

## Rapportering av säkerhetsincident som har haft en betydande påverkan på allmänt tillgängliga elektroniska kommunikationsnät eller kommunikationstjänster

Rapportering av inträffade säkerhetsincidenter kan göras med hjälp av denna blankett till [incidentrapport@pts.se](mailto:incidentrapport@pts.se). Säkerhetsincidenter och rapportering av dessa regleras i 1 kap. 7 § och 8 kap. 3 § Lagen ([2022:482)](https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2022482-om-elektronisk-kommunikation_sfs-2022-482#K8) om elektronisk kommunikation (LEK) samt i 17 kap. Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster ([PTSFS 2022:11](https://www.pts.se/globalassets/startpage/dokument/legala-dokument/foreskrifter/internet/nya-lek/ptsfs-2022_11-om-sakerhet-i-nat-och-tjanster.pdf)). Föreskrifterna gäller från och med den 1 augusti 2022. Med blanketten avser PTS att underlätta för tillhandahållare att rapportera säkerhetsincidenter till myndigheten enligt lag och föreskrifter och skapa enkelhet, smidighet och likabehandling i incidenthanteringen vid PTS. För rapportering av integritetsincidenter finns en annan blankett och andra regler.

En inledande rapport ska vara Post- och telestyrelsen tillhanda inom 72 timmar från det att säkerhetsincidenten upptäcktes.

### Grundläggande uppgifter

|  |  |
| --- | --- |
| 1. Kontaktuppgifter och organisation[[1]](#footnote-2) | 1. Datum |
| 1. Ert referensnummer för ärendet | 1. PTS diarienummer (vid komplettering) |
| 1. Detta är en:   fullständig rapport (allt rapporteras på en gång och avses inte följas av fler rapporter)  inledande rapport (kommer att kompletteras)  kompletterande rapport (som kommer att kompletteras ytterligare)  kompletterande och slutlig rapport (avses inte att följas av fler rapporter) | |
| 1. Denna incident rapporteras även helt eller delvis som en integritetsincident. [[2]](#footnote-3) Ja  Nej | |
| 1. Vad var tillhandahållarens roll i samband med incidenten? [[3]](#footnote-4) | |
| 1. Säkerhetsincidenten haft betydande påverkan på nät eller tjänster.   Säkerhetsincidenten är av typen störning eller avbrott och har nått upp till PTS rapporteringströsklar.  Säkerhetsincidenten har medfört betydande påverkan på funktioner i samhället. | |
| 1. Önskas sekretess på uppgifter i rapporten? Ja  Nej   Om ja; sekretess önskas på grund av:  Affärspartners ekonomiska eller personliga förhållanden  Affärsförhållanden som kan antas skada bolaget om de offentliggörs  Driftsförhållanden som kan antas skada bolaget om de offentliggörs  Uppgift om säkerhets- eller bevakningsåtgärd om syftet med åtgärden motverkas om uppgiften röjs  Annat. Ange: | |

### Inledande rapport

|  |  |
| --- | --- |
| 1. När inträffade säkerhetsincidenten.[[4]](#footnote-5) | 1. När avhjälptes säkerhetsincidenten? |
| 1. Hur många aktiva anslutningar eller användare har drabbats av säkerhetsincidenten? | |
| 1. Ange berört geografiskt område, om det är relevant. [[5]](#footnote-6) | |
| 1. Vilka säkerhetsaspekter har berörts av säkerhetsincidenten?   tillgänglighet,  konfidentialitet,  riktighet  äkthet. | |
| 1. Vad har berörts av säkerhetsincidenten?   nät,  tjänster,  närliggande tjänster,  behandlade uppgifter  tillhandahållarens säkerhetsförmåga [[6]](#footnote-7) | |
| 1. Beskriv incidentens påverkan på nätet, tjänster eller funktioner i samhället. [[7]](#footnote-8) | |
| 1. Ange er preliminära bedömning av orsaken till säkerhetsincidenten. | |
| 1. Hur har säkerhetsincidenten påverkat berörda användare eller aktiva anslutningar? | |
| 1. Har säkerhetsincidenten medfört begränsningar i möjlighet till nödkommunikation? Ja  Nej | |

Tillhandahållaren ska lämna en kompletterande rapport till PTS inom två veckor från den dag då den inledande rapporten lämnats till PTS. Det går alltid bra att lämna samtliga uppgifter i en fullständig rapport inom 72 timmar från det att säkerhetsincidenten upptäcktes, genom att fylla i fält avsedda för kompletterande rapport även i en inledande rapport.

