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. 1.3

TLP:CLEAR

STADSNÄTS FÖRENINGEN

Innehåll

1 Inledning och bakgrund 5
1.1 Inledning 5
1.1.1 Definitioner, dokumentförteckningar och standarder 5
1.2 Vad är cybersäkerhetslagen 5
1.3 Dokumentets tillämpning och omfattning 9
2 Syfte och Mål 12
2.1 Syftet med dokumentet 12
2.2 Målet för riktlinjerna 12
2.3 Övergripande mål för säkerhetsarbetet 13
3 Verksamhetsbeskrivning 14
4 Verksamhetsplan 17
5 Organisation och ansvar 19
5.1 Styrelsens och Ledningens ansvar 20
5.1.1 Övergripande krav 20
5.1.2 Organisering av stadsnätsverksamheten 21
5.1.3 Stadsnätsverksamheten bedrivs inom kommunal förvaltning 22
5.1.4 Stadsnätsverksamheten bedrivs i ett kommunalt bolag inom en koncern 23
5.1.5 Stadsnätsverksamheten bedrivs i ett gemensamt bolag eller kommunalförbund 23
5.1.6 Privat verksamhet 23
5.2 Funktionsområden 24
5.3 Roller och ansvarsområden 28
6 Nätarkitektur, Teletjänster och kapacitet 30
6.1 Telenät- och Teletjänster 30
6.2 Nät- och tjänsteutveckling 31

6.3 Kapacitetsplanering 32
7 Dokumentation 33
8 Drift 35
9 Underhåll 39
9.1 Förebyggande underhåll 39
9.2 Reservdelshantering 40
9.3 Uppdateringar av mjukvara 42
9.4 Akut underhåll 44
10 Anskaffning 45
10.1 Anskaffningsrutin 45
10.2 Anskaffningskontroll och dokumentation 45
10.3 Utbildning och medvetenhet 46
11 Förändringar 47
11.1 Förändringsprocesser 47
11.1.1 Särskilda åtgärder vid planerade förändringar (nytt avsnitt) 48
11.2 Testning av Förändringar 48
11.3 Godkännande av förändringar 48
11.4 Kommunikation och medvetenhet 49
11.5 Implementering och kontroll 49
11.6 Dokumentation 49
12 Incidenter 51
12.1 Incidenthantering 51
12.1.1 Incident 51
12.1.2 Integritetsincident 52
12.2 Incidentrapportering 53
12.2.1 Intern rapportering 53
12.2.2 Bedömning av betydande incident 53

12.2.3 Incidenter som alltid är betydande ... 56
12.2.4 Återkommande incidenter ... 56
12.2.5 Incidenter vid planerade förändringar ... 56
12.2.6 Rapportering av betydande incident ... 57
12.2.7 Incidenter hos leverantör, kommunikationsoperatör eller annan extern part ... 58
12.2.8 Integritetsincident ... 58
13 Riskanalys, risk- och åtgärdshantering ... 59
13.1 Övergripande arbetsmetod ... 59
13.2 Riskanalys ... 59
13.3 Risk-och åtgärdshantering ... 61
13.4 Kommunikation och rapportering ... 61
13.5 Efterlevnad och revision ... 62
14 Säkerhetshantering ... 63
14.1 Skydd av anläggningar ... 63
14.2 Skyddsåtgärder för information ... 65
14.3 Leverantörshantering ... 72
15 Kontinuitetshantering ... 77
15.1 Kontinuitetshantering ... 77
15.2 Kris och katastrofhantering ... 78
16 Extern kommunikation - information ... 79
16.1 Information till mottagare av tjänster ... 79
16.2 Samarbete med myndigheter och operatörer ... 79
17 Utbildning och kompetensutveckling ... 81
17.1 Ledningens och personalens utbildning ... 81
17.1.1 Styrelsens och ledningens utbildning ... 81
17.1.2 Övrig personalutbildning ... 81
17.2 Certifieringar ... 82

17.3 Kompetensutveckling 82
17.4 Utvärdering och förbättring 83
18 Kvalitetskontroll - uppföljning 84
18.1 Driftsäkerhet 84
18.2 Uppföljning av säkerhetsarbetet 85
18.3 Fysisk säkerhet 86
18.4 Logisk säkerhet 86
18.5 Egenkontroll och revision 87
18.6 Säkerhetsrevision vid tillsyn 88
19 Fredstida planering för totalförsvarets behov av elektronisk kommunikation 90
19.1 Kontinuitetsplanering 90
19.2 Samverkan med PTS 91

Revisionshistorik

Version	Datum	Vem	Ändring
1.3		JP, LB	Förtydligat och kompletterat den tidigare implementeringen av PTSFS 2026:1–3 avseende skydd och utlämnande av uppgifter samt fredstida totalförsvarsplanering. Omarbetat incidenthantering och incidentbedömning enligt PTSFS 2026:5 om vad som utgör en betydande incident inom telekomområdet. Kompletterat riktlinjerna med MCFFS 2026:1 om anmälan och identifiering, MCFFS 2026:8 om incidentrapportering och informationsskyldighet, MCFFS 2026:11 om säkerhetsåtgärder och ledningens utbildning samt MCFFS 2026:12 om säkerhetsrevision och säkerhetsskanning. Förtydligat föreskrifternas tillämpningsområden, klassning och ansvar samt kraven på riskhantering, förändringar, behörigheter, kryptering, leverantörer, utbildning, kontinuitet och uppföljning. Stärkt samordningen mellan huvuddokument och bilagor.

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 (2022:482) om elektronisk kommunikation (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).

Införandet av cybersäkerhetslagen har medfört ändringar i lagen om elektronisk kommunikation. Bestämmelser om säkerhetsåtgärder, säkerhetsrevision, incidentrapportering och informationsskyldighet finns nu i cybersäkerhetslagen med tillhörande reglering. Samtidigt kvarstår särskilda skyldigheter enligt lagen om elektronisk kommunikation, bland annat avseende behandling och skydd av uppgifter. Verksamhetsutövaren ska därför identifiera och tillämpa kraven i båda regelverken samordnat.

1.1.1 Definitioner, dokumentförteckningar och standarder

Definitioner, dokumentförteckningar och standarder som hanteras i detta dokument framgår av *Bilaga Definitioner, dokumentförteckningar 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
- allmänna elektroniska kommunikationsnät och allmänt tillgängliga 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

Cybersäkerhetslagen skiljer mellan väsentliga och viktiga verksamhetsutövare. Tillhandahållare av allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster som storleksmässigt motsvarar eller är större än ett medelstort företag är väsentliga enligt 1 kap. 9 § första stycket 3 cybersäkerhetslagen (2025:1506). Verksamhetsutövare som inte är väsentliga är viktiga enligt samma paragraf.

Klassningen av en juridisk person som är verksamhetsutövare ska beakta hela den juridiska personens verksamhet. Storleksbedömningen ska utgå från definitionerna av anknutet företag, medelstort företag och partnerföretag i 1 kap. 2 § punkterna 2, 13 och 18 cybersäkerhetslagen och de storleksberäkningsregler som definitionerna bygger på.

Om stadsnätsverksamheten bedrivs som en verksamhetsdel inom ett energibolag ska storleksbedömningen avse bolaget och inte begränsas till stadsnätsverksamhetens personal

och ekonomiska uppgifter. Är energibolaget att klassificera som en väsentlig verksamhetsutövare gäller klassificeringen alla verksamhetsdelar. Ett mindre stadsnät kan därför vara en verksamhetsutövare som ska klassas som väsentlig, även om stadsnätsverksamheten som sådan är liten.

Om stadsnätsverksamheten bedrivs i ett separat bolag ska det bolagets sektorsverksamhet bedömas separat, samtidigt som uppgifter gällande partnerföretag och anknutna företag ska beaktas vid storleksberäkningen. Klassningen av stadsnätsbolaget följer inte automatiskt av att ett ägarbolag bedriver energiverksamhet eller är väsentligt.

Bedömningen ska dokumentera juridisk person, berörda sektorsverksamheter, ägarförhållanden, storleksunderlag och rättslig grund för klassningen. Resultat från myndigheternas vägledande bedömningsverktyg ska kontrolleras mot dessa förutsättningar.

Undantaget för partnerföretag och anknutna företag i 3 kap. 1 § MCFFS 2026:1 gäller under vissa förutsättningar för verksamhetsutövare som omfattas av cybersäkerhetslagen med stöd av 1 kap. 4 § och endast uppfyller storlekskravet genom sin anknytning till andra företag. För undantaget krävs även att föreskriftens villkor om oberoende är uppfyllda. Undantaget innebär inte att en tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster undantas från lagen när verksamheten omfattas enligt 1 kap. 6 §.

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

Anmälan enligt cybersäkerhetslagen

Verksamhetsutövaren ska så snart det kan ske anmäla verksamheten till Nationellt cybersäkerhetscenter (NCSC) vid Försvarets radioanstalt (FRA), enligt myndighetens aktuella anvisningar. Anmälan enligt cybersäkerhetslagen hanteras separat från anmälan enligt lagen om elektronisk kommunikation.

- Anmälan ska innehålla:
  - verksamhetsutövarens namn,
  - adress, e-postadress, organisationsnummer och telefonnummer till verksamhetsutövaren eller dess svenska företrädare,
  - identifierare mot internet i form av IP-adresser och domännamn,
  - berörda sektorer och viktiga samhällsfunktioner,
  - verksamhetstyp,
  - uppgift om verksamheten är identifierad enligt 4 kap. MCFFS 2026:1, och
  - uppgift om verksamhetsutövaren är väsentlig eller viktig.
- Vid sektorsverksamhet i andra EU- eller EES-länder ska även kontaktuppgifter till dessa etableringsställen lämnas.
- En ansvarig funktion ska utses för anmälan och för att hålla uppgifterna aktuella. Ändrade förhållanden ska anmälas så snart det kan ske, dock senast 14 dagar efter förändringen.

Tillsyn och påföljder

För verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster är Post- och telestyrelsen (PTS) tillsynsmyndighet.

Vid bristande efterlevnad får tillsynsmyndigheten besluta om ingripanden enligt cybersäkerhetslagen, bland annat föreläggande, anmärkning och sanktionsavgift.

För en enskild väsentlig verksamhetsutövare får sanktionsavgiften uppgå till högst det högsta av 2 procent av den totala globala årsomsättningen närmast föregående räkenskapsår eller ett belopp i kronor motsvarande 10 miljoner euro.

För en enskild viktig verksamhetsutövare är motsvarande högsta nivå det högsta av 1,4 procent av årsomsättningen eller ett belopp i kronor motsvarande 7 miljoner euro. För en offentlig verksamhetsutövare är den högsta sanktionsavgiften 10 miljoner kronor.

Vid tillämpning av bestämmelserna om sanktionsavgifter ska verksamhetsutövarens rättsliga organisationsform beaktas. En kommun eller ett kommunalförbund är en offentlig verksamhetsutövare enligt cybersäkerhetslagen. Ett kommunalt aktiebolag är däremot en enskild verksamhetsutövare; kommunalt ägande innebär inte i sig att bolaget omfattas av reglerna för offentliga verksamhetsutövare. Sanktionsavgiften bestäms enligt cybersäkerhetslagens bestämmelser 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 (SFS 2025;1506) och cybersäkerhetsförordningen (SFS 2025:1507)
- lagen om elektronisk kommunikation (SFS 2022:482) och förordning om elektronisk kommunikation (SFS 2022:511)
- PTS föreskrifter:
    - PTSFS 2026:1–3 och 2026:5, avseende skydd och utlämnande av uppgifter, totalförsvarsplanering samt kriterier för betydande incidenter,
- MCF föreskrifter
    - MCFFS 2026:1, 2026:8, 2026:11 och 2026:12, avseende anmälan, incidentrapportering, säkerhetsåtgärder och ledningens utbildning samt säkerhetsrevision och säkerhetsskanning vid tillsyn.

