhetskonfigurerade (härdade) och planer för återställning vara framtagna och godkända.
- Kontrollera och övervaka förändringsimplementeringen noggrant och ha beredskap för att snabbt kunna återgå till tidigare konfiguration om problem uppstår.
- Säkerställa att genomförda förändringar följs upp i syfte att verifiera att avsedd funktion och säkerhetsnivå har uppnåtts samt att inga oönskade effekter har uppstått.

11.6 Dokumentation

Mål: Att alla förändringar är noggrant dokumenterade för att säkerställa spårbarhet och efterlevnad.

Åtgärder:

- Dokumentera varje förändring inklusive dess syfte, detaljer om genomförandet, testresultat, ansvariga och godkännanden.
- Säkerställa att dokumentationen är tillgänglig för alla relevanta parter och uppdateras vid behov.
- Dokumentation av förändringar ska bevaras under sådan tid att spårbarhet, uppföljning, incidentutredning och tillsyn kan säkerställas.

12 Incidenter

Syfte: Säkerställa att alla incidenter- och integritetsincidenter identifieras, hanteras, dokumenteras och rapporteras internt, till berörda parter och relevanta myndigheter på ett strukturerat sätt för att minimera påverkan och förbättra den övergripande säkerheten.

12.1 Incidenthantering

12.1.1 Incident

Mål: Att processer för identifiering, hantering och dokumentering av incidenter är framtagna och implementerade.

Åtgärder incidenter:

- Identifiering: Verksamhetsutövaren ska ha en *Process för incidenter* baserad på etablerade standarder.
- Hantering: Processen ska medge initial bedömning, isolering av påverkat system, åtgärdsplanering och genomförande.
- Dokumentation: Alla incidenter ska noggrant dokumenteras för att säkerställa spårbarhet och framtida analyser.
- Analys: Genomföra en analys och ta fram en rapport för varje incident för att bedöma orsaker, påverkan och konsekvenser. Om det kvarstår en okänd underliggande orsak till en eller flera incidenter som har lett till en störning i Telenät eller Teletjänster ska Verksamhetsutövaren ha en *Process för problemhantering* för att hantera dessa.
- Rapportering: Det ska finnas en rutin för rapportering av Incidenter.
- Löpande uppföljning: *Process för incidenter* och rutiner ska löpande utvärderas och förbättras baserat på erfarenheter och lärdomar från tidigare incidenter.
- Tillgänglighet: Det ska finnas en förteckning som hanterar vilka som ska ges tillgång till dokument och rapporter.

Vid incidenter som riskerar att påverka verksamhetens kontinuitet ska incidenthanteringen samordnas med kontinuitets- och krishanteringsprocesserna enligt kapitel 15 och 19.

Incidenter som har sitt ursprung hos eller påverkar leverantörer ska hanteras i samverkan med leverantören enligt kapitel 14.3.5.

12.1.2 Integritetsincident

Mål: Att processer och rutiner för identifiering, hantering och dokumentering av integritetsincidenter är framtagna och implementerade.

Åtgärder integritetsincidenter - brottsdatalagringsincidenter

- Identifiering: Verksamhetsutövaren ska ha en *Process för integritetsincidenter* baserad på etablerade standarder.
- Hantering: Processen ska medge initial bedömning av integritetstyp, isolering av påverkat system, åtgärdsplanering och genomförande.
- Dokumentation: Alla incidenter ska noggrant förtecknas för att säkerställa spårbarhet och underlätta framtida analyser. Förteckningen ska innehålla:
  1. datum då integritetsincidenten inträffade,
  2. en beskrivning av integritetsincidenten,
  3. uppskattat antal berörda abonnenter eller användare,
  4. bedömda konsekvenser av integritetsincidenten,
  5. orsak till att integritetsincidenten inträffade,
  6. de åtgärder som vidtagits, och
  7. referensnummer.
- Analys: Genomföra en analys och ta fram en rapport för varje incident för att bedöma orsaker, påverkan och konsekvenser.
- Rapportering: Det ska finnas en rutin för rapportering av Incidenter.
- Löpande uppföljning: *Process för integritetsincidenter* och rutiner ska löpande utvärderas och förbättras baserat på erfarenheter och lärdomar från tidigare incidenter.
- Tillgänglighet: Det ska finnas en förteckning som hanterar vilka som ska ges tillgång till dokument och rapporter.

12.2 Incidentrapportering

12.2.1 Incident

Intern rapportering

Mål: Att alla inträffade incidenter och integritetsincidenter rapporteras internt.

Åtgärder:

- Internrapportera till Incidentansvarig i enlighet processen för incidenthantering.
- Rapporterna ska dokumenteras och finnas tillgängliga.
- Det ska finnas en förteckning som hanterar vilka som ska ges tillgång till dokument och rapporter.

Rapportering till myndigheter

Mål: Att inträffade incidenter dokumenteras och rapporteras till MCF enligt gällande föreskrifter.

Åtgärder:

En incident är en inträffad oönskad händelse som påverkar:

- Konfidentialitet (till exempel obehörig åtkomst)
- Riktighet (till exempel förvanskning eller förlust)
- Tillgänglighet (till exempel avbrott)
- En incident kan bero på brister i det systematiska cybersäkerhetsarbetet, resursbrist, säkerhetsläget och kriminalitet samt förändringar i klimat och miljö. En incident kan leda till påverkan på it-miljö, verksamhet och samhälle.

Verksamhetsutövare ska rapportera betydande incidenter. Följande typer av incidenter anses vara betydande enligt Cybersäkerhetslagen:

- En incident som orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamheten
- En incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

Upplysning inom 24 timmar
Inom 24 timmar från det att verksamhetsutövaren identifierat en incident som är rapporteringspliktig ska verksamhetsutövaren inkomma med en Upplysning. Den ska redogöra för om den betydande incidenten misstänks ha orsakats av olagliga eller avsiktligt skadliga handlingar eller kan ha gränsöverskridande verkningar.
1. verksamhetsutövarens namn, kontaktuppgifter och organisationsnummer,
2. när incidenten inträffade,
3. när incidenten upptäcktes,
4. om incidenten är pågående,
5. en preliminär bedömning om incidenten orsakats av en olaglig eller avsiktligt skadlig handling,
6. information om incidenten har sitt ursprung hos en leverantör, inklusive namn och organisationsnummer till leverantören,
7. en preliminär bedömning om vilka konsekvenser incidenten medför eller riskerar att medföra, och
8. en preliminär bedömning om incidenten har eller riskerar att få gränsöverskridande konsekvenser.

