Riktlinjer för säkerhet i telenät och teletjänster

Bilaga. Definitioner, dokumentförteckning och standarder

Ver. 1.2

TLP:CLEAR

STADSNÄTS FÖRENINGEN

Innehåll

1 Definitioner 2

2 Dokumentförteckning 7

3 Standarder och ramverk 10

1 Definitioner

I detta dokument används begrepp som hämtas från gällande lagstiftning, internationella standarder och etablerad praxis inom området för elektronisk kommunikation och cybersäkerhet. Definitionerna syftar till att skapa en gemensam och entydig förståelse och ska tillämpas konsekvent inom ramen för riktlinjerna.

Om inget annat anges ska begrepp som används i cybersäkerhetslagen, cybersäkerhetsförordningen och lagen om elektronisk kommunikation tolkas i enlighet med dessa regelverk.

Begreppet cybersäkerhet används i detta dokument som ett övergripande begrepp som omfattar fysisk säkerhet, logisk säkerhet, informationssäkerhet och IT-säkerhet i den utsträckning dessa påverkar telenät och tillhandahållna teletjänster.

Definitioner

Autenticitet
Förmågan att verifiera identitet, ursprung och äkthet hos information, system, användare eller transaktioner.

Allmänt tillgängligt elektroniskt kommunikationsnät
Ett elektroniskt kommunikationsnät som helt eller huvudsakligen används för att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster och som stöder informationsöverföring mellan nätanslutningspunkter,

(Allmänt tillgänglig) elektronisk kommunikationstjänst
En tjänst som vanligen tillhandahålls mot ersättning via elektroniska kommunikationsnät

Anläggningstillgångar
Fysiska tillgångar som ingår i telenätet, såsom nätverksutrustning, fiber, noder, byggnader och tekniska installationer.

Behandlade uppgifter
Uppgifter som behandlas i samband med tillhandahållande av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster, kommunikation så att de lagrade uppgifterna inte är av samma kvalitet och föremål för samma säkerhet och skydd som vid den behandling som skett före lagringen,

Brottsdatalagringsincident
En händelse som leder till oavsiktlig eller otillåten förstöring av, oavsiktlig förlust eller ändring av, otillåten behandling av, otillåten lagring av, otillåtet avslöjande av eller otillåten tillgång till uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (2022:482) om elektronisk

Cyberhot
Ett potentiellt eller faktiskt hot som kan utnyttja sårbarheter i nätverk, informationssystem eller tjänster och därigenom påverka tillgänglighet, riktighet, konfidentialitet eller autenticitet.

Cybersäkerhet
Skyddet av nätverk och informationssystem mot fysiska och logiska hot som kan påverka drift, funktion eller information. Cybersäkerhet omfattar förebyggande, upptäckt, hantering och

återhämtning från incidenter och syftar till att säkerställa tillgänglighet, riktighet, konfidentialitet och autenticitet.

Datasäkerhet
Skydd av data mot oavsiktlig eller avsiktlig förlust, förvanskning eller otillåten åtkomst för att säkerställa dataintegritet och tillgänglighet.

Dataskydd
Hantering av personuppgifter i enlighet med tillämplig dataskyddslagstiftning i syfte att skydda individers integritet.

Driftsäkerhet
Förmågan hos nät och tjänster att fungera tillförlitligt och vara tillgängliga över tid, inklusive tekniska och organisatoriska åtgärder för att förebygga och hantera störningar.

Efterlevnad
Säkerställande av att verksamheten följer tillämpliga lagar, förordningar, föreskrifter och interna styrande dokument.

Funktionssäkerhet (Reliability performance)
Förmågan hos en enhet att utföra en krävd funktion under givna förhållanden under ett specificerat tidsintervall. Vanliga mått är exempelvis MTBF (Mean Time Between Failures).

Fysisk säkerhet
Åtgärder som syftar till att skydda människor, anläggningar och utrustning mot fysiska hot såsom intrång, sabotage, stöld, vandalism och naturhändelser.

Förbindelse
Del av ett allmänt elektroniskt kommunikationsnät mellan två tillgångar eller mellan en tillgång och en anslutning till ett sådant kommunikationsnät,

Förändringshantering
Kontrollerad hantering av förändringar i nät, system och tjänster för att minimera risker och oönskade konsekvenser.