Föreskrifterna tillämpas utifrån verksamhetsutövarens sektorsverksamhet och respektive föreskrifts tillämpningsområde. Särskilda avgränsningar för digital infrastruktur beskrivs i berörda avsnitt. Fullständiga författningshänvisningar finns i bilagan *Definitioner, dokument och standarder*.

Riktlinjerna stödjer även genomförandet av de interna säkerhetskrav som styrelsen och ledningen fastställer.

För verksamhetsutövare som uteslutande bedriver sektorsverksamhet inom digital infrastruktur gäller endast kraven på ledningens utbildning i 2 kap. 1 § MCFFS 2026:11. Övriga säkerhetsåtgärder i dessa riktlinjer ska grundas på cybersäkerhetslagen, tillämpliga sektorsregler och verksamhetens egna riskbaserade beslut; de ska inte generellt beskrivas som bindande krav enligt MCFFS 2026:11 för en sådan verksamhetsutövare.

Om samma juridiska person även bedriver sektorsverksamhet inom exempelvis energi ska tillämpningsområdet för MCFFS 2026:11 och övriga föreskrifter bedömas för

verksamhetsutövarens samlade sektorsverksamhet. Undantaget för verksamhetsutövare som uteslutande bedriver verksamhet inom de uppräknade sektorerna kan då inte förutsättas vara tillämpligt. Ett separat telekombolag blir däremot inte energiverksamhetsutövare enbart genom att ingå i en energikoncern.

Om verksamhetsutövaren även tillhandahåller exempelvis DNS-, moln- eller datacentraltjänster ska tillämpligheten av genomförandeförordning (EU) 2024/2690 bedömas. Bedömningen ska omfatta både säkerhetsåtgärder och kriterier för betydande incidenter.

Tillämpliga föreskrifter och deras ikraftträdande framgår av bilagan Definitioner, dokument och standarder. Ansvarig funktion ska följa regelutvecklingen och säkerställa att riktlinjerna och berörda bilagor uppdateras när kraven förändras.

Verksamheten är i detta sammanhang både verksamhetsutövare enligt cybersäkerhetslagen och tillhandahållare av allmänna elektroniska kommunikationsnät och/eller allmänt tillgängliga 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.

Dokumentet innehåller både beskrivningar av bindande krav och rekommenderade arbetssätt. Bindande krav gäller enligt respektive regelverks tillämpningsområde. Rekommendationer, exempel på tekniska lösningar och föreslagna ambitionsnivåer ska anpassas till verksamhetens risker och förutsättningar. När verksamhetsutövaren antar sådana arbetssätt som interna krav ska detta framgå av verksamhetens styrande dokument.

Riktlinjerna ska tillämpas tillsammans med bilagan Definitioner, dokument och standarder samt tillhörande processbilagor. Huvuddokumentet anger säkerhetsarbetets inriktning, omfattning, ansvar och uppföljning. Processbilagorna beskriver genomförandet. Verksamhetsutövaren ska anpassa och fastställa de verksamhetsspecifika planer, rutiner och anvisningar som behövs samt säkerställa att dokumenten används samordnat.

Riktlinjernas omfattning och huvudsakliga tillämpningsområden illustreras i nedanstående figur.

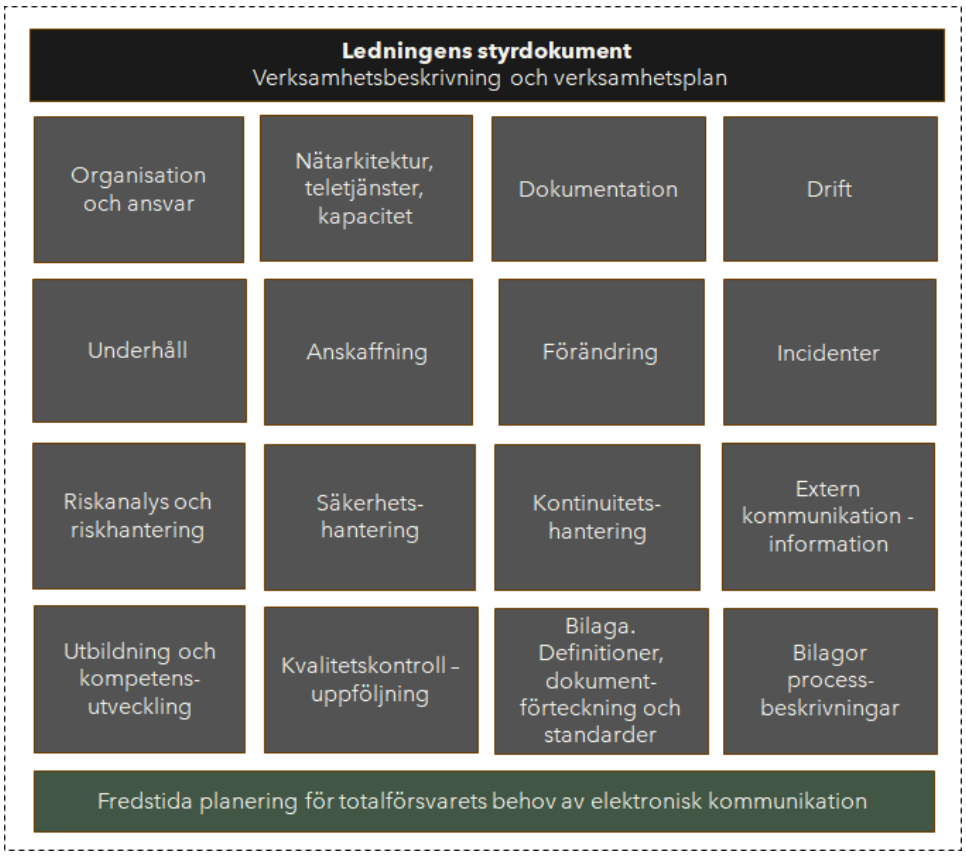


Bild Riktlinjernas omfattning

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 beskriver utbildning och kompetensutveckling
- Kapitel 18 beskriver kvalitetskontroll, uppföljning, egenkontroll och beredskap för tillsyn.
- Kapitel 19 beskriver den fredstida planeringen för totalförsvarets behov av elektroniska kommunikationer.

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.
- utföra dokumenterat revisionsarbete,
- förmåga att vid tillsyn visa hur säkerhetsåtgärder är beslutade, genomförda, tillämpade, kontrollerade och förbättrade.

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 verksamhetsutövarens roll som nätägare, kommunikationsoperatör och/eller tjänsteleverantör samt vilka elektroniska kommunikationsnät och kommunikationstjänster som tillhandahålls inom respektive roll.
- 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.
- Identifiering av kundgrupper, användare, anslutningar, samhällsfunktioner och 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.
- Beskrivning av principer för hur verksamheten identifierar omfattningen av driftstörningar och incidenter i nät och tjänster, inklusive påverkan på förbindelser, användare, anslutningar, kapacitet och geografiska områden.

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.
- Beskriv vilka nät, tjänsteplattformar, verksamhetssystem och gemensamma stödfunktioner som ingår i säkerhetsarbetet. Omfattningen ska även beakta externa och koncerngemensamma funktioner som verksamheten är beroende av. För kritiska funktioner och tillgångar ska ansvar, beroenden och gränssnitt mot andra aktörer framgå.

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.
- Beskrivning av vilka delar av verksamheten respektive regelverk omfattar, vilka särskilda skyldigheter som är tillämpliga samt vilka funktioner som ansvarar för att regelverksbedömningen hålls aktuell.

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.
- **Genomförande och verifiering:** För varje planerad åtgärd ska ansvarig funktion, planerad sluttid, resursbehov och metod för kontroll av åtgärdens genomförande och effekt anges.
- **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)

Reglerar bland annat anmälan av verksamhet, skydd och behandling av uppgifter, integritetsincidenter samt lagring och utlämnande av uppgifter för brottsbekämpande ändamål. Tillämpliga skyldigheter enligt LEK och tillhörande föreskrifter ska hanteras parallellt och samordnat med kraven enligt cybersäkerhetslagen.

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

MCF kompletterande föreskrifter avseende cybersäkerhetslagen
Preciserar tillämpliga krav på anmälan, incidentrapportering och ledningens utbildning samt reglerar säkerhetsrevision och säkerhetsskanning vid tillsyn. Föreskrifterna ska tillämpas med beaktande av respektive föreskrifts tillämpningsområde och särskilda avgränsningar för digital infrastruktur.

Lagen om extraordinära händelser i fredstid och höjd beredskap (LEH)

Reglerar kommuners och regioners beredskapsplanering. För kommunala bolag ska samordningen med denna planering bedömas utifrån tillämpliga ägardirektiv, avtal och verksamhetens egna skyldigheter. Se kapitel 19.

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 genom utbildning ha sådan kunskap och kompetens att den kan fastställa mål och inriktning för cybersäkerheten, utifrån identifierade risker bedöma behovet av lämpliga och proportionerliga säkerhetsåtgärder samt övervaka genomförandet av åtgärderna.

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

Utbildningsbehovet ska omprövas regelbundet och genomförda utbildningsinsatser dokumenteras. Närmare riktlinjer framgår av kapitel 17.

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

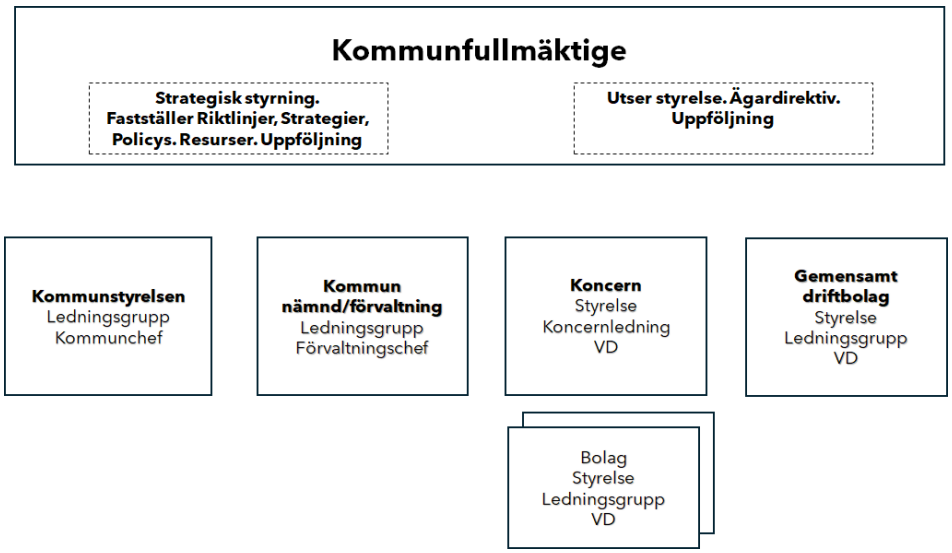


Bild. Organisationsalternativ kommunal verksamhet

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 kan samordna koncernens säkerhetsarbete och fastställa gemensamma principer inom ramen för ägarstyrningen. Varje bolag som är verksamhetsutövare behåller dock sitt eget ansvar för efterlevnaden av cybersäkerhetslagen och övriga tillämpliga krav. Koncerngemensam styrning ersätter inte stadsnätsbolagets styrelses och verkställande lednings ansvar.
- 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.
- I ett gemensamt aktiebolag ansvarar bolagsstyrelsen för bolagets organisation, säkerhetsarbete och interna kontroll. Den verkställande ledningen ansvarar för genomförandet.
- I ett kommunalförbund ska motsvarande ansvar fördelas mellan beslutande organ och verkställande ledning enligt förbundets organisationsform, förbundsordning och övriga styrande dokument. Ansvar, mandat och rapporteringsvägar för cybersäkerhetsarbetet ska dokumenteras.