Incidentanmälan inom 72 timmar
Inom 72 timmar från att verksamhetsutövaren har identifierat en incident som är rapporteringspliktig ska verksamhetsutövaren inkomma med en Incidentanmälan. Incidentanmälan ska uppdatera den information som lämnats i Upplysning samt innehålla en bedömning av den betydande incidenten, dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer.
1. hur länge incidenten pågått,
2. hur incidenten upptäcktes,
3. i tillämpliga fall, när incidenten avhjälptes,
4. en preliminär bedömning om incidentens orsak,

5. i tillämpliga fall, information om angreppsindikatorer,
6. påverkan på ett systems förmåga att upprätthålla konfidentialitet, riktighet inklusive autenticitet, och tillgänglighet,
7. i tillämpliga fall, påverkan på behandlad informations konfidentialitet, riktighet inklusive autenticitet, och tillgänglighet,
8. i tillämpliga fall, en detaljerad beskrivning av de konsekvenser som incidenten medfört eller riskerar att medföra, och
9. information om a) antalet drabbade slutanvändare, b) berört geografiskt område, c) ekonomisk skada, och d) gränsöverskridande konsekvenser.

Slutrapport inom en månad
Inom en månad från det första rapporteringstillfället ska verksamhetsutövaren inkomma med en slutrapport. Slutrapporten ska innehålla en komplettering och uppdatering av uppgifter som lämnats enligt 2–3 §§. I tillämpliga fall ska den även innehålla en beskrivning av vilka tekniska och organisatoriska åtgärder som vidtagits eller kommer att vidtas för att:
1. hantera incidenten,
2. hantera och minimera konsekvenserna av incidenten, och
3. undvika att liknande incidenter inträffar.
En lägesrapport ska innehålla uppgifter om :
1. varför incidenten fortfarande är pågående,
2. hur länge incidenten förväntas pågå,
3. i tillämpliga fall, information om angreppsindikatorer, och
4. om incidenten fortfarande påverkar eller riskerar att påverka, verksamhetsutövarens egen verksamhet, annan sektorsverksamhet eller viktiga samhällsfunktioner.
Kan verksamhetsutövaren lämna den information som behöver ingå i Slutrapport inom 72 timmar efter Upplysning, är det tillåtet att lämna Incidentanmälan och Slutrapport vid samma rapporteringstillfälle. Verksamhetsutövaren behöver i dessa fall inte inkomma med en tredje rapport.

12.2.2 Integritetsincident

Mål: Att alla inträffade integritetsincidenter dokumenteras och rapporteras till relevanta myndigheter så som Post- och telestyrelsen (PTS) och Integritetsskyddsmyndigheten (IMY)

Åtgärder:

- Rapporterna ska dokumenteras och finnas tillgängliga.
  - Om en personuppgiftsincident inträffat ska den anmälas till IMY inom 72 timmar. För ytterligare information se IMY (imy.se), ”Hantering av personuppgiftsincidenter”.
  - Om en integritetsincident inträffat ska den anmälas till PTS:
    - En inledande rapport ska lämnas in utan dröjsmål dock senast inom 24 timmar.
    - En kompletterande rapport med ytterligare uppgifter ska lämnas så snart som det är möjligt, dock senast tre dagar efter den inledande rapporten.
    - Om incidenten skulle kunna ha negativ påverkan på kunder eller andra användare negativt, ska även dessa informeras utan onödigt dröjsmål.

13 Riskanalys, risk- och åtgärdshantering

Syfte: Att identifiera, bedöma och hantera risker som kan påverka säkerheten för Telenätet och Teletjänsterna, inklusive organisatoriska, logiska och fysiska hot. Arbetet ska följa etablerade standarder, normer, säkerhetsvägledningar och praxis.

Rekommendation: För hantering av risk- och sårbarhetsanalyser samt åtgärdshantering har Stadsnätsföreningen tagit fram ett verktyg. Verktyget ***Bashot telekom*** är tillgängligt under: Robust digital infrastruktur - Stadsnätsföreningen

13.1 Övergripande arbetsmetod

Mål: Att ha infört dynamiska arbetsmetoder som snabbt kan anpassas till nya hot och förändringar i verksamhetsmiljön.

Åtgärder:

- Ta fram processer och rutiner för riskanalys.
- Ta fram processer och rutiner för risk-och åtgärdshantering.
- Inkludera processerna som en integrerad del av Verksamhetsutövarens strategiska planering och beslutsfattande.
- Beakta erfarenheter från tidigare inträffade integritets- eller brottsdatalagringincidenter, allmänt uppmärksammade integritets- eller brottsdatalagringsincidenter samt aktuella och relevanta omvärldsföreteelser.
- Tillämpa processer och åtgärder som utgår från etablerad standarder, normer, säkerhetsvägledningar och praxis.

13.2 Riskanalys

Riskanalyser ska omfatta organisatoriska, logiska och fysiska hot.

Riskanalyser ska göras för varje informationsbehandlingstillgång och förbindelse.

För likvärdiga informationsbehandlingstillgångar och förbindelser kan en gemensam riskanalys göras.

Riskanalyserna ska genomföras minst en gång per år samt:

- inför anskaffning av informationsbehandlingstillgångar och förbindelser där behandlade uppgifter förekommer och vid anlitande av uppdragstagare,
- efter att tidigare okända hot som är relevanta för riskanalysen identifierats,
- inför planerade förändringar.

Information om sådana hot som avses i första stycket kan förmedlas av Post- och telestyrelsen.

Mål: Att riskerna för att informationsbehandlingstillgångar eller förbindelser är identifierade och inte orsakar integritets- eller brottsdatalagringsincidenter.

Åtgärder:

- Ta fram en plan för vid vilka tidpunkter och i vilka situationer riskanalyser ska genomföras.

- Identifiera relevanta hot mot den aktuella informationsbehandlingstillgången eller förbindelsen som kan leda till att en integritets- eller brottsdatalagringsincident inträffar.
- Gör en bedömning av vilka konsekvenser som kan uppstå i händelse av att identifierade hot realiseras.
- Gör en bedömning av sannolikheten för att identifierade hot realiseras.
- Gör en sammanvägd bedömning av sannolikheten för att identifierade hot inträffar och de konsekvenser det kan medföra om de realiseras (riskbedömning).

Anm: I riskanalyser inför planerade förändringar ska tillhandahållare som är lagringsskyldiga enligt 9 kap. 19 lagen (2022:482) om elektronisk kommunikation analysera risken för att förändringarna orsakar en brottsdatalagringsincident genom att:

- Identifiera relevanta hot mot säkerheten för uppgifter som lagras för brottsbekämpande ändamål med anledning av den planerade förändringen.
- Göra en bedömning av vilka konsekvenser som kan uppstå i händelse av att identifierade hot realiseras.
- Göra en bedömning av sannolikheten för att identifierade hot realiseras
- Gör en sammanvägd bedömning av sannolikheten för att identifierade hot inträffar och de konsekvenser det kan medföra om de realiseras (riskbedömning).
- Dokumentera genomförda riskanalyser.

