Riktlinjer för säkerhet i telenät och teletjänster

Bilaga 2: Anvisning för säkerhetsincidenter

Ver. 1.2

TLP:CLEAR

STADSNÄTS FÖRENINGEN

INNEHÅLSFÖRTECKNING

1 Inledning 2
2 Syfte 2
3 Begrepp och definitioner 3
4 Roller och ansvarsfördelning 4
Roller och ansvarsfördelning 4
5 Tillämpning 6
5.1 Tar emot 6
5.3 Loggar ärendet i CRM (företagsspecifik) 6
5.4 Initial analys, kategorisering, dokumentation och rapportering av ärendet 7
5.5 Eskalering 8
5.6 Tilldelar 8
5.7 Fördjupad analys, analys av tidigare incidenter och kända fel 8
5.8 Utarbetar lösning, implementerar och dokumenterar lösning 8
5.9 Verifierar lösningen 8
5.10 Dokumenterar, Klarrapporterar och incidentrapporterar internt 9
5.11 Stänger ärende 9
6 Rapportering till myndighet 10
7 Uppföljningsmöte 10
8 Underlag till andra processer 10

1 Inledning

Detta dokument utgör ett förslag till utformning av en process för ett stadsnäts hantering av säkerhetsincidenter. Anvisningen beskriver hanteringen av en oplanerad händelse som lett till avbrott eller störningar i Telenät och Teletjänster eller vid en uppenbar risk för en sådan händelse.

Processen baseras på ITIL Incident Management och tillämpliga delar av Problem Management med beaktande av nedanstående krav:

PTSFS 2022:11, Kap. 13 § 1: Kräver att alla incidenter rapporteras internt.
PTSFS 2022:11, Kap. 17 § 1: Kräver att alla säkerhetsincidenter rapporteras.
CSL/NIS2: Kräver att incidenter rapporteras inom 24 timmar.

Lag (2006:544): Föreskriver åtgärder vid extraordinära händelser och incidenter.

2 Syfte

Processen ska säkerställa att alla säkerhetsincidenter identifieras, hanteras, dokumenteras och rapporteras internt och externt, till berörda parter och relevanta myndigheter på ett strukturerat sätt för att minimera påverkan och förbättra den övergripande säkerheten.

3 Begrepp och definitioner

Begrepp	Definition
Aktivitet	Lägsta nivån i processhierarkin. En serie logiskt samman- hängande handlingar som en person eller roll utför, utförs på ett sätt.
Delprocess	En delprocess är en logiskt avgränsad del av en huvudprocess, kan finnas på flera nivåer.
Funktionell eskalering (tilldelning)	När incidenten inkommit måste den tilldelas antingen till personer inom Servicedesk eller till personer i andra och tredje linjens support.
Hierarkisk eskalering	När det är fråga om en allvarlig incident eller där ärenden tar för lång tid, eskaleras ärenden till ansvarig roll som vidtar åtgärder.
Huvudprocess	Huvudprocesser är den högsta nivån av processer i en verksamhet. Kan vara både internt och externt värdeskapande.
Incident	En oplanerad händelse som leder till avbrott eller störning i en tjänst eller en reduktion av kvalitén av tjänsten eller en uppenbar risk att det blir en störning.
ITIL	IT Infrastructure Library (ITIL) är ett ramverk bestående av ”best practice” som beskriver olika IT- processer som kan realiseras inom en organisation för att få en hög kvalitet på IT-tjänsterna och för att effektivisera leveransen och supporten av tjänsterna.
Känt fel	Ett problem som har en känd grundorsak och en workaround
Process	En process är ett flöde av sammanhängande aktiviteter som skapar ett förutbestämt resultat. Processen har alltid kunder - interna eller externa.
Processansvarig (process manager)	En person utsedd av ledningen för att ansvara för att processen som helhet både är effektiv och ändamålsenlig.
Roll	En roll är knuten till en process. Varje roll har ansvar att leverera ett resultat i processen. En person kan inneha flera roller och samma roll kan innehas av flera personer.
Rollbeskrivning	En beskrivning av de roller som är knutna till processen. I roll-beskrivningen ingår att beskriva rollens ansvar och befogenhet.
SPOC	Utgör en Single Point of Contact ("SPOC") för kommunikation med kunder, personal och leverantörer.
Tjänstenivåavtal (SLA)	Service Level Agreement. En överenskommelse mellan en tjänsteleverantör och en kund.
Workaround	En åtgärd som har till syfte att minimera konsekvenserna av en incident eller ett problem där det ännu inte finns någon fullständig lösning.
Ärende	Ett ärende kan vara en incident men det kan också vara en beställning eller en förfrågan.