Hanterade tjänster
Tjänster där extern leverantör ansvarar för drift, övervakning, underhåll eller utveckling av nät, system eller informationsbehandlingstillgångar.

Historiska uppgifter
Uppgifter som ska lagras enligt 9 kap. 19 och31 §§ lagen om elektronisk kommunikation och9 kap. 7 och 8 §§ förordningen (2022:511) om elektronisk kommunikation, uppgifter som ska bevaras efter beslut enligt 27 kap. 16 § rättegångsbalken samt övriga uppgifter som behandlas för egna ändamål av den lagringsskyldige,

Incident
En händelse som påverkar eller riskerar att påverka tillgänglighet, riktighet, konfidentialitet eller autenticitet i nätverk, informationssystem eller tjänster.

Incidenthantering
Process för att upptäcka, rapportera, analysera, åtgärda och följa upp incidenter.

Incidenthanteringssystem
Stödjande system för dokumentation, spårning och uppföljning av incidenter och vidtagna åtgärder.

Informationsbehandlingstillgångar
Tillgångar som används för att behandla, lagra, överföra eller skydda information, exempelvis information, mjukvara, hårdvara, tjänster och lokaler.

Informationsbehandlingssystem
System eller tekniska komponenter som används för att behandla, lagra, överföra eller skydda information.

Informationsbehandlingssystem kan bestå av programvara, databaser, nätverkskomponenter, servrar, lagringssystem och andra tekniska resurser som tillsammans möjliggör informationshantering.

Informationssäkerhet
Skydd av information för att säkerställa konfidentialitet, riktighet och tillgänglighet.

Integritetsincident
Incident som innebär att personuppgifter eller annan skyddsvärd information exponeras, förloras, förändras eller behandlas på ett otillbörligt sätt.

IT-system
Sammanhängande helhet av programvara, hårdvara, nätverk och databaser som stödjer en eller flera verksamhetsfunktioner.

Konfidentialitet

Konfidentialitet innebär att information skyddas mot obehörig åtkomst, insyn, spridning eller användning, så att endast behöriga aktörer får ta del av informationen.

Kontinuitetshantering
Arbete för att säkerställa att verksamheten kan upprätthållas eller återställas vid störningar, kriser eller extraordinära händelser.

Kritiska tillgångar
Anläggningstillgångar och informationsbehandlingstillgångar som är avgörande för funktion och säkerhet i telenät och teletjänster.

Kryptering
Metod för att skydda information genom att göra den oläsbar för obehöriga.

Lagringsskyldig
Den som enligt 2 kap. 1 § lagen (2022:482) om elektronisk kommunikation är skyldig att anmäla sin verksamhet,

Ledningssystem
Ett ledningssystem är den samlade strukturen av styrning, processer, ansvar, rutiner och kontroller som används för att säkerställa uppfyllnad av kraven. Syftet är att skapa ett systematiskt och upprepbart sätt att styra, driva, utveckla och följa upp verksamheten.

Loggning
Registrering av händelser och aktiviteter i system för att möjliggöra spårbarhet, analys och incidentutredning.

Logisk säkerhet
Tekniska och organisatoriska åtgärder som skyddar informationssystem och data mot obehörig åtkomst, manipulation eller förlust.

Nätverk och informationssystem
Elektroniska kommunikationsnät, tillhörande informationssystem samt digitala stödsystem som är nödvändiga för att tillhandahålla teletjänster.

Penetrationstest
Kontrollerad simulering av angrepp mot system i syfte att identifiera sårbarheter.

Realtidsuppgifter
Uppgifter i realtid som omfattas av beslut om hemlig avlyssning av elektronisk kommunikation eller beslut om hemlig övervakning av elektronisk kommunikation samt beslut om inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Redundans
Användning av parallella eller ersättande komponenter för att säkerställa fortsatt funktion vid fel.

Resiliens
Förmåga att motstå, anpassa sig till och återhämta sig från störningar och incidenter.

Riskanalys
Systematisk bedömning av risker utifrån sannolikhet och konsekvens.