13.3 Risk-och åtgärdshantering

Mål: Organisationen har säkerställt att identifierade risker hanteras på ett strukturerat, proportionerligt och dokumenterat sätt. Beslut om hur risker ska hanteras baseras på genomförda riskbedömningar och leder till att risker undviks, reduceras eller, när det är motiverat, accepteras. Lämpliga tekniska och organisatoriska åtgärder vidtas för att säkerställa att risknivåerna hålls på en acceptabel nivå med hänsyn till riskernas allvar, tillgänglig teknik och kostnader.

Åtgärder riskhantering:

- Genomföra riskbedömning och besluta om hur respektive risk ska hanteras genom att avgöra om riskerna ska undvikas, reduceras eller accepteras.
- Dokumentera beslut om åtgärd, Beslut om att acceptera en risk ska motiveras.

Anm: *Tillhandahållaren bör eftersträva att reducera risker framför att acceptera dem.*

Åtgärder efter riskbedömning

- Vidta de tekniska och organisatoriska åtgärder som krävs för att hantera de risker som ska undvikas eller reduceras. Åtgärderna ska vidtas på en nivå som är anpassad till den risk som föreligger, med beaktande av tillgänglig teknik och kostnaderna för åtgärderna.
  Anm: *Första stycket andra meningen gäller inte för sådana uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (2022:482) om elektronisk kommunikation. Tillhandahållaren ska för sådana uppgifter vidta åtgärder i enlighet med 9 kap. 4 § förordningen (2022:511) om elektronisk kommunikation.*

- Dokumentera bedömningen vid val av åtgärder.
- Följ upp åtgärderna årligen och vid behov.

Särskilda åtgärder vid planerade förändringar

När tillhandahållarens riskanalys visar att det finns risker för att planerade förändringar kan orsaka en brottsdatalagringsincident ska tillhandahållaren tillämpa en process som utgår från etablerad standard på området och utöver vad som följer av punkten ovan åtminstone vidta följande åtgärder:

- Utföra tester inför förändringen och efter förändringen verifiera att den inte påverkat säkerheten negativt.
- Säkerhetskonfigurera (härda) berörda informationsbehandlingstillgångar.
- Ta fram planer för att återställa behandlade uppgifter i händelse av att en brottsdatalagringsincident inträffar.

Tester, härdning, och planer för återställande eller åtgärdande ska vara anpassade till den planerade förändringens art och omfattning.

13.4 Kommunikation och rapportering

Mål: Att riskrelaterad information kommuniceras effektivt inom Verksamhetsutövarens organisation och till relevanta externa parter.

Åtgärder:

- Ta fram en *Rutin för riskrapportering* till ledningen och andra intressenter.
- Rapporterna ska dokumenteras enligt rutin och finnas tillgängliga.
- Det ska finnas en förteckning som hanterar vilka som ska ges tillgång till dokument och rapporter.

13.5 Efterlevnad och revision

Mål: Att riskhanteringsprocesserna uppfyller relevanta lagar, föreskrifter och standarder.

Åtgärder:

- Genomföra årliga revisioner av riskhanteringsprocesserna för att identifiera och åtgärda eventuella brister.
- Anpassa riskhanteringsstrategier baserat på resultaten från interna och externa revisioner.

14 Säkerhetshantering

Syfte: Syftet med detta kapitel är att säkerställa att verksamhetsutövaren vidtar lämpliga och proportionerliga tekniska, organisatoriska och administrativa säkerhetsåtgärder för att skydda telenät och tillhandahållna teletjänster.

Kapitlet ska säkerställa skydd av anläggningar, informationsbehandlingstillgångar och information samt hantering av säkerhetsrisker kopplade till leverantörer och leveranskedjan.

Säkerhetsåtgärderna ska baseras på genomförda riskanalyser och syfta till att upprätthålla tillgänglighet, riktighet, konfidentialitet och autenticitet i telenät och teletjänster i enlighet med gällande lagstiftning.

14.1 Skydd av anläggningar

Syfte: Säkerställa att Telenätet, exempelvis förbindelser, kopplingsskåp och annan kritisk utrustning, är skyddad mot fysiska hot som kan påverka säkerheten. Säkerställa att endast behöriga individer har åtkomst till Verksamhetsutövarens anläggningar och system genom att reglera och kontrollera en användares behörighet.

Skyddsåtgärder för anläggningar ska fastställas utifrån anläggningarnas betydelse och påverkan för verksamheten, samhällsfunktioner och användare samt resultatet av genomförd riskanalys enligt kapitel 12 Riskanalys, risk- och åtgärdshantering. Skyddsnivån ska vara proportionerlig mot den påverkan en incident kan få på telenät, teletjänster och samhällsviktiga funktioner.

14.1.1 Fysiskt skydd

Mål: Att kritisk utrustning skyddas från fysiska skador och miljöpåverkan.

Åtgärder:

- Förstärka byggnader och rum som innehåller kritisk utrustning för att motstå fysiska attacker.
- Säkerställa att all utrustning är installerad i säkra rack och skåp.
- Installera brandsläckningssystem och säkerställa att branddetektorer är fullt fungerande.
- Implementera översvämningsskydd och säkerställa att dräneringssystem är effektiva.

14.1.2 Skyddsåtgärder för tillträde till anläggningar

Mål: Att tillträde till anläggningar endast tilldelas behöriga anställda eller uppdragstagare som behöver det för att kunna utföra sina arbetsuppgifter.

Åtgärder:

- Ansvaret för hantering av åtkomst och behörighet har säkerhetsansvarig eller motsvarande roll inom Verksamhetsutövarens organisation.
- Upprätta och underhålla en *Rutin för tillträde till anläggningar*.
- Implementera ett System för tilldelning, ändring, uppföljning och kontroll av identiteter och behörigheter för att säkerställa spårbarhet och efterlevnad.
- Införa en funktion för begränsning av tid och omfång för tilldelade behörigheter. Tilldelade behörigheter ska tas bort efter utfört uppdrag.

- Tilldelade behörigheter ska följas upp årligen och vid behov justeras eller återkallas.

14.1.3 System för tillträde

Mål: Begränsa obehörig åtkomst till kritiska anläggningar.

Åtgärder:

- Implementera system för tillträdeskontroll.
- Installera säkerhetsdörrar med elektroniska låssystem och kortläsare.
- Använda biometriska autentiseringsmetoder där det är möjligt.
- Upprätta en åtkomstlogg för att registrera alla personer som får tillträde till anläggningarna.