5.1.6 Privat verksamhet

Formell verksamhetsutövare är den fysiska eller juridiska person som bedriver den verksamhet som omfattas av cybersäkerhetslagen.

Ansvar och befogenheter ska beskrivas utifrån verksamhetens organisationsform. I ett aktiebolag ansvarar styrelsen för bolagets organisation och interna kontroll, medan verkställande direktören ansvarar för den löpande förvaltningen. Arbetsuppgifter kan fördelas inom organisationen eller utföras av externa parter, men verksamhetsutövarens ansvar för efterlevnaden kvarstår.

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 8-12.

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)*
- Identifiera och dokumentera ansvar och mandat för bedömning av incidenters omfattning och rapporteringsskyldighet, beslut om extern incidentrapportering samt kontakt med NCSC, PTS och andra berörda myndigheter.
- Säkerställa att ansvariga roller och ersättare kan initiera och genomföra incidentrapportering inom föreskrivna tidsfrister även utanför ordinarie arbetstid. Mandat, kontaktvägar och tillgång till rapporteringsunderlag ska vara dokumenterade.

  ***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 5.2,

- **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 av nätarkitektur, anläggningstillgångar, informationsbehandlingstillgångar, förbindelser och tillhandahållna tjänster. Beskrivningen ska dokumenteras i verksamhetsbeskrivningen eller i tillhörande teknisk dokumentation.
- Dokumentera tillgångar i enlighet med kap 7 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 (PTSFS 2022:11) 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 behovet av reservkraft och uthållighet vid bortfall av ordinarie elförsörjning är identifierat, dimensionerat och dokumenterat.

Åtgärder:

- Identifiera behovet av reservkraft utifrån riskanalys, kritiska funktioner och beroenden. Bedöm erforderlig effekt, drifttid, omkopplingsförmåga, bränsleförsörjning, tillgång till mobil reservkraft samt behov av redundans i strömförsörjningen.
- Upprätta och underhåll en *Åtgärdsplan för reservkraft till kritiska tillgångar*. Planen ska omfatta prioritering, dimensionering, anslutning, underhåll, provning och ansvar.

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 uppdragstagare 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.

Dokumentation enligt 4 kap. 1 § PTSFS 2026:1 ska hållas aktuell och bevaras i fem år från upprättandet. Ändringar av de föreskrivna uppgifterna om uppdragstagare, informationsbehandlingstillgångar och förbindelser ska kunna spåras i fem år.

För övrig dokumentation ska bevarandetid fastställas utifrån tillämpliga krav samt behov för uppföljning, incidentutredning och tillsyn.

Spårbarhet och uppföljning

Dokumentationen ska visa vilka krav och identifierade risker som ligger till grund för säkerhetsåtgärderna. Det ska framgå vilka åtgärder som har beslutats och genomförts, vem som ansvarar för dem och hur deras funktion har kontrollerats. Identifierade brister och åtgärder för att rätta till eller förebygga dem ska dokumenteras och följas upp.

För väsentliga säkerhetsåtgärder ska det finnas tillräckligt underlag för att verifiera både hur åtgärden är utformad och hur den faktiskt tillämpas i verksamheten.

Underlag för incidentbedömning

Dokumentationen av nät, tjänster, förbindelser, kunder, användare, anslutningar och andra relevanta tillgångar ska vara utformad så att verksamhetsutövaren vid en incident skyndsamt kan ta fram de uppgifter som krävs för att bedöma incidentens omfattning och konsekvenser enligt kapitel 12.

Dokumentationen ska, där det är relevant för verksamheten, ge underlag för att fastställa eller uppskatta:

· antal påverkade slutanvändare, användare eller aktiva anslutningar,
· antal påverkade uthyrda passiva fiberförbindelser eller svartfiberförbindelser,
· berört geografiskt område,
· påverkan på nätets eller tjänstens kapacitet, och
· beroenden till kunder eller organisationer som tillhandahåller viktiga samhällsfunktioner.

Det ska framgå vilka informationskällor som används för incidentbedömningen, vem som ansvarar för uppgifterna och hur underlaget kan tas fram vid bortfall av ordinarie verksamhetssystem. Uppskattningar och antaganden ska kunna särskiljas från verifierade uppgifter.

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 eskaleringsåtgärder är tydligt reglerade.
- Säkerställa tillgång till teknisk kompetens och incidenthanteringsförmåga i den omfattning och med de inställelse- och svarstider som verksamhetens risker, tjänsteåtaganden och rapporteringsskyldigheter kräver. Förmågan kan upprätthållas genom ordinarie bemanning, beredskap eller avtalad extern funktion. Ansvar, tillgänglighet och eskaleringsvägar ska vara dokumenterade.
- 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.
- Säkerställa att driftövervakning och incidenthantering, där det är tekniskt möjligt och relevant, kan ge underlag för att fastställa eller uppskatta incidentens starttid, varaktighet, antal påverkade användare eller aktiva anslutningar, kapacitetsbortfall och geografiska omfattning.
- Säkerställa att driftinformation kan sammanställas och göras tillgänglig för den funktion som ansvarar för bedömning och rapportering av incidenter enligt kapitel 12.

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
- Säkerställa tillgång till teknisk kompetens och incidenthanteringsförmåga i den omfattning och med de inställelse- och svarstider som verksamhetens risker, tjänsteåtaganden och rapporteringsskyldigheter kräver. Förmågan kan upprätthållas genom ordinarie bemanning, beredskap eller avtalad extern funktion. Ansvar, tillgänglighet och eskaleringsvägar ska vara dokumenterade.
- 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.

- Säkerställa att verksamhetssystem som används för nätövervakning, kund- och abonnemangsadministration, dokumentation och rapportering kan ge erforderligt underlag för bedömning av incidenters omfattning när sådan information behandlas i systemen.

9 Underhåll

Underhållskraven omfattar telenät, teletjänster och verksamhetssystem samt tillhörande utrustning, programvara, databaser och integrationer.

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:

- Underhållsplanerna ska beskriva riskbedömning inför underhåll, verifiering efter genomförandet samt hantering av oförutsedda problem. Driftstörningar och säkerhetsincidenter ska hanteras enligt kapitel 12 och vid behov samordnas med återställnings- och kontinuitetsplaneringen.

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 säkerhetsuppdateringar och andra nödvändiga uppdateringar genomförs inom tidsramar som är anpassade till identifierade risker och systemens betydelse.

Åtgärder:

- Fastställ tidsramar för bedömning, testning och införande av uppdateringar utifrån sårbarhetens allvar, exponering, eventuell aktiv exploatering och konsekvenser för verksamheten.
- Information från leverantörer ska skyndsamt bedömas och leda till beslut om uppdatering eller andra skyddsåtgärder. Kritiska säkerhetsrisker får inte lämnas obehandlade i väntan på ordinarie underhållstillfälle.
- När en uppdatering inte kan införas inom beslutad tid ska skälen, tillfälliga skyddsåtgärder, ansvarig och ny tidpunkt dokumenteras.

9.3.3 Testning av Uppdateringar

Mål: Att uppdateringar före införande verifieras i en omfattning som är anpassad till deras risk och möjliga påverkan. Brådskande säkerhetsuppdateringar ska hanteras genom fastställd rutin för akuta förändringar.

Åtgärder:

- Säkerställ tillgång till en lämplig testmiljö eller annan kontrollerad testmetod för att verifiera uppdateringens funktion och säkerhet enligt kapitel 11.
- 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 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 Stadsnätsföreningens *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 en strukturerad och riskbaserad anskaffning av utrustning, programvara, system och tjänster samt anlitande av uppdragstagare för telenät, teletjänster och verksamhetssystem.

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.

  Bedömningens omfattning och detaljeringsgrad ska anpassas till anskaffningens risker och betydelse för verksamheten. Förenklad bedömning kan användas när det är motiverat, utan att särskilda krav på riskanalys enligt tillämpliga föreskrifter åsidosätts. Anskaffningar som berör kritiska funktioner, känsliga uppgifter eller betydande leverantörsberoenden ska omfattas av fördjupad bedömning enligt avsnitt 10.2.

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 förändringar i telenät, teletjänster och verksamhetssystem planeras, riskbedöms, godkänns, testas och följs upp för att begränsa 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 och tillämpa en *Process för förändring i telenät, teletjänster och verksamhetssystem*. Processen ska omfatta normala förändringar, standardförändringar och akuta förändringar, med anpassade krav på riskbedömning, tester, godkännande och återställning.
- För akuta förändringar ska det finnas ett särskilt förfarande inom förändringsprocessen för anpassad riskbedömning, testning och godkännande. Processen ska ange vilka kontroller som ska genomföras före införandet, hur återställningsförmågan säkerställs och hur kompletterande verifiering och uppföljning genomförs efteråt. Avsteg och beslut ska dokumenteras. Anpassningen får inte innebära avsteg från bindande krav.
- Komplettera förändringsprocessen med erforderliga rutiner och anvisningar.
- Genomför och dokumentera riskanalys inför planerade förändringar. Analysera riskerna för integritetsincidenter och, när verksamheten är lagringsskyldig, brottsdatalagringsincidenter. Identifiera nödvändiga säkerhetsåtgärder.
- Riskbedömningen inför en förändring ska identifiera och dokumentera förutsebara konsekvenser för telenät, teletjänster, verksamhetssystem, användare och berörda samhällsfunktioner.
- Riskanalysen inför planerade förändringar ska ge underlag för att bedöma om inträffade negativa konsekvenser var förutsedda eller oförutsedda enligt kapitel 12. Dokumentationens omfattning ska anpassas till förändringens risk och betydelse.
- Säkerställ att förändringar klassificeras utifrån omfattning, risk, betydelse och påverkan på telenätets, teletjänsternas och verksamhetssystemens funktion, och att hanteringen inom förändringsprocessen anpassas därefter.
- Genomförda säkerhetsåtgärder ska verifieras genom relevanta kontroller och tester. Penetrationstest ska övervägas när förändringens art, exponering och

riskbild motiverar det. Tester ska planeras och genomföras så att risken för driftpåverkan begränsas.

11.1.1 Särskilda åtgärder vid planerade förändringar (nytt avsnitt)

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 de säkerhetsåtgärder som följer av riskbedömningen, 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.

11.2 Testning av Förändringar

Mål: Säkerställa att förändringar testas och verifieras i den omfattning som krävs utifrån riskanalys och tillämpliga krav.

Åtgärder:

- Säkerställ tillgång till en lämplig testmiljö eller annan kontrollerad testmetod som gör det möjligt att bedöma förändringens påverkan.
- 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.

Vid förändringar som berör utlämnande av uppgifter till brottsbekämpande myndigheter ska testerna omfatta förmågan att uppfylla tillämpliga tidsfrister, standarder och formatkrav.

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.
- Teknisk behörighet att genomföra en förändring innebär inte rätt att genomföra den utan det godkännande som krävs enligt förändringsprocessen.



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.
- Övervaka genomförandet och ha beredskap att avbryta förändringen, återgå till tidigare konfiguration eller återställa funktion och uppgifter enligt fastställd plan.
- Säkerställa att genomförda förändringar följs upp i syfte att verifiera att avsedd funktion och säkerhetsnivå har uppnåtts samt att inga oönskade effekter har uppstått.
- Bedöm om förändringen påverkar kontinuitetsanalyser eller planer för höjd beredskap och krig och uppdatera dem vid behov enligt kapitel 19.

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.
- Dokumentera identifierade och förutsebara drift- och säkerhetskonsekvenser samt de förutsättningar och antaganden som låg till grund för beslutet att genomföra förändringen.



- Uppdatera dokumentationen över berörda informationsbehandlingstillgångar, förbindelser och uppdragstagare. För uppgifter som omfattas av PTSFS 2026:1, 4 kap. 1 §, ska dokumentation och ändringsspårbarhet bevaras enligt föreskriftens femårskrav.