Riktighet
Riktighet innebär att information, data, konfigurationer, signaleringsinformation, driftdata och annan information som används i eller av telenät och teletjänster är korrekt, fullständig, aktuell och inte obehörigen eller oavsiktligt förändrad.

Risk- och åtgärdshantering
Process för att besluta om och följa upp åtgärder baserat på identifierade risker.

Sårbarhetsanalys
Identifiering och bedömning av tekniska, organisatoriska eller administrativa svagheter.

Sårbarhetshantering
Kontinuerligt arbete med att identifiera, prioritera och åtgärda sårbarheter.

Säkerhetsincident
Incident som påverkar eller hotar säkerheten i nät, system eller tjänster.

Säkerhetskopiering
Skapande av kopior av data och systemkonfigurationer för återställning vid förlust.

Säkerhetsåtgärder
Tekniska, organisatoriska och administrativa åtgärder för att minska risker och skydda verksamheten.

Telenät
Samtliga anläggnings- och informationsbehandlingstillgångar som krävs för att tillhandahålla teletjänster.

Teletjänst
Tjänst som möjliggör elektronisk kommunikation mellan användare och/eller system.

Tillbud
Oönskad händelse som hade kunnat leda till en incident.

Tillgänglighet
Andel av tiden som en tjänst eller funktion är tillgänglig för användning.

Tillförlitlighet
Sammantagen förmåga hos system och organisation att leverera tjänster enligt krav över tid.

Tillhandahållare
Verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster som avses i 1 kap. 7 § lagen om elektronisk kommunikation,

Uppdragstagare
Den som anlitats av tillhandahållaren för att utföra installation, underhåll, felavhjälpning, drift eller liknande hantering av tillhandahållarens informationsbehandlingstillgångar och förbindelser.

Utlokaliserad säkerhetstjänst
Säkerhetstjänst som helt eller delvis utförs av extern leverantör, exempelvis övervakning, incidenthantering eller sårbarhetshantering.

Verksamhetssystem
Verksamhetssystem omfattar de tekniska system, applikationer och arbetsprocesser som används för att hantera hela livscykeln av telekomtjänster – från kundbeställning och provisionering till drift, övervakning, fakturering och kundsupport.

Verksamhetsutövare
Med verksamhetsutövare avses den juridiska person som har det faktiska ansvaret för drift, förvaltning och styrning av nätverk och informationssystem och som därmed ansvarar för efterlevnad av cybersäkerhetslagen.

Åtkomstkontroll
Åtgärder som säkerställer att endast behöriga personer får tillgång till system och information.

2 Dokumentförteckning

För att underlätta hanteringen och tillgången till de olika dokument som kompletterar och fördjupar innehållet i detta dokument, presenteras här en sammanställning av alla dokument:

Tillämpliga lagar och föreskrifter

Cybersäkerhetslagen (2025:1506) och cybersäkerhetsförordningen (2025:1507)
Ställer krav på att verksamhetsutövaren ska kunna visa efterlevnad av lagens krav. Detta förutsätter att styrande dokument, rutiner, riskanalyser, åtgärdsplaner och uppföljning är dokumenterade, spårbara och tillgängliga vid tillsyn.

MCFFS 2026:1 Föreskrift om anmälan och identifiering av väsentliga och viktiga verksamhetsutövare
Reglerar hur verksamhetsutövare som omfattas av cybersäkerhetslagen ska anmäla sin verksamhet till Myndigheten för civilt försvar. Föreskriften anger vilka uppgifter anmälan ska innehålla och hur verksamhetsutövaren ska identifieras och klassificeras som väsentlig eller viktig. Den fungerar därmed som den praktiska anmälnings- och identifieringsföreskriften till cybersäkerhetslagen.

MCFFS 2026:8 Föreskrifter om incidentrapportering och informationsskyldighet för väsentliga och viktiga verksamhetsutövare
Reglerar hur väsentliga och viktiga verksamhetsutövare ska rapportera betydande incidenter enligt cybersäkerhetslagen. Föreskriften anger vilka incidenter som är rapporteringspliktiga, hur rapporteringen ska gå till samt vilka uppgifter som ska lämnas och när. Den reglerar även verksamhetsutövarens informationsskyldighet vid betydande incidenter och betydande cyberhot.