14.1.4 Övervakning

Mål: Att alla kritiska anläggningar är övervakade dygnet runt.

Åtgärder:

- Installera övervakningskameror med inspelningskapacitet vid alla ingångar och viktiga områden inom anläggningarna.
- Anslut övervakningssystemen till en central övervakningsenhet som är bemannad dygnet runt.
- Implementera rörelsedetektorer och larm för att upptäcka och rapportera obehöriga intrång.
- Lagringstid, åtkomst och ändamål för inspelat material ska dokumenteras och begränsas i enlighet med dataskyddsförordningen (GDPR).

14.1.5 Säkerhetsrevisioner

Mål: Att den fysiska säkerheten för att identifiera och åtgärda potentiella säkerhetsbrister regelbundet granskas och förbättras.

Åtgärder**:**

- Ta fram en *Plan säkerhetsrevisioner kritiska anläggningar*.
- Utföra årliga säkerhetsrevisioner av alla kritiska anläggningar.
- Dokumentera resultaten av revisionerna och skapa en åtgärdsplan för att hantera identifierade brister.
- Säkerställa att alla åtgärder genomförs inom tre månader efter revisionen.

14.2 Skyddsåtgärder för information

Syfte: Säkerställa att behandlade uppgifter, nätdata samt uppgifter för brottsbekämpande ändamål identifieras, klassas och skyddas mot oavsiktlig eller otillåten utplåning samt oavsiktlig förlust eller ändring.

Anm:

I en kommunal verksamhet ska villkoren i Offentlighets- och sekretesslagen tillämpas vid utlämnande av uppgifter.

14.2.1 Informationssäkerhet

Mål: Säkerställa att informationen endast ska vara tillgänglig för behöriga (konfidentialitet), är korrekt och skyddad mot obehörig förändring (riktighet), finns tillgänglig när den behövs (tillgänglighet).

Åtgärder:

- Klassa information för behandlade uppgifter, nätdata och brottsbekämpande ändamål. Ska minst omfatta:
    - Kund- och avtalsinformation
    - Drift- och övervakningsinformation
    - Nät- och arkitekturdokumentation
    - Konfigurationsdata och behörighetsinformation
    - Loggar och incidentrapporter
    - Information som omfattas av sekretess eller dataskydd
    - Klassningen ska dokumenteras och kopplas till respektive Informationsbehandlingstillgång.
- Fastställ skyddsåtgärder för respektive klass
- Dokumentera skyddsåtgärderna
- Klassningsmodell. Utifrån konfidentialitet, riktighet och tillgänglighet fastställa skyddsnivåer för informationen. Exempel på nivåer:
    - Strängt konfidentiell
    - Konfidentiell
    - Intern
    - Öppen
- Nivåernas innebörd ska vara dokumenterade och kända i organisationen.

14.2.2 Åtkomst och behörighet för behandlade uppgifter och nätdata

Mål: Att åtkomst/behörighet till Verksamhetsutövarens system för behandlade uppgifter och nätdata endast tilldelas anställda eller uppdragstagare som behöver det för att kunna utföra sina arbetsuppgifter.

Åtgärder:

- Ansvaret för hanteringen av åtkomst och behörighet tilldelas säkerhetsansvarig eller motsvarande roll inom Verksamhetsutövarens organisation.
- Ta fram en process för tilldelning, ändring och uppföljning av tilldelade behörigheter. Tilldelade behörigheter ska dokumenteras samt följas upp årligen och vid behov.

- Implementera ett System för tilldelning, ändring, uppföljning och kontroll av identiteter och behörigheter för att säkerställa spårbarhet och efterlevnad.
- Följa upp tilldelade behörigheter årligen och vid behov justera eller återkalla.
- Granska åtkomstloggar regelbundet för att upptäcka avvikelser och misstänkt aktivitet. Identifierade avvikelser ska hanteras i enlighet med Verksamhetsutövarens process för incidenthantering enligt kapitel 11.
- Säkerställ att åtkomst endast ges till den som har upplysts om tystnadsplikten i de fall 9 kap. 31 och 32 §§ lagen (2022:482) om elektronisk kommunikation är tillämpliga.

Rekommendationer:

- Införa en funktion för begränsning av tid och omfattning för tilldelade behörigheter särskilt för tillfälliga uppdragstagare.
- Ta bort tilldelade behörigheter efter utfört uppdrag.
- Utbilda och informera regelbundet den som kommer i kontakt med behandlade uppgifter om när och på vilket sätt behandlade uppgifter får hanteras.
- Utbilda den som kommer i kontakt med behandlade uppgifter i att upptäcka integritets- eller brottsdatalagringsincidenter och att analysera tänkbara konsekvenser
- av en inträffad integritets- eller brottsdatalagringsincident för abonnenter och användare, inklusive brottsbekämpande myndigheter.

14.2.3 Skyddsåtgärder för uppgifter för brottsbekämpande ändamål

Mål: Att åtkomst/behörighet till Verksamhetsutövarens system för hantering av uppgifter för brottsbekämpande ändamål endast tilldelas anställda eller uppdragstagare som behöver det för att kunna utföra sina arbetsuppgifter.

Åtgärder:

- Ansvaret för hanteringen av åtkomst och behörighet tilldelas säkerhetsansvarig eller motsvarande roll inom Verksamhetsutövarens organisation.
- Upprätta och underhålla en *Rutin för åtkomst och behörighet till uppgifter för brottsbekämpande ändamål*.
- Implementera ett System för tilldelning, ändring, uppföljning och kontroll av identiteter och behörigheter för att säkerställa spårbarhet och efterlevnad.
- Införa en funktion för begränsning av tid och omfång för tilldelade behörigheter. Tilldelade behörigheter ska tas bort efter utfört uppdrag.
- Tilldelade behörigheter ska följas upp årligen och vid behov justeras eller återkallas.
- Åtkomst och användning av uppgifter för brottsbekämpande ändamål ska loggas och följas upp regelbundet. Avvikelser ska hanteras enligt fastställd incidenthanteringsprocess.

14.2.4 Skyddsåtgärder mot oavsiktlig eller otillåten utplåning eller förlust av uppgifter

Behandlade uppgifter och nätdata

Mål: Att behandlade uppgifter och nätdata skyddas mot oavsiktlig eller otillåten utplåning samt oavsiktlig förlust eller ändring.

Åtgärder:

- Ta fram en *Rutin för säkerhetskopiering av behandlade uppgifter* och nätdata för varaktig lagring av behandlade uppgifter och driftinformation.