12 Incidenter

Syfte: Säkerställa att incidenter och integritetsincidenter identifieras, bedöms, hanteras, dokumenteras och rapporteras internt, till berörda parter och till relevanta myndigheter på ett strukturerat sätt för att begränsa påverkan och förbättra säkerheten.

För ett stadsnät kan verksamhetsutövaren vara nätägare, kommunikationsoperatör eller bedriva båda funktionerna. Vilka kriterier i PTSFS 2026:5 som ska tillämpas beror därför på vilka elektroniska kommunikationsnät och kommunikationstjänster som den aktuella juridiska personen faktiskt tillhandahåller.

Om verksamhetsutövaren både äger ett passivt fibernät och tillhandahåller elektroniska kommunikationsnät eller kommunikationstjänster i rollen som kommunikationsoperatör ska incidenten bedömas mot samtliga kriterier som är relevanta för respektive del av verksamheten.

12.1 Incidenthantering

12.1.1 Incident

Mål: Att processer och rutiner för identifiering, bedömning, hantering och dokumentation av incidenter är framtagna och implementerade.

Åtgärder:

- **Identifiering:** Verksamhetsutövaren ska ha en *Process för incidenthantering* baserad på etablerade standarder och tillämpliga regelverk. Processen ska säkerställa att incidenter kan identifieras genom bland annat övervakning, larm, felanmälningar samt information från kunder, leverantörer, andra operatörer och myndigheter.
- **Initial bedömning:** När en incident identifierats ska verksamhetsutövaren bedöma incidentens typ, omfattning, berörda nät, tjänster, informationssystem och uppgifter samt faktisk och potentiell påverkan.
- **Bedömning av betydande incident:** Verksamhetsutövaren ska utan onödigt dröjsmål bedöma om incidenten utgör en betydande incident enligt cybersäkerhetslagen och PTSFS 2026:5, så att tillämpliga tidsfrister för incidentrapportering kan uppfyllas.
- **Hantering:** Processen ska medge isolering eller begränsning av påverkat system eller nät, åtgärdsplanering, återställning och andra åtgärder som krävs för att begränsa incidentens påverkan och konsekvenser. Processen ska också medge teknisk och organisatorisk eskalering vid allvarliga incidenter.
- **Dokumentation:** Incidenten och bedömningen av dess påverkan ska dokumenteras så att händelseförlopp, beslut, vidtagna åtgärder och grunden för bedömningen av rapporteringsskyldigheten är spårbara.
- **Analys:** Analys ska genomföras i en omfattning som är proportionerlig mot incidentens allvar och konsekvenser. Analysen ska ge underlag för att identifiera orsaker, påverkan, brister och behov av förbättringsåtgärder.

- **Problemhantering:** Om det finns en okänd eller återkommande underliggande orsak till en eller flera incidenter som lett till störning i telenät eller teletjänster ska verksamhetsutövaren ha en *Process för problemhantering*.
- **Rapportering:** Det ska finnas rutiner för intern och extern incidentrapportering.
- **Löpande uppföljning:** Processer och rutiner för incidenthantering ska löpande utvärderas och förbättras baserat på erfarenheter och lärdomar från inträffade incidenter.
- **Tillgänglighet:** Det ska vara fastställt vilka roller som ska ha tillgång till incidentdokumentation och rapporter.

Vid bedömningen ska verksamhetsutövaren använda den information som finns tillgänglig eller rimligen kan inhämtas. Om incidentens omfattning inte säkert kan fastställas ska en rimlig uppskattning göras. Bedömningen och dess underlag ska dokumenteras för att säkerställa spårbarhet.

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.

12.1.2 Integritetsincident

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

Åtgärder för integritetsincidenter:

- **Identifiering:** Verksamhetsutövaren ska ha en *Process för integritetsincidenter* baserad på etablerade standarder och tillämpliga regelverk.
- **Hantering:** Processen ska medge initial bedömning av incidentens typ, isolering av påverkat system, åtgärdsplanering och genomförande.
- **Dokumentation:** Alla integritetsincidenter ska förtecknas för att säkerställa spårbarhet och underlätta framtida analyser. Förteckningen ska minst 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:** Genomför en analys och ta fram en rapport i den omfattning som krävs för att bedöma orsaker, påverkan och konsekvenser.
- **Rapportering:** Det ska finnas en rutin för rapportering av integritetsincidenter.
- **Löpande uppföljning:** Processen och rutinerna ska löpande utvärderas och förbättras baserat på erfarenheter och lärdomar från tidigare incidenter.
- **Tillgänglighet:** Det ska vara fastställt vilka roller som ska ha tillgång till dokument och rapporter.



Processen ska även omfatta brottsdatalagringsincidenter när verksamhetsutövaren lagrar uppgifter för brottsbekämpande ändamål. Sådana incidenter ska rapporteras internt och hanteras skyndsamt. Erfarenheterna ska användas i riskanalyser och förebyggande arbete.

Intern rapportering ska ske enligt 12.2.1. Eventuell extern rapporteringsskyldighet ska bedömas enligt 12.2.2–12.2.6 och 12.2.8.

12.2 Incidentrapportering

12.2.1 Intern rapportering

Mål: Att incidenter och integritetsincidenter rapporteras internt så att de kan bedömas, hanteras och vid behov rapporteras externt inom föreskrivna tidsfrister.

Åtgärder:

- Incidenter ska rapporteras till incidentansvarig eller annan utpekad funktion enligt *Rutin för intern incidentrapportering*.
- Intern rapportering ska ske så skyndsamt att verksamhetsutövaren kan bedöma om incidenten är betydande och uppfylla tillämpliga tidsfrister för extern rapportering.
- Incidentrapporteringen ska dokumenteras.
- Roller och kontaktvägar för eskalering ska vara dokumenterade och kända.
- Det ska vara fastställt vilka som ska ges tillgång till incidentdokumentation och rapporter.

Vid en brottsdatalagringsincident ska även eventuell extern rapporteringsskyldighet bedömas enligt 12.2.2–12.2.6 och 12.2.8.

12.2.2 Bedömning av betydande incident

Mål: Att verksamhetsutövaren på ett enhetligt och dokumenterat sätt kan avgöra om en incident utgör en betydande incident enligt cybersäkerhetslagen och PTSFS 2026:5.

Åtgärder:

Bedömningen ska utgå från incidentens samlade faktiska och potentiella påverkan. Samtliga kriterier i PTSFS 2026:5 som är relevanta för de nät och tjänster som verksamhetsutövaren tillhandahåller ska beaktas. Om minst ett tillämpligt kriterium är uppfyllt ska incidenten bedömas som betydande.

Ett betydande cyberhot, en betydande sårbarhet eller en annan upptäckt risk eller händelse ska bedömas som en betydande incident när den sannolikt kan orsaka, bidra till eller möjliggöra sådan påverkan eller sådana konsekvenser som anges i PTSFS 2026:5, enligt 3 kap. 2 §. Bedömning och rapportering får inte invänta ett faktiskt avbrott eller en realiserad skada när dessa förutsättningar redan är uppfyllda. Vid bedömning av en betydande sårbarhet bör särskilt beaktas om den har utnyttjats eller kan utnyttjas under de förhållanden som råder hos verksamhetsutövaren.

Undergrävd tillgänglighet (4 kap. 1 § punkt 1)
En incident som har undergrävt tillgängligheten till nät, tjänster eller uppgifter ska bedömas mot följande tröskelvärden. Tidsgränsen i en rad ska vara uppfylld tillsammans med minst ett av radens omfattningskriterier: antal berörda användare eller anslutningar, kapacitetsbortfall eller sammanhängande berört område.

Incidentens varaktighet	**Användare/anslutningar**	**Kapacitetsbortfall**	**Sammanhängande område**
minst 1 timme	minst 150 000	minst 50 %	minst 15 000 km²
minst 2 timmar	minst 30 000	minst 30 %	minst 5 000 km²
minst 6 timmar	minst 5 000	minst 20 %	minst 2 500 km²
minst 24 timmar	minst 2 000	minst 10 %	minst 1 000 km²

Om incidenten avser undergrävd tillgänglighet till uppgifter som under normala förhållanden görs tillgängliga för slutanvändare eller användare ska omfattningen bedömas utifrån incidentens varaktighet och antalet berörda slutanvändare eller användare.

Kapacitetsbortfall och geografisk omfattning ska i sådana fall inte användas som bedömningskriterier.

Med användare/anslutningar avses slutanvändare, användare eller aktiva anslutningar enligt föreskriftens kriterier. För en kommunikationsoperatör ska bedömningen göras utifrån den påverkan incidenten har på de elektroniska kommunikationsnät och kommunikationstjänster som verksamhetsutövaren tillhandahåller.

Kapacitetsbortfall ska bedömas i jämförelse med normala driftsförhållanden enligt 2 kap. 1 § 5 PTSFS 2026:5. Omfattningen ska anges som andelen reducerad kapacitet av verksamhetsutövarens totala kapacitet, andelen berörda aktiva anslutningar eller användare av verksamhetsutövarens totala antal samt andelen berörda slutanvändare av verksamhetsutövarens totala antal. För användare och anslutningar avses de som på grund av incidenten inte kan nyttja nätet eller tjänsten på samma sätt som vid normala driftsförhållanden. Beräkningsunderlag och uppskattningar ska dokumenteras i incidentbedömningen.

Passiva fibernät och svartfibernät (4 kap. 1 § punkt 2)
En incident i ett passivt fibernät eller svartfibernät ska bedömas som betydande om tillgängligheten har undergrävts till minst 400 uthyrda passiva fiberförbindelser eller svartfiberförbindelser. Det är ägaren av det passiva nätet som ska identifiera om incidenten är betydande enligt detta kriterium.

Om verksamhetsutövaren både äger ett passivt fibernät och är kommunikationsoperatör ska incidenten bedömas mot samtliga kriterier som är relevanta för de nät och tjänster som verksamhetsutövaren tillhandahåller.

Landsbygdskommun (4 kap. 1 § punkt 3)
En incident ska bedömas som betydande när den har undergrävt tillgängligheten till nät eller tjänster i en landsbygdskommun så att nätet eller tjänsten i praktiken varit obrukbar under

minst 48 timmar för minst 100 slutanvändare, användare eller aktiva anslutningar. Begreppet landsbygdskommun ska tillämpas enligt definitionen i 2 kap. 1 § 6 PTSFS 2026:5.

Gränsöverskridande incident (4 kap. 1 § punkt 4)
En incident ska bedömas som betydande om den är gränsöverskridande mellan Sverige och minst ett annat land, har pågått i minst sex timmar och undergrävt tillgänglighet, riktighet, autenticitet eller konfidentialitet för minst 5 000 slutanvändare.

Riktighet, autenticitet och konfidentialitet (4 kap. 1 § punkt 5)
En incident ska bedömas som betydande om den undergrävt riktigheten, autenticiteten eller konfidentialiteten i nät, tjänster eller uppgifter för minst 20 företagskunder eller minst 500 slutanvändare.

Ekonomisk skada (4 kap. 2 §; kostnadsberäkningen i 3 §)
En incident ska bedömas som betydande om den orsakat ekonomisk skada för verksamhetsutövaren som överstiger 5 miljoner kronor. Vid bedömningen ska de kostnader och intäktsbortfall som anges i PTSFS 2026:5 beaktas. Om den faktiska ekonomiska skadan inte kan fastställas ska den uppskattas.

Påverkan på viktiga samhällsfunktioner (4 kap. 4 § punkt 1)
För nät, tjänster eller uppgifter som används av en organisation med en viktig samhällsfunktion i Sverige ska alternativen i 4 kap. 4 § 1 PTSFS 2026:5 prövas: minst sex timmars incident med anledning att anta betydande störningar, eller kännedom om eller rimligen inhämtbar information om stabsläge eller annan organisatorisk eskalering på grund av incidenten.