Lagen (2022:482) om elektronisk kommunikation (LEK)
Ställer krav på att tillhandahållare ska kunna visa hur driftsäkerhet, tillförlitlighet och kontinuitet säkerställs. Dokumentation av nät, processer, incidenter och vidtagna åtgärder är en förutsättning för detta.

Post- och telestyrelsens föreskrifter och allmänna råd om skyddsåtgärder vid behandling av uppgifter och vid lagring av uppgifter för brottsbekämpande ändamål (2026:1)
Innehåller bestämmelser om skyddsåtgärder vid lagring och behandling av uppgifter enligt 8 kap. lagen om elektronisk kommunikation. Föreskrifterna omfattar krav på tekniska och organisatoriska säkerhetsåtgärder, åtkomstkontroll, loggning, skydd mot obehörig behandling samt säker lagring av uppgifter.

Post- och telestyrelsens föreskrifter och allmänna råd om den fredstida planeringen för totalförsvarets behov av elektroniska kommunikationer (2026:2)
Innehåller bestämmelser om fredstida planering för totalförsvarets behov av elektroniska kommunikationer enligt 1 kap. 11 § lagen om elektronisk kommunikation. Föreskrifterna ställer krav på systematisk kontinuitetsplanering, identifiering av kritiska verksamhetsdelar och resurser samt upprättande och underhåll av planer för verksamhet vid omfattande störningar, höjd beredskap och krig.

Post- och telestyrelsens föreskrifter och allmänna råd om utlämnande av uppgift som gäller brottslig verksamhet eller misstanke om brott (2026:3)
Innehåller bestämmelser om utlämnande av uppgifter som gäller brottslig verksamhet eller misstanke om brott enligt 9 kap. lagen om elektronisk kommunikation. Föreskrifterna reglerar bland annat organisatoriska och tekniska förutsättningar för utlämnande av uppgifter, tidskrav för utlämnande samt hantering av realtidsuppgifter till behöriga brottsbekämpande myndigheter.

Offentlighets- och sekretesslagen (2009:400) (OSL)
För kommunala och regionala verksamhetsutövare reglerar lagen hur handlingar ska hanteras, bevaras och skyddas. Dokumentförteckningen ska beakta vilka handlingar som är allmänna, sekretessbelagda eller skyddsvärda.

Dataskyddsförordningen (EU) 2016/679 (GDPR)
Ställer krav på dokumentation av behandling av personuppgifter, tekniska och organisatoriska skyddsåtgärder samt ansvarsfördelning. Dokumentförteckningen ska omfatta relevanta styrande och redovisande dokument kopplade till personuppgiftsbehandling.

Lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap (LEH)

Arbetsmiljölagen (1977:1160)

Arkivlagen (1990:782)
För offentliga verksamhetsutövare ställer lagen krav på att handlingar ska hållas ordnade, bevaras och vårdas så att rätten att ta del av allmänna handlingar, behovet av information för rättskipning och förvaltning samt forskningens behov tillgodoses.

Anm: Tidigare gällande föreskrifter och vägledningar från Post- och telestyrelsen avseende dokumentation och spårbarhet kan användas som vägledning i den mån de är förenliga med gällande regelverk och kraven enligt cybersäkerhetslagen.

Det saknas specifika krav på innehållet i bilagor eller processbeskrivningar.

Framtagna processer kopplat till riktlinjerna
Rekommenderade processer för säkerställandet av viktiga funktioner.

Processer
Process för förändring i Telenät och Teletjänster
Process för problemhantering
Process för incidenter
Process för integritetsincidenter
Process för kontinuitet

Roller och ansvar
HUKI (Huvudansvarig/Beslutsfattare, Utförare/Uppdrags- och underlagsansvarig, Konsulteras, Informeras)

Rekommendation till egenframtagna planer och rutiner
Dessa planer och rutiner är viktiga för införandet av riktlinjerna och tas fram genom workshops i Verksamhetsutövarens organisation.