Rekommendationer:

- Säkerhetskopiera behandlade uppgifter och nätdata.
- Återläsning av säkerhetskopior ska verifieras åtminstone årligen.

Uppgifter för brottsbekämpande ändamål

Mål: Att behandlade uppgifter för brottsbekämpande ändamål skyddas mot oavsiktlig eller otillåten utplåning samt oavsiktlig förlust eller ändring.

Åtgärder:

- Ta fram en *Rutin för säkerhetskopiering av uppgifter för brottsbekämpande ändamål* för uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (2022:482) om elektronisk kommunikation.
- Lagra uppgifter för brottsbekämpande ändamål på minst två fysiskt åtskilda platser.
- Säkerhetskopior ska omfattas av samma skydd och utplånas samtidigt som de uppgifter som lagras för brottsbekämpande ändamål.
- Återläsning av säkerhetskopior ska verifieras åtminstone årligen.

14.2.5 Loggning

Mål: Att systemen för behandlade uppgifter, nätdata och uppgifter för brottsbekämpande ändamål har funktioner för att logga all läsning, kopiering, ändring och utplåning av uppgifter, samt för åtkomsten till systemen.

Åtgärder:

- Ta fram en *Rutin för hantering av loggar*.
- Logga all läsning, kopiering, ändring och utplåning av behandlade uppgifter
- Logga åtkomst till de system som används för behandling av behandlade uppgifter.
- Logga på ett sådant sätt att det går att se vem som har vidtagit vilken åtgärd med vilka uppgifter och vid vilken tidpunkt.
- Kontrollera relevanta loggar vid misstanke om att en integritets- eller brottsdatalagringsincident har inträffat.
- Inför en kontroll som säkerställer att den som har haft tillgång till uppgifter enligt ovan inte kan ges tillgång till loggar avseende åtkomst till uppgifterna.
- Kontrollera loggarna systematiskt och återkommande.
- Dokumentera genomförda kontroller av loggar.
- Logga alla systemhändelser som är nödvändiga för att kunna utreda säkerhetsincidenter.
- Innan uppgifter som lagras för brottsbekämpande ändamål utplånas ska ansvarig utföra en systematisk kontroll av loggar avseende åtkomst till uppgifterna. I samband med att uppgifterna utplånas ska även loggar utplånas.

Rekommendationer:

- Övervaka alla loggar automatisk. Detta gäller inte för loggar avseende åtkomst till uppgifter som ska lagras för brottsbekämpande ändamål.

14.2.6 Utlämnande av uppgift som gäller brottslig verksamhet eller misstanke om brott

Mål: Målet är att säkerställa att relevant information om brott eller misstänkta brott kan delas på ett korrekt, lagligt och säkert sätt med behöriga myndigheter, så att brott kan förebyggas, upptäckas och utredas.

Åtgärder:

Utlämnande utan dröjsmål

- Vid en begäran om utlämnande av historiska uppgifter ska den lagringsskyldige lämna ut uppgifter i sin helhet enligt följande:

  1. Omedelbart vid akut hot mot person eller egendom eller vid fara för liv eller hälsa.

  2. Så snart som möjligt, dock senast inom 8 timmar, när det är av avgörande vikt enligt begärande myndighet.

  3. Så snart som möjligt, dock senast inom 48 timmar, i andra fall än vad som anges i punkterna 1 och 2, om inte en längre tidsfrist har accepterats av begärande myndighet.

  Tidsfristerna räknas från den tidpunkt när begärande myndighet skickar begäran. Om begärande myndighet särskilt efterfrågar det och uppgifter inte kan lämnas ut i sin helhet vid samma tillfälle ska uppgifterna lämnas ut successivt så snart uppgifterna blir tillgängliga hos den lagringsskyldige, dock inom ovan angivna tidsfrister.

- Vid en begäran om utlämnande av realtidsuppgifter ska den lagringsskyldige lämna ut uppgifter omedelbart, om inte annat har accepterats av begärande myndighet i det enskilda fallet.

Utlämnande i enhetligt format

- Vid utlämnande av uppgifter ska den lagringsskyldige använda etablerad standard.
- Vid utlämnande av historiska uppgifter ska den lagringsskyldige använda filformatet .xml, om inte begärande myndighet i det enskilda fallet har efterfrågat eller accepterat ett annat filformat.

Etablerad standard som bör användas är den senaste versionen av ETSI TS 102.232-1 – 7 (för realtidsuppgifter) och ETSI TS 102.657 (för historiska uppgifter) om inget annat är överenskommet med begärande myndighet.
För vidare vägledning kan den lagringsskyldige utgå från de tillämpningsanvisningar som Polismyndigheten lämnar angående enhetligt format.

14.2.7 Kryptering

Mål: Att behandlade uppgifter som överförs över Internet skyddas.

Åtgärder övergripande:

- Ta fram en *Rutin för hantering av kryptering och kryptonycklar* avseende behandlade uppgifter, nätdata och uppgifter för brottsbekämpande ändamål samt hantering av krypteringsnycklar.
- Inriktningen ska vara att krypteringen sker med en allmänt erkänd krypteringsmetod med tillräcklig nyckellängd.

Åtgärder behandlade uppgifter:

- Behandlade uppgifter som överförs via internet ska skyddas genom kryptering.
- Uppgifterna behöver dock inte skyddas genom kryptering om det med hänsyn till uppgifternas art och sammanhang är osannolikt att överföring utan kryptering kan leda till en säkerhets- eller Integritetsincident.
- Koder, lösenord och sammanställningar av uppgifter som rör en användare eller abonnent bör krypteras vid överföring via internet.

Åtgärder nätdata:

- Anslutningar för konfigurering och styrning av tillgångar via internet eller kommunikationsnät som även andra än tillhandahållaren har rådighet över ska skyddas genom kryptering.

Åtgärder brottsbekämpande ändamål:

- Loggar avseende åtkomst till uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (LEK) om elektronisk kommunikation ska skyddas genom kryptering under lagring och överföring.

Hantering av krypteringsnycklar

- Krypteringsnycklar ska hanteras genom dokumenterade rutiner, med begränsad åtkomst, regelbunden rotation och särskild hantering vid incidenter. Krypteringsnycklar ska hanteras på ett säkert sätt.

14.2.8 Utbildning och medvetenhet

Mål: Att personal som hanterar behandlade uppgifter, nätdata och uppgifter för brottsbekämpande ändamål är väl insatta i gällande krav och hantering.