Nödkommunikation och viktigt meddelande till allmänheten (4 kap. 4 § punkt 2 - 4 kap. 4 § punkt 3)
Bedömningen ska även omfatta incidenter där verksamhetsutövaren har fått kännedom om eller har särskild anledning att anta att medverkan till nödkommunikation eller förmedling av viktigt meddelande till allmänheten har misslyckats. Bedömningen ska göras enligt kriterierna i PTSFS 2026:5.

Enbart täckningsbortfall är inte tillräckligt för nödkommunikationskriteriet. VMA-kriteriet avser verksamhetsutövarens medverkan till förmedling av meddelanden som skickas till terminalutrustning.

Personskada (4 kap. 4 § punkt 4)
En incident ska bedömas som betydande om den har orsakat eller bidragit till en fysisk persons dödsfall eller betydande skada på en fysisk persons hälsa.

12.2.3 Incidenter som alltid är betydande

Följande typer av incidenter omfattas av särskilda bestämmelser i PTSFS 2026:5 och ska bedömas som betydande när förutsättningarna i respektive bestämmelse är uppfyllda:

- incident till följd av naturkatastrof som har undergrävt tillgängligheten i verksamhetsutövarens nät, tjänster eller uppgifter oavsett incidentens omfattning,
- internt eller externt angrepp eller intrång som sannolikt kan orsaka, bidra till eller möjliggöra allvarliga driftsstörningar,
- incident i central infrastruktur som under minst sex timmar medfört betydande påverkan på infrastrukturens eller nätets stabilitet, motståndskraft eller skyddsförmåga,
- nedsatt redundans i central infrastruktur som har betydelse för nät eller tjänster mellan Sverige och ett annat land.

Med central infrastruktur avses i detta sammanhang sådan infrastruktur, sådana förbindelser och knutpunkter som omfattas av definitionen i PTSFS 2026:5.

12.2.4 Återkommande incidenter

Incidenter som var för sig inte är betydande ska tillsammans bedömas som betydande enligt 4 kap. 6 § PTSFS 2026:5 när samtliga tre följande villkor är uppfyllda:

1. har inträffat minst två gånger inom sex månader,
2. bedöms ha samma orsak, sårbarhet, bristande säkerhetsåtgärd, rutin eller redundanta lösning, och
3. sammantaget medfört ekonomisk skada som överstiger fem miljoner kronor, beräknad enligt 4 kap. 2–3 §§ PTSFS 2026:5.

Processen för incidenthantering ska möjliggöra uppföljning och korrelation av återkommande incidenter.

12.2.5 Incidenter vid planerade förändringar

Incidenter vid planerade förändringar ska endast identifieras som betydande om oförutsedda negativa konsekvenser uppfyller någon bestämmelse i PTSFS 2026:5.

Bedömningen ska utgå från vad verksamhetsutövaren har förutsett eller skäligen borde ha kunnat förutse och dokumenterat i riskanalysen inför förändringen. Se även kapitel 11 Förändringar.

12.2.6 Rapportering av betydande incident

För sektorsverksamhet inom digital infrastruktur tillämpas rapporteringsbestämmelserna i 2 kap. MCFFS 2026:8. Bestämmelserna om betydandekriterier i 3–4 kap. och informationsskyldighet i 5 kap. gäller inte för denna sektorsverksamhet. För allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster görs bedömningen av betydande incidenter enligt PTSFS 2026:5. Om verksamhetsutövaren även tillhandahåller andra tjänster inom digital infrastruktur, exempelvis DNS- eller datacentraltjänster, ska tillämpliga kriterier för dessa tjänster bedömas separat, bland annat enligt EU:s genomförandeförordning (EU) 2024/2690 där den är tillämplig. Informationsskyldigheten gentemot mottagare av tjänster behandlas i kapitel 16.

Mål: Att betydande incidenter rapporteras skyndsamt, inom föreskrivna tidsfrister och med fullständigt underlag.

Åtgärder:

Betydande incidenter ska rapporteras till NCSC vid FRA genom myndighetens anvisade rapporteringssätt. Rapporteringen ska följa cybersäkerhetslagen och 2 kap. MCFFS 2026:8.

- **Upplysning och incidentanmälan**
  Upplysning ska lämnas så snart det kan ske, senast inom 24 timmar efter att verksamhetsutövaren fått kännedom om den betydande incidenten. Incidentanmälan ska lämnas så snart det kan ske, senast inom 72 timmar efter sådan kännedom.
- **Slutrapport och lägesrapport**
  Slutrapport ska lämnas senast en månad efter incidentanmälan. Om incidenten fortfarande pågår ska en lägesrapport lämnas vid denna tidpunkt. Slutrapport ska därefter lämnas inom en månad efter att incidenten har hanterats.
- **Delrapport**
  På myndighetens begäran ska en delrapport med relevanta statusuppdateringar lämnas.
- **Rapporteringsrutin**
  Verksamhetsutövaren ska ha en dokumenterad *Rutin för incidentrapportering* som:
  - utser ansvariga och ersättare,
  - innehåller checklistor för samtliga rapportuppgifter enligt 2 kap. 3–6 §§ MCFFS 2026:8,
  - säkerställer tillgång till aktuella formulär och rapporteringsvägar,
  - hanterar myndighetens reservförfarande,
  - möjliggör uppdatering av tidigare rapporter, och
  - säkerställer spårbarhet mellan rapporteringsstegen.

Tidpunkter för kännedom, bedömning och rapportering samt inskickade underlag och mottagningsbekräftelser ska dokumenteras. Rutinen ska kunna tillämpas även utanför ordinarie arbetstid.



12.2.7 Incidenter hos leverantör, kommunikationsoperatör eller annan extern part

Mål: Att verksamhetsutövaren kan identifiera, bedöma och rapportera incidenter även när deras ursprung finns hos en extern part.

Åtgärder:

- Avtal och *Rutiner för samverkan med externa parter* ska säkerställa att verksamhetsutövaren utan onödigt dröjsmål får sådan information från leverantörer, kommunikationsoperatörer och andra externa parter som krävs för att bedöma incidentens påverkan och rapporteringsskyldighet.
- Verksamhetsutövaren ska bedöma incidentens påverkan på de egna nät och tjänster som tillhandahålls.
- När flera verksamhetsutövare påverkas av samma bakomliggande händelse ska respektive verksamhetsutövare göra den bedömning och rapportering som krävs för den egna verksamheten.
- Incidenter hos eller med beroende till leverantörer ska hanteras enligt bestämmelserna om leverantörshantering i kapitel 14.3.

12.2.8 Integritetsincident

Mål: Att integritetsincidenter och personuppgiftsincidenter dokumenteras och rapporteras till relevant myndighet enligt tillämpligt regelverk.

Åtgärder:

- Ta fram en Rutin för rapportering av integritetsincidenter till myndigheter.

- Rapporter och underlag ska dokumenteras och finnas tillgängliga.

- Om en personuppgiftsincident ska anmälas enligt dataskyddsförordningen ska den rapporteras till Integritetsskyddsmyndigheten (IMY) inom 72 timmar enligt tillämpliga regler.

- En rapporteringspliktig integritetsincident enligt lagen om elektronisk kommunikation ska rapporteras till PTS utan onödigt dröjsmål, senast 24 timmar efter upptäckt. Kompletterande rapport ska lämnas så snart som möjligt, senast tre dagar efter den inledande rapporten. Om uppgifter saknas ska skälen anges och återstående uppgifter lämnas så snart som möjligt.

  - Berörda kunder eller användare ska informeras när sådan informationsskyldighet föreligger.
  - Samma LEK-reglerade integritetsincident behöver inte rapporteras till både PTS och IMY. Om händelsen även berör annan personuppgiftsbehandling ska eventuell anmälningsskyldighet enligt GDPR bedömas särskilt. Händelsen ska också prövas mot kriterierna för betydande incident enligt cybersäkerhetsregleringen.

Referenser: PTSFS 2026:5, Post- och telestyrelsens föreskrifter och allmänna råd om vad som utgör en betydande incident för verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster; MCFFS 2026:8, föreskrifter om incidentrapportering och informationsskyldighet för väsentliga och viktiga verksamhetsutövare; cybersäkerhetslagen (2025:1506), 2 kap. 5–10 §§.

13 Riskanalys, risk- och åtgärdshantering

Syfte: Identifiera, bedöma och hantera risker som kan påverka säkerheten i telenät, teletjänster, verksamhetssystem och information. Arbetet ska omfatta organisatoriska, logiska och fysiska hot samt kritiska beroenden och ge underlag för beslut om säkerhetsåtgärder.

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 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 driftstörningar, säkerhetsincidenter, integritetsincidenter och brottsdatalagringsincidenter i den egna verksamheten och hos andra relevanta aktörer. Analysen ska även beakta förändringar i hotbild, teknik, leverantörsberoenden och övriga omvärldsförhållanden.
- Riskanalysprocesserna ska utgå från etablerad standard på området. Vid val av säkerhetsåtgärder ska relevanta standarder, normer, säkerhetsvägledningar och praxis beaktas.

13.2 Riskanalys

Riskanalyserna ska omfatta verksamhetens nät, tjänster, verksamhetssystem, information, tillgångar, personal, fysisk miljö och kritiska beroenden. Analysen ska beakta organisatoriska, logiska och fysiska hot som kan påverka tillgänglighet, riktighet, autenticitet eller konfidentialitet.

Riskanalyserna ska även omfatta risken för integritetsincidenter och brottsdatalagringsincidenter enligt PTSFS 2026:1. Dessa analyser får ingå i den samlade riskanalysen, förutsatt att föreskriftens krav uppfylls och resultaten kan följas upp.

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 tidigare okända relevanta hot kan förmedlas av Post- och telestyrelsen.

Mål: Att risker för verksamhetens nät, tjänster, system och uppgifter är identifierade, bedömda och dokumenterade samt ger underlag för prioritering och beslut om säkerhetsåtgärder.

Åtgärder:

- Ta fram en plan för vid vilka tidpunkter och i vilka situationer riskanalyser ska genomföras.
- Identifiera relevanta hot och sårbarheter som kan orsaka driftstörningar, säkerhetsincidenter, integritetsincidenter eller brottsdatalagringsincidenter samt bedöm påverkan på verksamheten, kunder, användare och viktiga samhällsfunktioner.
- När verksamheten omfattas av krav på utlämnande av uppgifter till brottsbekämpande myndigheter ska analysen även beakta risken att tidsfrister, standarder och formatkrav inte kan uppfyllas.
- Konsekvensanalyser för höjd beredskap och krig ska genomföras enligt kapitel 19 och omfatta bortfall av nödvändiga verksamhetsdelar och resurser.
- 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.
- Göra 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: Identifierade risker hanteras genom dokumenterade beslut och säkerhetsåtgärder som uppfyller tillämpliga krav. Åtgärderna följs upp så att deras effekt och kvarstående risker kan bedömas.

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 riskhantering. Motivera riskacceptans och ange beslutsfattare och tidpunkt för omprövning. Riskacceptans får inte ersätta bindande skyddskrav.

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. För uppgifter som lagras för brottsbekämpande ändamål gäller de särskilda skyddskraven i 9 kap. 4 § förordningen (2022:511) om elektronisk kommunikation.*
- Dokumentera bedömningen vid val av åtgärder.
- Följ upp åtgärderna årligen och vid behov.
- Ange ansvarig och tidsfrist för beslutade åtgärder. Följ upp genomförande, effekt och kvarstående risker.

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.
- Upptäckta cyberhot, sårbarheter och andra risker ska utan dröjsmål föras till incidenthanteringen när de kan omfattas av kriterierna för betydande incident enligt PTSFS 2026:5. Bedömning och eventuell rapportering ska ske enligt kapitel 12.