### Kompletterande rapport / fortsättning

|  |
| --- |
| 1. Om kompletterande rapport; Vad var orsakerna till säkerhetsincidenten? |
| 1. Vilken information har ni lämnat till allmänheten och/eller personer berörda av incidenten? När och hur lämnades informationen? |
| 1. Vad har ni gjort för att temporärt minska effekterna av säkerhetsincidenten? |
| 1. Vad har ni gjort för att avhjälpa de fel och brister som orsakade säkerhetsincidenten? När vidtogs de åtgärderna? |
| 1. Vad har ni gjort och/eller planerar ni att göra för att undvika att liknande säkerhetsincident inträffar igen? När vidtog ni dessa åtgärder eller när kommer planerade åtgärder att införas? |

**PTS behandling av personuppgifter**

PTS behandlar personuppgifter som inkommit inom ramen för incidentrapportering för att kommunicera och handlägga ärendet. Den rättsliga grunden för behandlingen är att behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i PTS myndighetsutövning.

För mer information om PTS personuppgiftsbehandling, se [Behandling av personuppgifter | PTS](https://pts.se/sv/om-pts/behandling-av-personuppgifter/)

Incidentrapporten skickas till [incidentrapport@pts.se](mailto:incidentrapport@pts.se).

1. Ange vem som är ansvarig tillhandahållare och en kontaktuppgift. Då handlingen är allmän lämnar PTS alltid ut kontaktuppgifter om någon begär att få ta del av handlingen. Ange därför bara uppgifter som kan lämnas ut. [↑](#footnote-ref-2)
2. Uppgiften behövs för att säkerställa att en och samma händelse som rapporterats till PTS enligt två olika regelverk för rapportering av säkerhetsincidenter respektive rapportering av integritetsincidenter handläggs samordnat. [↑](#footnote-ref-3)
3. Det är rollen i samband med incidenten som är central. T.ex. nätägare, internet- eller mobiltjänsteleverantör, kommunikationsoperatör, internetknutpunktsleverantör och/eller tillhandahållare av nummeroberoende interpersonella kommunikationstjänster, s.k. NI-ICS, m.fl. [↑](#footnote-ref-4)
4. Tillhandahållaren bör göra en uppskattning av tidpunkten för när säkerhetsincidenten har inträffat i de fall en exakt tidpunkt inte kan fastställas med stöd av system för övervakning eller loggning. Uppskattningen bör göras med utgångspunkt från kända fakta om incidenten. Ange om det är en uppskattning. [↑](#footnote-ref-5)
5. Berört område för kommunikationstjänster som tillhandahålls över mobila nätanslutningar bör normalt vara det sammanlagda täckningsområdet för berörda celler eller motsvarande i mobilnätet. [↑](#footnote-ref-6)
6. Med tillhandahållarens säkerhetsförmåga menas: Tillhandahållarens förmåga att motstå händelser som undergräver tillgängligheten, äktheten, riktigheten eller konfidentialiteten hos näten eller tjänsterna, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via era elektroniska kommunikationsnät eller elektroniska kommunikationstjänster, eller på er förmåga att motstå sådana händelser (se definitionen av säkerhetsincident i 1 kap 7 § LEK). [↑](#footnote-ref-7)
7. ENISA har lämnat följande exempel på påverkan på ekonomisk och samhällelig verksamhet (eller på funktioner i samhället enligt uttrycket i prop. 2021/22:136). Det kan vara att incidenten har skapat:

   1. Påverkan på möjligheten att nå 112 eller nationell nödkommunikation (national emergency numbers)
   2. Påverkan på public warning systems
   3. En hög risk för allmänhetens säkerhet (public safety and public security), för liv, höga kostnader, stor materiell förstörelse (ryktesskador, påverkan på moral, dataförlust för konsumenter och påverkan på produktivitet)
   4. Mediapublicering
   5. Påverkan på kontinuiteten hos essentiella tjänster (NIS-begrepp) eller kritiska sektorer eller operatörer
   6. Påverkan under särskilt kritiska dagar som till exempel valdagar eller dagar för folkomröstning
   7. Påverkan på kritiska funktioner i samhället som till exempel regeringen eller myndigheter m.fl.
   8. Högprofilerade användare har berörts av incidenten som till exempel politiska personer eller statsminister.

   (Se ENISA *Technical guideline for incident reporting under EECC)* [↑](#footnote-ref-8)