4 Roller och ansvarsfördelning

Roller och ansvarsfördelning

I detta avsnitt används begreppet (företagsspecifik) för att ange att rollen/funktionen är beroende av hur företaget väljer att organisera verksamheten.

- **Funktionen Servicedesk/Första linjens support (företagsspecifik)**

  Utgör en Single Point of Contact ("SPOC") för kommunikation med kunder, personal och leverantörer. Äger ärendet från det är mottaget till att det stängs, oavsett vad ärendet handlade om. Loggar, prioriterar, fördelar och eskalerar ärenden. Svarar för uppdatering, statushantering, informationshantering och slutligen återkoppling till kund.

  (Servicedesken kan också hantera flera olika uppgifter som hantering av kundförfrågningar, mottagning av förändringsbegäran, underhållsfrågor m.m. beroende på hur företaget valt att organisera verksamheten. Servicedesk/första linjens support är också första nivån i en hierarki av supportgrupper som är involverade i lösningen av en incident).

- **Andra linjens support**
  Den andra nivån av support i en hierarki av supportgrupper involverade i arbetet med att lösa incidenter och med att undersöka problem samt för att hantera beredskapsfunktionen.

- **Tredje linjens support**
  Tredje nivån i en hierarki av supportgrupper inblandade i lösningen av incidenter och utredningen av problem.

- **Incidentansvarig (Incident manager)**
  Incidentansvarig ansvarar för att:

  - Koordinera och driva arbetet vid stora eller allvarliga incidenter.
  - Säkerställa att alla berörda parter får relevant information. Informationen till kunderna prioriteras.
  - Rapportera incidenter till PTS i enlighet med föreskriften *PTSFS 2022:11*.
  - Utveckla och förvalta processen genom att planlägga och genomföra:
    - regelbundna översyner
    - identifiering av förbättrings- och anpassningsbehov
    - ledning och koordinering av arbetet med förbättringar och anpassning i samråd med Processägaren.
  - Dokumentera, publicera och kommunicera processen.
  - Utveckla och förvalta ärendehanteringsverktygen.
  - Bedöma bemanningsbehov för processen.

- Genomföra uppföljningsmöten för granskning av hanteringen av större och allvarliga incidenter.
- Utbilda medarbetare i supportorganisationen kring arbetet i ärendehanteringsprocessen

5 Tillämpning

Förtydligande av aktiviteter i Incident Management-processen

Se Bilaga 1, Process för säkerhetsincidenter.

5.1 Tar emot

Ärendet tas emot och identifieras.

5.2 Kontrollerar om det är ett pågående ärende

Kontrollerar om ärendet är pågående, kontrollerar status och informerar anmälaren om så är fallet.

5.3 Loggar ärendet i CRM (företagsspecifik)

Alla ärenden loggas i CRM (företagsspecifik). I loggningen ingår vem som är användare/kund, beskrivning av ärendet och tidpunkt för mottagningen av incidenten. Detta gäller oavsett om incidenten kommer in via servicedesk eller upptäcks inom driften.

Information som ska finnas med i ett ärende:

- Ärendenummer
- Kontaktperson och kontaktuppgifter
- Kategori av ärende
- Prioritering
- Datum och tid
- Ärendebeskrivning
- Status för ärendet

5.4 Initial analys, kategorisering, dokumentation och rapportering av ärendet

Initial analys

En initial analys görs för att få en så klar bild av incidenten, och hur den ska hanteras.

Kategoriserar

Ärendet kategoriseras i nät- och kundincidenter och efter upprättad lista över de tjänster som huvudsakligen berörs. Kategoriindelningen är viktig för att kunna generera olika typer av statistik.

Prioriterar

Prioritering av varje ärende görs efter vilken påverkan incidenten har på tjänsten, hur många kunder som berörs och tjänstenivåavtalen (Servicenivå) med dessa samt hur brådskande det är att lösa incidenten.

Liten incident	Begränsad incident	Stor incident	Allvarlig incident
≤ 5000 abonnenter eller ≤ 2 500 km² sammanhängande berört område eller ≤ 20 % kapacitetsbortfall	≥ 5 000 abonnenter eller ≥ 2 500 km² sammanhängande berört område eller ≥ 20 % kapacitetsbortfall	≥ 30 000 abonnenter eller ≥ 5 000 km² sammanhängande berört område eller ≥30 % kapacitetsbortfall	≥ 150 000 abonnenter eller ≥ 15 000 km² sammanhängandeberört område eller ≥ 50 % kapacitetsbortfall
Rapport till PTS enligt nedan vid ≥ 24 timmar **≥ 2000 abonnenter eller** **≥ 1 000 km² sammanhängande berört område eller** **≥ 10 % kapacitetsbortfall**	**Rapport till PTS vid ≥ 6 timmar**	**Rapport till PTS vid ≥ 2 timmar**	**Rapport till PTS vid ≥ 1 timmar**

Är det fråga om en stor eller allvarlig incident ska incidenten eskaleras (se avsnitt Eskalering).