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. Granskning och revision ska samordnas med egenkontroll och revision enligt kapitel 18.
- 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 13 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.
- Välj tillträdeslösning utifrån anläggningens skyddsbehov och dokumenterad riskbedömning. Om biometrisk identifiering övervägs ska behov, proportionalitet och rättsliga förutsättningar för personuppgiftsbehandlingen bedömas före införandet.
- 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:

- Fastställ behovet av kameraövervakning, larm och andra övervakningsåtgärder utifrån anläggningens skyddsbehov. Placering, omfattning och behandling av inspelat material ska bedömas enligt tillämpliga regler.
- Säkerställ att larm tas emot, bedöms och leder till åtgärd inom fastställda tider. Funktionen kan upprätthållas internt eller genom avtalad extern tjänst.
- 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.
- Identifierade brister ska riskbedömas och tilldelas ansvarig samt tidsfrist för åtgärd. Allvarliga brister ska hanteras skyndsamt. Tillfälliga skyddsåtgärder ska införas när permanent åtgärd inte kan genomföras omedelbart. Genomförande och effekt ska följas upp.

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
- Klassningsmodellen ska beskriva konsekvenserna av brister i konfidentialitet, riktighet och tillgänglighet samt, där det är relevant, autenticitet. Dessa aspekter ska bedömas var för sig och tillsammans ge underlag för skyddsåtgärder.

- Nivåerna, till exempel strängt konfidentiell, konfidentiell, intern och öppen kan användas för konfidentialitet. För övriga aspekter ska verksamheten fastställa dokumenterade konsekvensnivåer. Klassningens innebörd och tillhörande skyddskrav ska vara kända av berörda roller.

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 och tillämpa en gemensam *Process för tilldelning, ändring, uppföljning och återkallande av behörigheter*. Komplettera processen med rutiner för berörda system och informationsslag.
- Tilldelning och utökning av behörigheter ska godkännas av utsedd systemägare, informationsägare eller annan ansvarig roll innan behörigheten aktiveras. Dokumentationen ska ange innehavare, berörda resurser, tillåtna åtgärder, godkännare och eventuell giltighetstid.
- Implementera ett System för tilldelning, ändring, uppföljning och kontroll av identiteter och behörigheter för att säkerställa spårbarhet och efterlevnad.
- Dokumentera tilldelade behörigheter och följ upp dem minst årligen samt vid behov. Justera eller återkalla behörigheter när behovet förändras.
- Granska åtkomstloggar regelbundet för att upptäcka avvikelser och misstänkt aktivitet. Identifierade avvikelser ska hanteras i enlighet med verksamhetsutövarens process för incidenthantering enligt kapitel 12.
- 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.
- Utbildning och information ska genomföras enligt 14.2.8 och kapitel 17.

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.
- Tillämpa den gemensamma behörighetsprocessen enligt 14.2.2. Upprätta och underhåll en *Rutin för de särskilda krav som gäller åtkomst och behörighet till uppgifter för brottsbekämpande ändamål*. Rutinen ska även säkerställa separationen mellan åtkomst till uppgifterna och deras åtkomstloggar enligt 14.2.5.
- 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.
- Dokumentera tilldelade behörigheter och följ upp dem minst årligen samt vid behov. Justera eller återkalla behörigheter när behovet förändras.
- 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:

- Säkerställ att behandlade uppgifter som lagras varaktigt skyddas mot oavsiktlig eller otillåten utplåning eller förlust.
- 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 bör 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.

- Kravet på lagring på minst två fysiskt åtskilda platser gäller även åtkomstloggar för uppgifter som lagras för brottsbekämpande ändamål.
- Säkerhetskopior ska omfattas av samma skydd och utplånas samtidigt som de uppgifter som lagras för brottsbekämpande ändamål.
- Återläsning av säkerhetskopior bör 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.
- För uppgifter som lagras för brottsbekämpande ändamål ska verksamhetsutövaren säkerställa att den som haft tillgång till uppgifterna inte ges tillgång till loggar över åtkomsten.
- 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 automatiskt. 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.

Begreppet lagringsskyldig används i detta avsnitt enligt definitionen i 2 § PTSFS 2026:3 och avser den som är anmälningsskyldig enligt 2 kap. 1 § lagen om elektronisk kommunikation. Begreppet ska här inte begränsas till den särskilda lagringsskyldigheten för brottsbekämpande ändamål.

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, anslutningar för konfigurering och styrning samt åtkomstloggar enligt nedan skyddas genom kryptering enligt tillämpliga krav.

Åtgärder enligt PTSFS 2026:1, 10 kap.:

- Behandlade uppgifter som överförs via internet ska skyddas genom kryptering. Undantag får tillämpas om det med hänsyn till uppgifternas art och sammanhang är osannolikt att överföring utan kryptering kan leda till en integritetsincident eller brottsdatalagringsincident.
- Anslutningar för konfigurering och styrning av informationsbehandlingstillgångar via internet eller allmänna elektroniska kommunikationsnät som även andra än tillhandahållaren har rådighet över ska skyddas genom kryptering.
- Loggar avseende åtkomst till uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (2022:482) om elektronisk kommunikation ska skyddas genom kryptering under lagring och överföring.
- Kryptering ska ske med en allmänt erkänd krypteringsmetod med tillräcklig nyckellängd. Krypteringsnycklar ska hanteras säkert.
- Verksamhetsutövaren ska ha en dokumenterad *Rutin för hantering av kryptering och kryptonycklar*.

Undantaget för överföring av behandlade uppgifter via internet gäller inte de särskilda krypteringskraven för anslutningar för konfigurering och styrning eller åtkomstloggar för brottsbekämpande ändamål.

Interna krav på genomförande och uppföljning:

Bedömningar som ligger till grund för undantag från kryptering ska dokumenteras. Dokumentationen ska ange berörda uppgifter och överföringar, bedömda risker, skäl för undantaget, ansvarig beslutsfattare samt när bedömningen ska omprövas.

Rutinerna för krypteringsnycklar ska omfatta åtkomst, skapande, distribution, lagring, byte, återkallande och avveckling samt hantering vid misstänkt eller konstaterad kompromettering. Intervall för nyckelbyte ska fastställas utifrån användning, risk och tillämpliga krav.

Rekommendation:

Koder, lösenord och sammanställningar av uppgifter som rör en användare eller abonnent bör krypteras vid överföring via internet, enligt det allmänna rådet till 10 kap. 1 § PTSFS 2026:1.

14.2.8 Utbildning och medvetenhet

Mål: Att anställda och uppdragstagare som hanterar behandlade uppgifter har den kunskap som behövs för att tillämpa säkerhetskrav, skydda uppgifterna och hantera incidenter.

Åtgärder enligt PTSFS 2026:1:

Verksamhetsutövaren ska säkerställa att anställda och uppdragstagare har kunskap om och tillämpar de processer, rutiner och planer som de berörs av, enligt 3 kap. 4 §.

Åtkomst till behandlade uppgifter ska endast ges till personer som har upplysts om tystnadsplikten när 9 kap. 31 och 32 §§ lagen (2022:482) om elektronisk kommunikation är tillämpliga, enligt 7 kap. 2 § PTSFS 2026:1. För verksamhet som bedrivs inom kommunal förvaltning ska även tillämpliga bestämmelser om sekretess och tystnadsplikt enligt offentlighets- och sekretesslagen (2009:400) beaktas.

Interna krav på utbildning och information:

Personal som hanterar behandlade uppgifter, nätdata eller uppgifter för brottsbekämpande ändamål ska regelbundet få utbildning och information anpassad till sin roll, sina arbetsuppgifter och sin åtkomst. Detta fastställs som ett internt krav i dessa riktlinjer och genomför det allmänna rådet till 7 kap. 1 § PTSFS 2026:1.

Utbildningen och informationen ska omfatta:

- när och hur uppgifter får hanteras samt tillämpliga krav på behörighet och tystnadsplikt,
- relevanta rutiner för informationsskydd, loggning, kryptering och säker hantering,
- hur integritetsincidenter och brottsdatalagringsincidenter upptäcks och rapporteras internt,
- hur incidenternas möjliga konsekvenser för abonnenter, användare och brottsbekämpande myndigheter bedöms.

Utbildningsbehovet ska omprövas vid förändringar i arbetsuppgifter, system, riskbild eller regelverk samt efter relevanta incidenter. Genomförda utbildningsinsatser ska dokumenteras och följas upp enligt kapitel 17.

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 leverantörens förmåga att uppfylla verksamhetsutövarens säkerhetskrav är bedömd innan avtal ingås.

Åtgärder:

- Bedöm leverantörens betydelse för verksamheten utifrån levererade produkter och tjänster, åtkomst till system och uppgifter samt möjliga konsekvenser vid störningar eller brister.
- Anpassa säkerhetsutvärderingens omfattning till identifierade risker. Leverantörer av kritiska produkter eller tjänster ska omfattas av en fördjupad bedömning.
- Granska relevanta säkerhetsåtgärder, incidenthantering, kontinuitetsförmåga och beroenden till underleverantörer.
- Begär underlag som styrker leverantörens förmåga att uppfylla säkerhetskraven. Underlaget kan exempelvis bestå av dokumenterade rutiner, kontrollresultat, revisionsrapporter eller relevanta certifieringar.
- Dokumentera bedömningen, identifierade brister och villkor som behöver hanteras innan eller genom avtalet.

14.3.3 Avtalskrav och säkerhetsåtaganden

Mål: Att leverantörsavtalen innehåller tydliga säkerhetskrav och ansvar som motsvarar leveransens risker och betydelse för verksamheten.

Åtgärder:

- Fastställ säkerhetskrav utifrån leverantörsutvärderingen och dokumentera dem i avtalet. Kraven ska vara anpassade till leveransens innehåll, risker och betydelse.

- Reglera ansvar för informationsskydd, åtkomst, kontinuitet och relevanta underleverantörer samt hur efterlevnaden ska följas upp.
- För leveranser som kan påverka nät, tjänster, verksamhetssystem eller uppgifter ska avtalet kräva att leverantören utan onödigt dröjsmål meddelar säkerhetsincidenter och lämnar underlag för verksamhetsutövarens bedömning och rapportering enligt kapitel 12.
- Ange kontaktvägar, eskalering och tidsramar för incidentinformation så att verksamhetsutövaren kan uppfylla sina egna rapporteringsfrister.
- Reglera hur säkerhetsbrister ska åtgärdas och vilka konsekvenser bristande efterlevnad kan få.
- För kritiska tjänster och utlokaliserade säkerhetstjänster ska avtalet innehålla krav på en dokumenterad exit- och överlämningsplan som säkerställer kontinuitet och skydd av information vid avtalsupphörande.
- När leveransen kan beröras av tillsyn ska avtalet, där det är relevant och rättsligt möjligt, säkerställa leverantörens medverkan med nödvändig information och tekniskt stöd.

14.3.4 Uppföljning och revision av leverantörer

Mål: Att leverantörernas efterlevnad av avtalade säkerhetskrav följs upp under avtalstiden och att identifierade brister hanteras.

Åtgärder:

- Fastställ ansvar, metod och intervall för leverantörsuppföljning utifrån leveransens risker, betydelse och avtalskrav.
- Följ upp kritiska leverantörer regelbundet, med tätare uppföljning när riskbilden motiverar det. Som rekommenderad grundnivå bör en samlad uppföljning genomföras minst vartannat år.
- Genomför även uppföljning vid väsentliga förändringar i leveransen, leverantörens organisation, underleverantörer eller riskbild samt efter relevanta incidenter.
- Använd lämpliga underlag, exempelvis leverantörsrapporter, möten, kontrollresultat, revisionsrapporter och tekniska verifieringar. Revision på plats ska övervägas när riskerna och behovet av verifiering motiverar det.
- Dokumentera resultat, avvikelser, ansvariga och tidsfrister för korrigerande åtgärder. Följ upp att åtgärderna genomförs och får avsedd effekt.
- Upprätthåll aktuella kontaktvägar för löpande utbyte av säkerhetsinformation.