Åtgärder:

- Genomför regelbunden utbildning av personal som hanterar behandlade uppgifter och uppgifter för brottsbekämpande ändamål ska regelbundet få utbildning och information om hur uppgifter ska hanteras och hur integritetsincidenter kan upptäckas och analyseras.
- Personal som behandlar trafikuppgifter och integritetsskydd enligt 9 kap. 31 och 32 §§ i lagen om elektronisk kommunikation ska upplysas om tystnadsplikten och, för det fall att verksamheten är i kommunal regi, den tystnadsplikt som gäller enligt 29 kap. offentlighets- och sekretesslagen (2009:400).

14.3 Leverantörshantering

Syfte: Säkerställa säkerheten i hela leveranskedjan genom att alla uppdragstagare, leverantörer och underleverantörer som tillhandahåller tjänster och produkter till Verksamhetsutövaren uppfyller fastställda säkerhetskrav och har robusta säkerhetsåtgärder på plats.

14.3.1 Dokumentation

Mål: Att alla uppdragstagare, leverantörer och underleverantörer är dokumenterade.

Åtgärder:

- Alla uppdragstagare, leverantörer och underleverantörer ska dokumenteras i ett *Leverantörsregister* enligt nedan:
  - namn, organisationsnummer och kontaktuppgifter
  - beskrivning av uppdraget.
- Dokumentationen ska hållas uppdaterad och varje version ska bevaras i fem år från det att den upprättats eller uppdaterats.

14.3.2 Leverantörsutvärdering

Mål: Att leverantörernas säkerhetskapacitet och efterlevnad av säkerhetsstandarder är utvärderade innan avtal ingås.

Åtgärder:

- Genomföra en grundlig säkerhetsutvärdering av alla potentiella leverantörer, inklusive en granskning av deras säkerhetsrutiner, certifieringar och tidigare incidenthistorik.
- Använda en standardiserad bedömningsmetod för att jämföra och ranka leverantörernas säkerhetsnivåer.
- Kräva att leverantörer tillhandahåller dokumentation som bekräftar deras efterlevnad av relevanta säkerhetsstandarder (t.ex. ISO/IEC 27001).

14.3.3 Avtalskrav och säkerhetsåtaganden

Mål: Att specifika säkerhetskrav och åtaganden är inkluderade i alla leverantörsavtal.

Åtgärder:

- Formulera och inkludera tydliga säkerhetskrav och åtaganden i alla leverantörsavtal, inklusive krav på regelbunden rapportering och granskning.
- Säkerställ att avtalen innehåller klausuler som kräver att leverantörerna omedelbart rapporterar säkerhetsincidenter som kan påverka organisationens verksamhet.
- Inkludera bestämmelser om konsekvenser och åtgärder vid bristande efterlevnad av säkerhetskraven.

Avtal med leverantörer som tillhandahåller kritiska tjänster eller utlokaliserade säkerhetstjänster ska innehålla krav på dokumenterad exit- och överlämningsplan för att säkerställa kontinuitet och säkerhet vid avtalsupphörande.

14.3.4 Kontinuerlig övervakning och revision

Mål: Att leverantörernas säkerhetsåtgärder övervakas och revideras regelbundet för att säkerställa fortlöpande efterlevnad.

Åtgärder:

- Genomföra regelbundna säkerhetsrevisioner av leverantörernas anläggningar och säkerhetsåtgärder.
- Implementera ett system för kontinuerlig övervakning av leverantörernas prestanda och säkerhetsstatus.
- Upprätta en *Kommunikationsplan leverantörer* för att säkerställa att relevant säkerhetsinformation delas med leverantörerna i rätt tid.

Leverantörer som bedöms som kritiska för drift eller säkerhet ska följas upp regelbundet under avtalstiden, minst vartannat år eller vid väsentliga förändringar i tjänst, teknik eller riskbild.

14.3.5 Incidenthantering med leverantörer

Mål: Att effektiva processer för hantering av säkerhetsincidenter i samarbete med leverantörer är etablerade och upprätthålls.

Åtgärder:

- Utveckla och dokumentera en incidenthanteringsplan som inkluderar leverantörer och beskriver roller, ansvar och kommunikationsvägar vid säkerhetsincidenter.
- Säkerställa att leverantörerna har egna incidenthanteringsplaner och att dessa är kompatibla med Verksamhetsutövarens planer.

15 Kontinuitetshantering

Syfte: Att säkerställa att kritiska verksamhetsfunktioner, system och tjänster förblir tillgängliga och fungerar som förväntat, även i händelse av avbrott eller störningar. Det handlar om att minimera risker och upprätthålla verksamheten utan större avbrott.

15.1 Kontinuitetshantering

Mål: Att säkerställa att verksamhetsutövaren har förmåga att upprätthålla och återställa prioriterade funktioner, system och tjänster vid störningar och avbrott.

Åtgärder:

- Ta fram en *Metod för kontinuitetshantering* baserat på ISO 22301.
- Löpande identifiera de verksamhetsdelar och resurser som är nödvändiga för att kunna upprätthålla verksamheten och begränsa konsekvenserna av säkerhetsincidenter i form av hot, störningar eller avbrott
- Analysera vilka konsekvenser som kan uppstå när dessa verksamhetsdelar och resurser helt eller delvis blir otillgängliga.
- Konsekvensanalysen ska dokumenteras.
- Utifrån konsekvensanalysen upprättasen en åtgärdslista som hanterar de åtgärder som bör vidtas för att begränsa de konsekvenser som analyserats.
- Utifrån åtgärdslistan och andra verksamhetsfaktorer, som till exempel strategiska beslut, resurser och verksamhetsplan skapa en *Åtgärdsplan kontinuitet*.
- Fastställa tider och kriterier för revidering.
- Fastställa när och på vilket sätt kontinuitetsplanerna ska övas (minst vartannat år) och utvärderas.

15.2 Katastrofhantering

Mål: Att minimera skador och att snabbt kunna återställa verksamheten vid akuta krissituationer som inte hanteras inom ramen för kontinuitetsplanen.

Åtgärder:

- Ta fram en *Katastrofplan* som steg för steg beskriver hur funktionen av nät, tjänster och informationsbehandlingssystem temporärt ska återställas för att minimera avbrott i tid och omfattning samt återställa förlust av information.
- Planen skall också innehålla dokumenterad överlämning till driftsfunktionen.

16 Extern kommunikation - information

Syfte: Säkerställa att berörda användare och myndigheter får tillgång till information om inträffade incidenter, samt konkreta och betydande hot om att en säkerhetsincident kan inträffa, så att de kan vidta lämpliga åtgärder inom sina respektive verksamheter.

16.1 Kommunikationsstrategi användare

Mål: Att information om säkerhetsincidenter når ut till berörda användare och att den lämnas på ett säkert sätt så att inte informationen i sig ger upphov till nya säkerhetsincidenter.

