Avtal om Teletjänster i Öppet Nät TLA25

Bilaga 3.3

Tjänstespecifikation Säkerhet och incidenthantering

Version 1.0

Juni 2025

STADSNÄTS FÖRENINGEN

Innehållsförteckning

Inledning

Denna bilaga beskriver säkerhetskraven samt rutiner för incident- och problemhantering kopplat till TLA25-avtalet. Dokumentet baseras på Lagen (2022:482) om elektronisk kommunikation (LEK) samt Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2022:11), vilka trädde i kraft den 1 augusti 2022. Syftet med bilagan är att tydliggöra ansvarsförhållanden och skapa gemensamma riktlinjer mellan KO (Kommunikationsoperatör) och TL (Tjänsteleverantör) för effektiv hantering av säkerhetsincidenter och kontinuerligt säkerhetsarbete.

Säkerhetsarbetet och incidenthanteringen ska även ta hänsyn till krav som framgår av den nya Cybersäkerhetslagen (CSL) och NIS2-direktivet, vilket innebär ett ökat fokus på proaktiv hantering, riskbedömningar samt krav på incidentrapportering och kontinuitet i samhällsviktiga tjänster. KO och TL ansvarar gemensamt för att dessa krav efterlevs i enlighet med aktuell lagstiftning och riktlinjer.

1. Allmänt Säkerhetsarbete

1.1 Tekniska och organisatoriska säkerhetsåtgärder

Alla aktörer i leveranskedjan förväntas genomföra både tekniska och organisatoriska åtgärder för att minimera risker.

Det innefattar:

- Proaktiv riskhantering och sårbarhetsanalyser
- Upprättande av skyddsåtgärder för nätkomponenter och stödsystem
- Åtgärder för att säkerställa konfidentialitet, integritet och tillgänglighet i informationshanteringen
- System för incidentdetektion, övervakning och loggning
- Kontinuitetsplanering och övning av krishantering
- Tillämpning av principer för minst privilegium och separation av roller

1.2 Ansvarsfördelning

KO och TL ansvarar för att säkerhetskraven uppfylls inom sina respektive delar av leveransen. Detta kräver:

- En tydlig ansvarsfördelning dokumenterad mellan parterna
- Upprättande av kontaktvägar och samarbetsformer
- Regelbundna möten och informationsutbyten vid säkerhetsincidenter
- hantering av beroenden, särskilt vid användning av tredjepartsleverantörer

2. Incidenthantering

2.1 Definition och klassificering av säkerhetsincidenter

En säkerhetsincident definieras som en oplanerad händelse som leder till, eller riskerar att leda till, ett avbrott eller en negativ påverkan på tillgängligheten, riktigheten, konfidentialitet eller autenticiteten i ett kommunikationsnät eller tjänst.
Incidenter delas in i:

- Mindre incidenter som hanteras internt
- Betydande incidenter som uppfyller tröskelvärden enligt p(2.2 och ska rapporteras till PTS

2.2 Rapportering till PTS

Om en incident har haft betydande påverkan ska PTS underrättas utan onödigt dröjsmål och senast tre dagar efter att incidenten har upptäckts.

Rapporteringen sker via den blankett som finns på PTS webbplats: https://pts.se/internet-och-telefoni/rappportera-incident-till-pts/rapportera-sakerhetsincident

Tröskelvärden för betydande påverkan definieras enligt PTSFS 2022:11:

- Fler än 10 000 användare påverkas
- Incidenten pågår i över 8 timmar
- Ett större geografiskt område påverkas
- Det sker påverkan på samhällsviktiga funktioner

Det är alltid KO:s och TL:s gemensamma ansvar att bedöma incidentens påverkan och säkerställa att rapportering sker enligt gällande regelverk.

2.3 Incidenter hos leverantörer och följdincidenter

Om incidenten beror på en tredjepartsleverantör, eller får följdverkningar hos andra parter i kedjan, måste det ändå rapporteras. Leverantörens ansvar undantar inte KO eller TL från rapporteringsskyldigheten.

3. Felavhjälpning & problemhantering

3.1 Syfte och Omfattning

Problemhanteringsprocessen har två huvudsakliga mål:

- Minska återkommande incidenter genom att identifiera grundorsaker
- Begränsa effekten av incidenter som inte omedelbart kan lösas

Den omfattar både proaktiv och reaktiv hantering av problem:

- Reaktiva problem uppstår vid incidenter som inte kan lösas direkt
- Proaktiva problem identifieras genom trendanalys, observation eller extern information

3.2 Metodik

Problemhanteringen ska ske genom en metod för systematisk problemlösning som säkerställer tydlighet och konsekvens. För att stödja en effektiv analys ska följande frågeställningar alltid besvaras i varje problemärende:

- Vem påverkas av problemet? (t.ex. användargrupp eller funktion)
- Vad exakt är problemet? (tydlig beskrivning av symptom)
- Var och när uppstår problemet? (geografisk plats, teknisk komponent och tidpunkt)
- Vilka konsekvenser uppstår till följd av problemet? • Varför är det viktigt att lösa problemet?
- Vilka potentiella orsaker kan finnas? (identifiera och dokumentera samtliga rimliga orsaker)

Det är viktigt att dokumentera alla slutsatser noggrant så att problemlösningen blir transparent och möjlig att följa upp.

3.3 Processöversikt

Problemhanteringsprocessen ska genomföras stegvis enligt följande strukturerade flöde:

- Registrering och verifiering av problemärendet
- Klassificering av problem: Reaktivt (akut) eller Proaktivt (förebyggande)
- Analys av grundorsak
- Val av hanteringsstrategi:
    1. Permanent lösning
    2. Temporär lösning (Workaround)
    3. Ingen åtgärd
- Implementering och verifiering
- Stängning och uppföljning

3.4 Roller och ansvar

- **Service Desk:** Registrering och första kontaktpunkt
- **Problem Manager:** Leder processen och koordinerar lösningar
- **Problemlösare:** Utför teknisk analys och lösningsförslag
- **Change Management:** Godkännande av förändringar

3.5 Hantering av lösningar

- Permanenta lösningar dokumenteras och införs via Change Management
- Temporära lösningar används för att mildra påverkan tills permanent lösning finns
- Beslut att avstå från åtgärd ska dokumenteras med motivering och riskanalys

3.6 Stängning och uppföljning

Inkluderar uppdatering av dokumentation, verifiering av åtgärder och sammanställning av lärdomar. Erfarenhetsåterföring sker regelbundet.

4. Begrepp och definitioner

Begrepp	Definition
Change Management	En kontrollerad process för att hantera förändringar i nätet och tjänsternas miljöer.
Incident	En oplanerad händelse som leder till eller riskerar att leda till störning i en tjänst eller ett nät.
Problem	Den underliggande orsaken till en eller flera incidenter.
Proaktivt problem	Identifiering och hantering av potentiella problem innan de orsakar incidenter.
Reaktivt problem	En incident som inte omedelbart kan lösas och kräver skyndsam hantering.
SPOC **Single point of contact**	En central kontaktpunkt som koordinerar aktiviteter och information.
Temporär lösning (Workaround)	En tillfällig lösning som minimerar påverkan från ett problem tills en permanent lösning implementerats.