14.3.5 Incidenthantering med leverantörer

Mål: Att incidenter som berör leverantörer hanteras skyndsamt och samordnat samt att verksamhetsutövaren får underlag för egen bedömning, åtgärd och rapportering.

Åtgärder:

- Dokumentera *Rutiner för gemensam incidenthantering med relevanta leverantörer*. Rutinerna ska ange roller, ansvar, kontaktvägar och eskalering.
- Kontaktvägar, ansvariga, ersättare, eskalering och former för informationsutbyte ska hållas aktuella. Uppgifterna kan samlas i en *Kommunikationsplan för leverantörer* eller ingå i rutinerna för leverantörshantering och gemensam incidenthantering.
- För kritiska leveranser ska verksamhetsutövarens och leverantörens incidentrutiner samordnas och vid behov verifieras genom gemensamma genomgångar eller övningar.
- Säkerställ att leverantören utan onödigt dröjsmål lämnar tillgänglig information om incidentens art, tidpunkt, varaktighet, berörda system eller tjänster samt faktisk eller möjlig påverkan.
- Förmedla informationen skyndsamt till den funktion som ansvarar för incidentbedömning och rapportering enligt kapitel 12. Informationen ska kompletteras när nya uppgifter blir tillgängliga.
- Samordna åtgärder för begränsning, återställning och informationsutbyte. Kontaktvägar ska fungera även utanför ordinarie arbetstid när incidenthanteringen kräver det.
- Dokumentera händelseförlopp, beslut och åtgärder samt följ upp orsaker och förbättringsbehov tillsammans med leverantören.
- När flera verksamhetsutövare påverkas ska samverkan ske utan att respektive verksamhetsutövares ansvar för egen bedömning och rapportering inskränks.

14.4 Logisk säkerhet för nät och system

Syfte: Säkerställa att telenät, tjänsteplattformar och verksamhetssystem skyddas mot obehörig åtkomst, manipulation, störningar och spridning av incidenter.

Mål: Att logiska säkerhetsåtgärder är fastställda, genomförda och verifierade utifrån verksamhetens risker och tillgångarnas skyddsbehov.

Åtgärder:

- Fastställ och dokumentera rollbaserade behörigheter för telenät, teletjänster, verksamhetssystem, programvara och information. Behörigheterna ska begränsas till vad som behövs för arbetsuppgifterna och skilja mellan åtkomst och rätt att utföra olika åtgärder.
- Behörighetsmodellen ska, där det är relevant, skilja mellan att läsa, registrera, ändra, kopiera eller exportera, radera, installera eller uppdatera programvara, konfigurera och administrera system samt tilldela behörigheter. Rätt att godkänna en åtgärd ska skiljas från rätt att genomföra den när riskbedömningen motiverar det.
- Behörigheterna ska hanteras genom den gemensamma processen enligt 14.2.2.
- Fastställ principer för separation mellan kundtrafik, administration, verksamhetssystem och externa anslutningar.



- Begränsa och kontrollera administrativ åtkomst och fjärråtkomst, inklusive åtkomst för leverantörer och uppdragstagare.
- Använd personliga identiteter för användaråtkomst och separata administrativa konton för privilegierade åtgärder. Multifaktorautentisering ska användas för administrativ åtkomst och fjärråtkomst, om inte en dokumenterad bedömning visar att motsvarande skydd uppnås på annat sätt.
- Tjänstekonton ska ha utsedd ansvarig, avgränsade behörigheter och skyddade autentiseringsuppgifter. Nödåtkomst ska vara kontrollerad, spårbar och granskas efter användning.
- Säkerställ säker grundkonfiguration av utrustning och system samt kontroll av konfigurationsändringar och avvikelser.
- Bedöm och inför skydd mot överbelastning, missbruk och angrepp mot relevanta nätfunktioner och tjänsteplattformar.
- Säkerställ att sårbarheter identifieras, bedöms, åtgärdas och följs upp i samordning med underhålls- och förändringshanteringen.
- Skydda de arbetsstationer och verktyg som används för administration av nät och system.
- Dokumentera åtgärder, ansvar och motiverade undantag. Verifiera skyddens funktion inom ramen för kapitel 18.

Genomförandet ska beskrivas i verksamhetsanpassade tekniska anvisningar och rutiner. Åtgärdernas omfattning ska anpassas till verksamhetsutövarens roll, teknik, riskbild och beroenden.

14.5 Personalsäkerhet

Syfte: Säkerställa att anställda och uppdragstagare har förutsättningar att utföra sina uppgifter säkert och att personrelaterade risker hanteras.

Mål: Att säkerhetskrav för personal och uppdragstagare tillämpas vid anställning, uppdrag, förändrade arbetsuppgifter och avslut.

Åtgärder:

- Bedöm säkerhetskrav och kompetensbehov utifrån arbetsuppgifternas ansvar, åtkomst och möjliga påverkan på verksamheten.
- Säkerställ att berörda personer känner till sina säkerhetsåtaganden och får utbildning enligt kapitel 17.
- Tillämpa den gemensamma behörighetsprocessen enligt 14.2.2 vid anställning, ändrade arbetsuppgifter och avslut av anställning eller uppdrag.
- Samordna tilldelning, ändring och återkallande av behörigheter med anställningens eller uppdragets förändringar.



- Säkerställ återlämning av utrustning och återkallande av åtkomst när anställning eller uppdrag avslutas.
- Hantera risker kopplade till insideragerande och kritiska personberoenden.
- Dokumentera ansvar och arbetssätt i verksamhetens personal- och behörighetsrutiner. Eventuella personkontroller ska vara behovsanpassade och genomföras med hänsyn till rättsliga förutsättningar.

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 och tillämpa en verksamhetsanpassad metod för kontinuitetshantering med stöd av ISO 22301 eller liknade till exempel MCF:s metodstöd för kontinuitetshantering och 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 upprätta 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*.
- Upprätta *Kontinuitets- och återställningsplaner* som beskriver när planerna ska aktiveras, ansvar och mandat, kontaktvägar, alternativa arbetssätt, prioriterade funktioner, återställningsordning och nödvändiga resurser. Planerna ska ange mål för återställningstid och, där det är relevant, accepterad informationsförlust. Kritiska leverantörsberoenden och tillgång till planerna vid bortfall av ordinarie system ska beaktas.
- Fastställa tider och kriterier för revidering.
- Fastställa när och på vilket sätt kontinuitetsplanerna ska övas (minst vartannat år) och utvärderas.

Kontinuitets- och återställningsplaneringen ska även beakta risken för driftpåverkan vid myndighetsinitierad säkerhetsskanning. Inför sådan skanning ska verksamhetsutövaren kunna medverka till riskbedömning, planering för minimerad belastning, kriterier för avbrytande och säkerställande av erforderlig återställningsförmåga.

Återställningsförmågan ska omfatta de system, uppgifter, konfigurationer och stödfunktioner som behövs för att återställa prioriterade nät och tjänster. Planeringen ska beakta att ett intrång kan påverka både produktionsmiljön och ordinarie återställningsresurser. Tester och övningar ska ge underlag för att bedöma om återställning kan genomföras säkert och inom fastställda tidsmål.

15.2 Kris och katastrofhantering

Mål: Att begränsa konsekvenserna av omfattande störningar och katastrofer samt återställa prioriterade funktioner, system och tjänster. Katastrofhanteringen ska samordnas med verksamhetens incidenthantering, kontinuitetsplanering och krisledning.

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 Information till mottagare av tjänster

Mål: Att mottagare av verksamhetsutövarens tjänster skyndsamt får relevant information om betydande incidenter och betydande cyberhot samt om åtgärder som de kan vidta.

Åtgärder:

- Verksamhetsutövaren ska ha en dokumenterad *Rutin för information till berörda mottagare*. Rutinen ska ange ansvariga funktioner, beslutsvägar och kommunikationskanaler.
- Rutinen ska omfatta relevanta mottagare utifrån verksamhetsutövarens roll och tillhandahållna tjänster. Dessa kan vara slutanvändare, företagskunder, kommunikationsoperatörer, tjänsteleverantörer eller andra grossistkunder. Kontaktvägar och ansvar för vidare informationsförmedling ska vara tydliga.
- Vid en betydande incident som sannolikt inverkar negativt på tillhandahållandet av tjänsterna ska mottagarna informeras så snart det kan ske, om det är lämpligt.
- Vid ett betydande cyberhot ska mottagare som kan påverkas informeras så snart det kan ske om skydds- och motåtgärder som de kan vidta. Om det är lämpligt ska information även lämnas om själva hotet.

Informationen bör vara begriplig och beskriva berörda tjänster, känd påverkan och rekommenderade åtgärder. Beslut om information, berörda mottagare och tidpunkt för informationslämnandet ska dokumenteras. Informationen ska uppdateras när nya omständigheter motiverar det.

16.2 Samarbete med myndigheter och operatörer

Vid säkerhetsrevision eller säkerhetsskanning enligt cybersäkerhetslagen ska verksamhetsutövaren ha utpekade kontaktvägar och kunna samordna dokumentation, intervjuer, tekniska kontroller samt risk- och driftfrågor med behörig tillsynsmyndighet.

Informationsdelning

Mål: Att verksamhetsutövaren har etablerade kontaktvägar och förmåga att dela relevant information om cyberhot, incidenter och säkerhetsrelaterade händelser med behöriga myndigheter och andra berörda aktörer.

Åtgärder:

- Upprätthålla aktuella kontaktvägar till relevanta myndigheter och andra aktörer
- Dela information om cyberhot och incidenter när sådan informationsdelning följer av tillämpligt regelverk, myndighetsbegäran eller etablerad samverkan.

- Säkerställa att informationsdelning sker med beaktande av sekretess, konfidentialitet och skyddsvärdet hos den information som lämnas.

Rapportering och samarbete

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

Åtgärder:

- **Incidentrapportering:** Betydande incidenter enligt cybersäkerhetslagen ska rapporteras till Nationellt cybersäkerhetscenter (NCSC) enligt kapitel 12. Integritetsincidenter enligt lagen om elektronisk kommunikation ska rapporteras till PTS enligt tillämpliga regler. Om en händelse omfattas av flera regelverk ska rapporteringsskyldigheten bedömas enligt respektive regelverk.
- **Informationsdelning:** Verksamhetsutövaren ska kunna dela relevant information med PTS, NCSC, CERT-SE och andra behöriga myndigheter eller aktörer när detta krävs eller är motiverat.
- **Samverkan:** Vid incidenter som påverkar eller riskerar att påverka andra operatörer, kunder eller viktiga samhällsfunktioner ska verksamhetsutövaren ha förmåga att samverka med berörda aktörer.
- **Samordnade insatser:** Verksamhetsutövaren ska medverka i nationell eller internationell samordning när detta efterfrågas av behörig myndighet eller följer av tillämpligt regelverk.

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 Ledningens och personalens utbildning

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:

Följande krav och utbildningsinsatser ska tillämpas:

17.1.1 Styrelsens och ledningens utbildning

Mål: Styrelse och verkställande ledning ska ha den kunskap och kompetens om cybersäkerhet som krävs för att fullgöra ledningens ansvar enligt cybersäkerhetslagen och 2 kap. 1 § MCFFS 2026:11.

Åtgärder:

Ledningen ska genomgå utbildning som ger den förmåga att:

- fastställa mål och inriktning för verksamhetsutövarens cybersäkerhet,
- utifrån identifierade risker bedöma vilka säkerhetsåtgärder som behöver genomföras för att upprätthålla en lämplig och proportionerlig nivå av cybersäkerhet,
- övervaka genomförandet av säkerhetsåtgärderna.