Åtgärder:

- Ta fram en *Rutin för incidentinformation till användare* som påverkas vid en incident eller som kan komma att påverkas vid ett konkret och betydande hot om att en säkerhetsincident kan inträffa samt de skydds- eller motåtgärder som Verksamhetsutövaren rekommenderar.
- Informationen bör, om det är möjligt och lämpligt, beskriva den risk som hotet innebär och vad konsekvenserna kan bli om användarna inte vidtar rekommenderade åtgärder.

16.2 Samarbete med myndigheter och operatörer

Informationsdelning

Mål: Att Verksamhetsutövaren delar information med nationella och europeiska myndigheter om cyberhot och incidenter.

Åtgärder:

- Dela relevant information med:
  - Post- och telestyrelsen (PTS)
  - Myndigheten för samhällsskydd och beredskap (MSB/CERT-SE)

Rapportering och samarbete

Mål: Att samarbete med myndigheter och andra operatörer för att hantera och bemöta säkerhetshot och incidenter är etablerat.

Åtgärder:

- **Incidentrapportering**: Verksamhetsutövaren ska omedelbart rapportera alla incidenter till PTS och MCF enligt gällande föreskrifter.
- **Informationsdelning**: Verksamhetsutövaren ska delta i informationsdelning om så efterfrågas.
- **Samordnade insatser**: Vid incidenter som har en bredare påverkan än på den egna verksamheten ska Verksamhetsutövaren samarbeta med relevanta internationella organ om så efterfrågas.

17 Utbildning och kompetensutveckling

Syfte: Säkerställa att styrelsemedlemmar och alla anställda har den kunskap och kompetens som krävs för att upprätthålla den roll som man har i Verksamhetsutövarens organisation.

17.1 Personalutbildning

Mål: Att personalutbildningen är strukturerad, har rätt innehåll samt regelbundet erbjuds alla anställda och uppdragstagare. Detta säkerställer att relevant kunskap och kompetens finns för den roll den anställde/uppdragstagaren har i Verksamhetsutövarens organisation.

Åtgärder:

Implementera följande utbildningar och övningar:

- **Styrelse- och ledningsutbildning:** Styrelsen och ledningen ska genomgå utbildning om riskhanteringsåtgärder och anställda ska erbjudas sådan utbildning.
- **Grundutbildning**: Alla nya anställda, eller vid byte arbetsuppgift, ska genomgå en grundutbildning i säkerhetspolicyer och rutiner snarast efter anställning/ förändring.
- **Årlig utbildning**: Alla anställda ska delta i årlig utbildning avseende senaste säkerhetspolicys för Verksamhetsutövarens organisation.
- **Specialiserade utbildningar**: Personal med specifika roller och ansvar inom säkerhetsområdet, eller som arbetar i eller har tillträde till kritiska anläggningar, ska få specialiserad utbildning relaterad till deras arbetsuppgifter.
- **Övningar**: Delta i regelbundna säkerhetsövningar för att säkerställa att personalen är förberedd på att hantera olika säkerhetsscenarier och incidenter effektivt.

17.2 Certifieringar

Mål: Att personalen erbjuds möjlighet att erhålla relevanta certifieringar för att säkerställa en hög kompetensnivå.

Åtgärder:

- Certifieringsprogram: Identifiera och rekommendera certifieringsprogram som är relevanta för Verksamhetsutövarens organisation.
- Uppföljning och uppdatering: Regelbundet följa upp personalens certifieringsstatus och uppmuntra till fortlöpande utbildning för att hålla certifieringarna aktuella.

17.3 Kompetensutveckling

Mål: Att en strukturerad kompetensutveckling bedrivs för att upprätthålla och förbättra personalens kompetens.

Åtgärder:

- Personliga utvecklingsplaner: Varje anställd ska ha en personlig utvecklingsplan som definierar mål och åtgärder för deras kompetensutveckling.

17.4 Utvärdering och förbättring

Mål: Att utbildnings- och kompetensutvecklingsprogrammen är effektiva och relevanta.

Åtgärder:

- Feedback och enkäter: Samla in feedback från deltagarna i utbildningsprogrammen och använda enkäter för att bedöma deras effektivitet.
- Prestandamätning: Mätning av personalens prestation och kompetens före och efter utbildning, till exempel genom övningar, för att identifiera förbättringsområden.
- Kontinuerlig förbättring: Använda resultaten från utvärderingarna för att kontinuerligt förbättra utbildningsmaterial och metoder.

18 Kvalitetskontroll - uppföljning

Syfte: Säkerställa att verksamhetsutövaren systematiskt följer upp, utvärderar och förbättrar arbetet med säkerhet, drift, kontinuitet och incidenthantering avseende telenät, teletjänster och tillhörande verksamhetssystem. Kvalitetskontroll och uppföljning ska ge ledning och styrelse underlag för styrning, prioritering och beslut samt säkerställa efterlevnad av gällande regelverk.

18.1 Driftsäkerhet

Exempel på parametrar för driftsäkerhet.

18.1.1 Tillförlitlighetsprestanda (Reliability performance)

Öka medeltiden mellan fel MTBF (Mean Time Between Failures) i timmar vilket är ett mått på hur länge en enhet fungerar innan den drabbas av ett fel.

Mål: Öka MTBF med 10% årligen.

18.1.2 Underhållsmässighet (Maintainability performance)

Minska medelreparationstiden MTTR (Mean Time To Repair) i timmar för att ge insikt i hur snabbt en enhet kan återställas efter ett fel.

Mål: Minska MTTR med 15% årligen.

18.1.3 Underhållstid (Maintenance support performance)

Minska medelväntetiden på underhåll MTV (Mean Waiting Time) i timmar för att fokusera på tiden som krävs för att utföra underhållsåtgärder.

Mål: Minska MWT med 20% årligen.

18.1.4 Nättillgänglighet

Öka den totala nättillgängligheten, uttryckt som en procentandel av den totala tiden (365 dygn) som en enhet är tillgänglig för användning.

Mål: Uppnå en tillgänglighet på 99,99%.

Uppföljning av dessa mått ska genomföras regelbundet och användas som underlag för förbättring av drift, underhåll och säkerhetsåtgärder.

18.2 CSL - specifika mål

18.2.1 Efterlevnad av Cybersäkerhetslagen:

Säkerställa efterlevnad av Cybersäkerhetslagen genom årlig revision.

Mål: Ha 100% efterlevnad vid varje granskning.

18.2.2 Riskbedömningar:

Utföra årliga riskbedömningar för att identifiera och hantera nya och befintliga risker.

Mål: Genomföra nya riskbedömningar om så behövs och revidera riskbedömningar årligen.