Verksamhetsbeskrivning

Planer

Verksamhetsplan
Åtgärdsplan för hantering av redundans avseende förbindelser för kritiska tillgångar.
Åtgärdsplan för hantering av reservkraft för kritiska tillgångar.
Underhållsplan(er)
Plan för riskanalyser
Kommunikationsplan leverantörer
Plan säkerhetsrevisioner kritiska anläggningar.
Kontinuitetsplan
Åtgärdsplan kontinuitet.
Katastrofplan
Revisionsplan Cybersäkerhet
Kontinuitetsplan extraordinära händelser, höjd beredskap och krig
Plan för samverkan med PTS

Rutiner

Rutin för uppdatering mjukvara inkl. testprotokoll
Rutin för Riskbedömning och återställning mjukvara
Anskaffningsrutin
Rutin för intern incidentrapportering.
Rutin för incidentrapportering till myndigheter
Rutin för intern integritetsrapportering.
Rutin för integritetsrapportering till myndigheter.
Rutin för riskrapportering
Rutin för säkerhetskopiering av behandlade uppgifter och nätdata
Rutin för säkerhetskopiering av uppgifter för brottsbekämpande ändamål
Rutin för hantering av loggar.
Rutin för hantering av kryptering och kryptonycklar.
Rutin för incidentinformation till användare
Rutin för tilldelning, ändring och uppföljning av tilldelade behörigheter
Rutin för åtkomst och behörighet till uppgifter för brottsbekämpande ändamål.'
Rutin för tillträde till anläggningar.

3 Standarder och ramverk

1. ETSI TS 102 232 1-7

Innehåll: Beskriver hur operatörer tekniskt ska leverera avlyssningsdata (Lawful Interception, LI) till brottsbekämpande myndigheter.

Användning: Standardserien används i många europeiska länder för att säkerställa att operatörer kan uppfylla lagkrav på hemlig avlyssning och utlämning av trafikdata på ett standardiserat sätt.

2. ETSI TS 102 657

Innehåll: Definierar ett standardiserat gränssnitt för överföring av lagrade trafikdata från operatörer till myndigheter.

Användning: Används i samband med lagkrav på datalagring och utlämning av trafikuppgifter, t.ex. enligt europeiska regler om data retention och nationell lagstiftning. Det gäller alltså inte avlyssning i realtid, utan historiska uppgifter som operatören är skyldig att lagra.

3. ISO/IEC 27001: Information Security Management Systems (ISMS)

Innehåll: Standard för att hantera informationssäkerhet. Fokus ligger på att skydda informationstillgångar genom att identifiera och hantera säkerhetsrisker.

Användning: Implementering av säkerhetsåtgärder och kontroller för att skydda data och informationssystem mot hot.

Fördelar: Ökar säkerheten för känslig information, vilket är kritiskt för nätverksintegritet och kunddata.

4. ISO 27031: Guidelines for Information and Communication Technology Readiness for Business Continuity

Innehåll: Standard med riktlinjer för att säkerställa att IT-system och digital infrastruktur kan stötta affärskontinuitet.

Användning: Hanterar aspekter som riskhantering, återställning av system och säkrade datanätverk.

Fördelar: Ökar säkerheten i IT-systemen som är kritiska för funktion och tillgänglighet.

5. ISO/IEC 22301: Business Continuity Management Systems (BCMS)

Innehåll: Standard för kontinuitetshantering. Fokus på att identifiera hot mot verksamheten och etablera planer för att hantera dem.

Användning: Utveckla, implementera och underhålla kontinuitetsplaner för att minimera avbrott i tjänsterna.

Fördelar: Säkerställer att verksamheten kan återhämta sig från störningar och fortsätta operera effektivt.

6. ITIL: Information Technology Infrastructure Library

Innehåll: Ramverk för IT-tjänstehantering med fokus på att förbättra effektiviteten och kvaliteten i IT-tjänster.

Användning: Implementera ITIL-principer för att hantera IT-tjänster genom livscykelhantering och processförbättring.

Fördelar: Förbättrar tjänsteleverans och support genom bästa praxis för hantering av IT-tjänster.

7. NIST Cybersecurity Framework

Innehåll: Riktlinjer för hantering av cybersäkerhetsrisker. Fokus på identifiering, skydd, detektion, respons och återhämtning.

Användning: Implementera NIST-ramverket för att stärka cybersäkerheten och hantera hot mot telekominfrastrukturen.

Fördelar: Förbättrar säkerheten och förmågan att hantera och återhämta sig från cyberattacker.