

Regleringsbrevsuppdrag Rapportering it-incidenter

Övergripande beskrivning av Pensionsmyndighetens
processer och rutiner kring it-incidenter



PENSIONS
MYNDIGHETEN

Innehåll

1.	Inledning	1
2.	Övergripande beskrivning.....	1

Sammanfattning

Pensionsmyndigheten har väl fungerande processer och rutiner för att identifiera och rapportera it-incidenter i enlighet med 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, vilket redovisas nedan.

1. Inledning

Enligt regleringsbrevet för 2021 ska Pensionsmyndigheten kortfattat och övergripande redovisa processer och rutiner för att identifiera och rapportera it-incidenter.

2. Övergripande beskrivning

Pensionsmyndighetens it-avdelning ansvarar för och hanterar en stor mängd olika typer av it-incidenter (inklusive it-säkerhetsincidenter) enligt en fastställd it-incidenthanteringsprocess med tillhörande rutiner.

It-incidentprocessen omfattar även våra externa leverantörer / samverkanspartners och regleras i avtal eller skriftliga överenskommelser.

Arbetet startar i och med att en it-incident har rapporterats eller har upptäckts.

Myndigheten har speciellt utpekade incident managers (IM) för att driva och samordna it-incidenter. Vid en kritisk it-incident sammankallar IM representanter från berörda avdelningar och områdesansvariga för att hantera it-incidenten. IM samordnar även löpande avstämningar för återkoppling och uppföljning av rapporterade it-incidenter.

It-avdelningen ansvarar även för att hantera it-säkerhetsincidenter i enlighet med it-avdelningens it-incidentprocess. Alla medarbetare som upptäcker något som avviker från det normala och kan bedömas som en it-säkerhetsincident ska skyndsamt informera it-säkerhetsenheten om detta, för beslut om vidare hantering. It-säkerhetsenheten ansvarar för bedömning och hantering av incidenten.

Utifrån vad som har inträffat görs en första bedömning för att identifiera vem som ansvarar för it-incidenten och allvarlighetsgrad av det som inträffat. En fördjupad analys påbörjas parallellt med att identifiera åtgärder. It-incidenterna dokumenteras i myndighetens ärendehanteringssystem.

Efter analys av vad som hänt vidtas åtgärder för att lösa it-incidenten. Åtgärderna kan bestå av både administrativa och tekniska aktiviteter beroende på vad som hänt och vad/vem/vilka som berörs.

Efter prioritering informeras de intressenter som berörs. Under it-incidentarbetet informeras intressenterna kontinuerligt för att de ska kunna vidta egna åtgärder om det behövs.

Utifrån den fördjupade analysen identifieras eventuellt ytterligare åtgärder som kan behöva vidtas.

Berörda verksamheter vidtar beslutade åtgärder för att säkerställa att liknande incidenter inte ska uppstå igen.

Som en del av ordinarie process för it-incidenter ska it-avdelningen rapportera och hantera it-incidenter enligt överenskommelse med

avdelningen för myndighetsstyrning och stöd/säkerhetsenheten (MSS/SÄK). MSS analyserar incidenten tillsammans med IM samt it-säkerhetsenheten och därefter rapporterar MSS incidenten till MSB, om den uppfyller kriterierna för rapportering. I annat fall hanteras den internt på myndigheten.

Vid en eventuell brottsmisstanke görs en polisanmälan av det inträffade.

Vid större it-incidenter (kritiska) görs en it-incidentrapport som sprids till berörda intressenter. Efter större it-incidenter utvärderas händelsen i syfte att möjliggöra en förbättrad hantering och förebyggande arbete (ständiga förbättringar).

www.pensionsmyndigheten.se