Utbildningen bör behandla ledningens roll i det systematiska och riskbaserade cybersäkerhetsarbetet, relevant reglering och terminologi, cybersäkerhetens betydelse för verksamheten och berörda samhällsfunktioner, riskhantering och uppföljning samt relevanta interna regler och arbetssätt.
För att säkerställa spårbarhet och möjliggöra uppföljning av ledningens kompetens ska verksamhetsutövaren dokumentera genomförd utbildning, dess huvudsakliga innehåll, datum samt vilka personer som deltagit.

17.1.2 Övrig personalutbildning

- Utbildning i riskhanteringsåtgärder: Anställda och uppdragstagare ska erbjudas relevant utbildning om riskhanteringsåtgärder utifrån roll, arbetsuppgifter och verksamhetens riskbild.
- **Grundutbildning**: Alla nya anställda, eller vid byte arbetsuppgift, ska genomgå en grundutbildning i säkerhetspolicyer och rutiner snarast efter anställning/ förändring.

- Årlig uppdatering: Som rekommenderad grundnivå bör alla anställda årligen få en uppdatering om tillämpliga säkerhetsregler, aktuella hot och verksamhetens rutiner. Om verksamhetsutövaren fastställer årlig utbildning som ett internt krav ska detta anges i utbildningsplanen tillsammans med målgrupp, ansvar, innehåll och uppföljning.
- Återkommande utbildning: Personalens utbildningsbehov ska bedömas utifrån arbetsuppgifter, riskbild och förändringar i verksamheten. Fördjupad utbildning och uppdateringar utöver den rekommenderade årliga grundnivån ska anpassas till respektive roll och identifierade behov.
- **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.
  Ledningens utbildningsbehov ska omprövas regelbundet och vid väsentliga förändringar i regelverk, hotbild, riskbild, verksamhet eller teknik.

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.

Anm. Mått och målnivåer i detta kapitel är exempel som verksamhetsutövaren ska anpassa till sin riskbild, tekniska miljö och tjänsteåtaganden. Procentsatser, förbättringsmål och tekniska lösningar utgör inte i sig föreskrivna nivåer enligt cybersäkerhetslagen. Uppföljningen ska samtidigt verifiera att tillämpliga bindande krav uppfylls.

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 MWT (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 Uppföljning av säkerhetsarbetet

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: Genomför och dokumentera riskanalyser minst årligen och vid de ytterligare tillfällen som anges i kapitel 13.

18.2.3 Incidenthantering:

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

Mål: Säkerställa att incidenter identifieras, bedöms, hanteras, dokumenteras och rapporteras enligt fastställda processer och tillämpliga regelverk.

Uppföljning:
Verksamhetsutövaren ska regelbundet följa upp incidenthanteringsprocessens funktion och effektivitet. Uppföljningen bör minst omfatta:

- andel relevanta incidenter där bedömning av rapporteringsskyldighet har genomförts och dokumenterats,
- andel betydande incidenter där föreskrivna rapporteringsfrister har uppfyllts,
- incidenter där underlag för bedömning varit otillräckligt eller fördröjt,
- återkommande incidenter och identifierade gemensamma grundorsaker,
- genomförande och effekt av beslutade korrigerande och förebyggande åtgärder, och
- identifierade behov av förändringar i processer, organisation, teknik, dokumentation eller utbildning.

Resultatet ska användas som underlag för verksamhetsutövarens kvalitetsuppföljning och ledningens uppföljning av säkerhetsarbetet.

18.3 Fysisk säkerhet

18.3.1 Tillträdeskontroll:

Mål: Upprätthålla tillträdesskydd utifrån anläggningarnas fastställda skyddsbehov. Uppföljningen ska omfatta både tekniska skydd, behörigheter och tillämpade rutiner.

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: Identifierade brister ska åtgärdas inom riskbaserade tidsfrister enligt avsnitt 14.1.5.

18.4 Logisk säkerhet

18.4.1 Nätverkssäkerhet:

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

Mål: Följ upp förmågan att förebygga, upptäcka och begränsa intrång. Bedöm upptäckts- och hanteringstider, konsekvenser och återkommande orsaker.

18.4.2 Åtkomstkontroll:

Kontrollera att autentiseringskraven enligt 14.4 tillämpas, inklusive kraven för administrativ åtkomst och fjärråtkomst samt dokumenterade undantag.

Mål: Följ upp att fastställda autentiseringskrav är genomförda, särskilt för privilegierad åtkomst och fjärråtkomst. Dokumentera undantag, riskbedömning och kompenserande åtgärder.

18.4.3 Sårbarhetshantering:

Begreppet sårbarhetsskanning i detta avsnitt avser verksamhetsutövarens egen säkerhetsåtgärd. Det ska skiljas från säkerhetsskanning enligt MCFFS 2026:12, som är ett tillsynsverktyg som beslutas och genomförs inom ramen för myndighetstillsyn.

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

Mål: Följ upp att identifierade sårbarheter bedöms och hanteras inom fastställda riskbaserade tidsfrister. Redovisa särskilt kritiska sårbarheter som kvarstår efter beslutad åtgärdstid.

18.5 Egenkontroll och revision

Mål: Att verksamhetsutövarens egenkontroller samt interna och externt initierade revisioner genomförs regelbundet för att säkerställa att säkerhetsarbetet fungerar effektivt och i enlighet med lagar, föreskrifter och interna krav. Myndighetsinitierad säkerhetsrevision enligt cybersäkerhetslagen hanteras särskilt i avsnitt 18.6.

Åtgärder:

Ta fram och underhåll en *Plan för egenkontroll och revision av säkerhetsarbetet*. Planen ska ange omfattning, ansvariga, metoder, intervall och tidpunkter samt hur resultat och korrigerande åtgärder ska följas upp.

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.

Åtgärderna enligt PTSFS 2026:1 avseende riskbehandling, förändringar, behörigheter, lagringsskydd, loggning och kryptering ska dokumenteras och följas upp årligen och vid behov.

Uppföljningen ska ge underlag för att bedöma både efterlevnad och skyddsåtgärdernas funktion. Resultat, brister, beslutade förbättringar och ansvariga ska dokumenteras.

Uppföljningen ska omfatta tillämpningen av huvudriktlinjerna, processbilagorna och verksamhetens egna styrande dokument. För relevanta krav och säkerhetsområden ska det gå att visa ansvarig funktion, tillämpat arbetssätt, genomförda åtgärder och resultat av verifiering. Identifierade brister ska hanteras med ansvarig, tidsfrist och uppföljning.

Vid revidering av riktlinjerna ska bilagan Definitioner, dokument och standarder samt berörda processbilagor kontrolleras och uppdateras samordnat. Kontrollen ska särskilt säkerställa att definitioner, incidenttrösklar, beräkningsgrunder, rapporteringsfrister, myndighetskontakter och föreskrifternas tillämpningsområden överensstämmer med huvuddokumentet och gällande regler.

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.

18.6 Säkerhetsrevision vid tillsyn

Säkerhetsrevision och säkerhetsskanning enligt MCFFS 2026:12 genomförs inom ramen för myndighetstillsyn. Följande avsnitt beskriver därför främst de organisatoriska, dokumentationsmässiga och tekniska förberedelser som verksamhetsutövaren bör ha för att kunna medverka på ett kontrollerat och ändamålsenligt sätt vid sådan tillsyn.

Bestämmelserna i 2 kap. MCFFS 2026:12 tillämpas när tillsynsmyndigheten anlitar ett oberoende organ för säkerhetsrevision. Verksamhetsutövarens förberedelser enligt detta avsnitt ska stödja medverkan vid tillsyn och hållas åtskilda från verksamhetens egenkontroll och interna revision.

Mål: Säkerställa att verksamhetsutövaren har organisatorisk och dokumentationsmässig beredskap att medverka vid säkerhetsrevision som genomförs inom ramen för tillsyn enligt cybersäkerhetslagen och MCFFS 2026:12.

Åtgärder:

- Utse ansvarig kontaktfunktion för samordning med tillsynsmyndigheten.
- Kunna tillhandahålla relevanta styrande dokument, riskanalyser, teknisk dokumentation, avtal, kontrollresultat och andra underlag som behövs för revisionen.
- Säkerställa att berörda roller och ansvariga personer kan medverka vid intervjuer och sakgranskning.
- Kunna medverka till tekniska kontroller av relevanta system och nätsegment samt, när det krävs inom ramen för tillsynen, kontroll av berörda lokaler och anläggningar.
- Kunna visa både hur säkerhetsåtgärder är utformade och hur de faktiskt tillämpas i verksamheten.
- Dokumentera och riskbedöma identifierade avvikelser och sårbarheter samt besluta om korrigerande eller förebyggande åtgärder och följa upp att dessa genomförs.

18.7 Säkerhetsskanning vid tillsyn

Mål: Säkerställa att verksamhetsutövaren kan medverka vid säkerhetsskanning enligt cybersäkerhetslagen och MCFFS 2026:12 utan att i onödan äventyra driftsäkerheten i telenät, teletjänster eller tillhörande system.

Åtgärder:

- Ha en dokumenterad *Rutin för medverkan vid säkerhetsskanning* som beslutas av behörig tillsynsmyndighet.
- Kunna identifiera berörda system, nätsegment, systemberoenden, internetexponering och ansvariga tekniska funktioner.
- Medverka till bedömning av risken för driftpåverkan och planering av lämplig tidpunkt och genomförande.
- Medverka till att belastning och annan påverkan på systemen minimeras samt att det finns tydliga kriterier och en plan för att avbryta skanningen vid behov.
- Säkerställa erforderlig backup- och återställningsförmåga före skanning när riskbedömningen visar behov av detta.

- Skyndsamt riskbedöma, dokumentera, prioritera och åtgärda brister och sårbarheter som kommuniceras efter genomförd skanning.

***Anm.**: Säkerhetsskanning enligt detta avsnitt är ett tillsynsverktyg och ska inte förväxlas med verksamhetsutövarens egna sårbarhetsskanningar enligt avsnitt 18.4.3.*

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:

- Verksamhetsutövaren ska utse särskilt ansvariga för kontinuitetsplaneringen för höjd beredskap och krig. Rollfördelningen ska dokumenteras.
- Konsekvensanalyser, kontinuitetsplaner och planer för samverkan med PTS ska dokumenteras och revideras vid behov.
- Anställda och uppdragstagare ska ha kunskap om och tillämpa de planer som berör dem. Verksamhetsutövaren ska säkerställa detta genom information, utbildning och övning anpassad till respektive roll.
- 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.

  Rekommendation: Övning bör genomföras regelbundet och minst vartannat år. Omfattning och innehåll bör anpassas till verksamhetens risker och förändringar.

  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 verksamhet som bedrivs inom en kommun eller region ska planeringen samordnas med kommunens eller regionens skyldigheter enligt lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.

För kommunala bolag ska samordningen även beakta tillämpliga ägardirektiv, avtal och kommunens beredskapsplanering. Bolagets egna skyldigheter enligt PTSFS 2026:2 kvarstår.

19.2 Samverkan med PTS

Mål: Att verksamhetsutövaren har etablerade kontaktvägar och förmåga att samverka med PTS vid höjd beredskap och krig.

Åtgärder:

Ta fram *Plan för samverkan med PTS*, planen ska ange kontaktvägar, ansvariga, ersättare, bemanning och tekniska kommunikationslösningar. Planeringen ska möjliggöra att samverkansfunktionen upprätthålls dygnet runt i 90 dagar.

Samverkan genom NTSG, SISG eller andra samverkansstrukturer ska hanteras när detta är tillämpligt för verksamhetsutövaren och enligt den samverkansordning som gäller.