Dokumenterar

Vid säkerhetsincidenter upprättas en förteckning/incidentlogg. Incidentloggen ska innehålla nedanstående uppgifter och kompletteras under processen:

- 1. datum då incidenten inträffade,
- 2. en beskrivning av incidenten,
- 3. uppskattat antal berörda abonnenter eller användare,
- 4. bedömda konsekvenser av incidenten,
- 5. orsak till att incidenten inträffade,
- 6. de åtgärder som vidtagits, och
- 7. referensnummer.

Loggen kompletteras succesivt under ärendets process.

Initial incidentrapportering

Ärendet rapporteras till interna intressenter i enlighet med *Rutin för intern incidentrapportering*.

Kontrollerar om det krävs rapportering till myndigheter. Vid behov rapportera enligt gällande föreskrifter och enligt *Rutin för extern incidentrapportering*.

5.5 Eskalering

När en incident bedöms som stor eller allvarlig ska ärendet direkt eskaleras till 2:a linjens support och överlämnas till Incidentansvarig som övertar ansvaret för att koordinera och driva arbetet till det är klarrapporterat.
Incidentansvarig kontaktar Service Continuity Manager för gemensam bedömning om, och när, krisledningsgruppen ska sammankallas.

All kommunikation och information om ärendets fortskridande går via incidentansvarig som säkerställer att alla berörda parter fått relevant information i enlighet med organisationens, Informationspolicy (företagsspecifik).
Informationen till användarna prioriteras.

5.6 Tilldelar

Är incidenten liten kan Service desk/Första linjens support tilldela ärendet till sig själv. Om Service desk/Första linjens support bedömer att incidenten inte kan hanteras inom Service desk/Första linjens ska den tilldelas Andra alternativt Tredje linjens support.

5.7 Fördjupad analys, analys av tidigare incidenter och kända fel

En fördjupad analys av felsituationen genomförs. Det ska göras en kontroll av om det finns tidigare beskrivna incidenter och deras lösningar eller information om kända fel samt information om workaround.
Kontrollera om det krävs en ändring av tilldelningsbeslutet.

5.8 Utarbetar lösning, implementerar och dokumenterar lösning

När en lösning har utarbetats ska den implementeras. Att dokumentera incidenten och åtgärden som genomförts för att lösa incidenten ger viktig information när nya incidenter kommer in och bidrar till att man då snabbt kan lösa dem. Uppdatera CRM (företagsspecifik).

5.9 Verifierar lösningen

Det ska göras en verifiering att lösningen fungerar. Metoden för verifiering dokumenteras i CRM-systemet

5.10 Dokumenterar, Klarrapporterar och incidentrapporterar internt

Dokumenterar

CRM (företagsspecifik) uppdateras och Incidentloggen uppdateras med de åtgärder som genomförts för att lösa incidenten för att kunna ge viktig information när nya incidenter kommer in. Detta bidrar till att man då snabbt kan lösa dem. Uppdatera dokumentationen.

Klarrapporterar

Ärendet klarrapporteras till Service desk/Första linjens support. Kundinitierade incidenter klarrapporteras i enlighet med kunden överenskomna rutiner.

Intern incidentrapportering

En incidentrapport upprättas och rapporteras till interna intressenter i enlighet med *Rutin för intern incidentrapportering*.

Problemanmälan

Om den underliggande orsaken till incidenten inte har identifierats/åtgärdats görs en anmälan till Problem Manager för vidare hantering.

5.11 Stänger ärende

Ärenden stängs av den funktion som har ansvarat för ärendet. Vid kundinitierade ärenden stämmer Service desk/Första linjens support av med Kunden att det är ok att stänga ärende. Incidentansvarig meddelas att ärendet är avslutat.

6 Rapportering till myndighet

Att alla inträffade säkerhetsincidenter dokumenteras/kompletteras och rapporteras till myndigheter Rutin för rapportering av säkerhetsincidenter.

Ansvarig för incidentrapportering är incidentansvarig.

7 Uppföljningsmöte

Vid stor och/eller allvarlig incident ska ett uppföljningsmöte genomföras för att definiera orsaker till incidenten och för att fastställa och dokumentera åtgärder för att undvika framtida problem inom drabbat område.

8 Underlag till andra processer

Rapportering till processer som påverkats av incidenterna samt för kontinuitets- och kvalitetsuppföljning.