19.2.3 Incidenthantering:

Implementera och testa incidenthanteringsplaner för att säkerställa att alla incidenter hanteras effektivt och snabbt.

Mål: Minska den genomsnittliga tiden för incidenthantering med 20% årligen.

18.3 CSL - Fysisk säkerhet

18.3.1 Tillträdeskontroll:

Upprätthålla tillträdeskontrollsystem för alla Telenätets anläggningsdelar.

Mål: Säkerställa att 100% av Telenätets anläggningsdelar har uppdaterade och fungerande tillträdeskontrollsystem.

18.3.2 Övervakning:

I anläggningsdelar som har övervakningskameror så ska kontinuerlig kontroll av funktion genomföras.

Mål: Samtliga övervakningskameror ska ha full funktion.

18.3.3 Revision:

Genomföra årlig revision enligt RSA av Telenätet.

Mål: Åtgärda identifierade brister inom tre månader efter revision.

18.4 CSL - Logisk säkerhet

18.4.1 Nätverkssäkerhet:

Implementera nätverkssäkerhetsåtgärder exempelvis intrusion detection systems (IDS) och intrusion prevention systems (IPS).

Mål: Minska antalet nätverksintrång med 25% årligen.

18.4.2 Åtkomstkontroll:

Förbättra åtkomstkontroller genom implementering av multi-faktor autentisering (MFA) för alla system.

Mål: Ha MFA implementerat för 100% av alla system inom ett år.

18.4.3 Sårbarhetshantering:

Genomföra periodiska sårbarhetsskanningar, till exempel kvartalsvis, och åtgärda identifierade sårbarheter snarast.

Mål: Reducera antalet kritiska sårbarheter med 50% årligen.

18.5 Kontroller och revisioner

Mål: Att interna och externa revisioner av säkerheten genomförs regelbundet för att säkerställa att säkerhetsarbetet fungerar effektivt och i enlighet med lagar och förordningar.

Åtgärder:

Verksamhetsutövaren ska regelbundet genomföra kontroller och uppföljning av säkerhetsarbetet för att säkerställa att vidtagna säkerhetsåtgärder är ändamålsenliga, proportionerliga och effektiva i förhållande till verksamhetens riskbild.

Kontrollerna ska bidra till att:

- verifiera att fastställda processer, rutiner och säkerhetsåtgärder följs,
- identifiera brister eller behov av förbättringar i säkerhetsarbetet,
- utvärdera effektiviteten i genomförda säkerhetsåtgärder, samt
- säkerställa att verksamheten uppfyller krav enligt CSL, LEK och tillämpliga föreskrifter.

Kontroller och revisioner kan genomföras i form av exempelvis:

- intern uppföljning inom verksamheten,
- tekniska kontroller och tester,
- genomgång av incidenter och störningar,
- revision av processer och dokumentation.

Resultatet av kontroller och revisioner ska dokumenteras och vid behov leda till beslut om korrigerande eller förebyggande åtgärder.

19 Fredstida planering för totalförsvarets behov av elektronisk kommunikation

Syfte: Säkerställa att Verksamhetsutövarens arbete med kontinuitetsplanering för höjd beredskap och krig bedrivs långsiktigt, kontinuerligt och systematiskt.

19.1 Kontinuitetsplanering

Mål: Att förbereda organisationen så att den kan fortsätta fungera och stödja samhället även under mycket svåra förhållanden, som vid krig eller allvarliga kriser.

Åtgärder:

- Identifiera och dokumentera de verksamhetsdelar och resurser, inklusive roller, ansvar och beslutsvägar, som är nödvändiga för att konsekvenserna av omfattande störningar eller avbrott ska kunna begränsas vid höjd beredskap och krig. Analysera vilka konsekvenser som kan uppstå när dessa verksamhetsdelar och resurser helt eller delvis blir otillgängliga. Analysen ska omfatta en bedömning av när kontinuitetsplaner ska tillämpas.
  (En sådan verksamhetsdel och resurs som avses ovan kan till exempel utgöras av personella resurser som på grund av befattning, roll, funktion eller kunskap inom ett visst område är nödvändiga för att verksamheten ska fungera. Även en underleverantör av för tillhandahållaren helt nödvändig utrustning kan utgöra en sådan verksamhetsdel. En sådan verksamhetsdel kan även vara en central databas över användare som, om den slutar att fungera, omöjliggör användandet av tjänsten).
- Upprätta kontinuitetsplaner utifrån konsekvensanalysen ovan. Kontinuitetsplanerna ska åtminstone innehålla uppgifter om:

  1. de åtgärder som ska vidtas för att begränsa de konsekvenser som kan uppstå enligt konsekvensanalysen och för att återställa påverkade verksamhetsdelar eller resurser till normal funktionsförmåga,

  2. när och på vilket sätt kontinuitetsplanerna ska övas. Övning bör genomföras regelbundet och minst vartannat år.

  3. när och på vilket sätt kontinuitetsplanerna ska revideras.

  Tillhandahållaren ska utgå från etablerad standard på området vid framtagande av kontinuitetsplanerna.

Post- och telestyrelsen kan komma att informera tillhandahållare om:

1. vilka verksamhetsdelar och resurser som är kritiska för totalförsvarets behov av elektroniska kommunikationer vid höjd beredskap och i krig, och

2. vad kontinuitetsplanerna ska innehålla för att tillgodose totalförsvarets behov av elektroniska kommunikationer vid höjd beredskap och i krig.

När Post- och telestyrelsen förmedlar information enligt första stycket ska tillhandahållaren revidera sina kontinuitetsplaner i enlighet med informationen.

Tillhandahållaren ska ta fram planer för att vid höjd beredskap och i krig kunna ställa personal till förfogande för samverkan med Post- och telestyrelsen i den omfattning som krävs.
Tillhandahållaren ska planera för att upprätthålla samverkansfunktionen dygnet runt i 90 dagar.

(Tillhandahållaren bör i sina planer ha utpekade personella resurser tillgängliga för samverkan med Post- och telestyrelsen.

Tillhandahållarens planer bör också omfatta de tekniska lösningar som krävs för kommunikation och samverkan med Post- och telestyrelsen vid höjd beredskap och i krig).

Anm.
För kommunala och regionala verksamhetsutövare ska kontinuitetsplaneringen samordnas med krav enligt lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap (LEH).

19.2 Samverkan med PTS

Mål: Att ha etablerade effektiva kommunikationskanaler och samverkansmekanismer med PTS under extraordinära händelser, höjd beredskap och krig genom samverkan med NTSG och SISG.

Åtgärder:

- Använd framtagen plan för samverkan med PTS genom NTSG och SISG.