Informationssäkerhet

Svar på regeringsuppdrag

PENSIONS
MYNDIGHETEN

Innehåll

Sammanfattning

Pensionsmyndighetens verksamhet är både samhällsviktig och har betydelse för Sveriges säkerhet. Målet för säkerhetsarbetet är att Pensionsmyndigheten ska ha en väl avvägd och riskbaserad säkerhetsnivå. Myndigheten värnar om kundernas förmåner och integritet, medarbetarnas trygghet och skyddar våra tillgångar.

Det övergripande målet för säkerhetsarbetet är att Pensionsmyndigheten har en väl avvägd och riskbaserad säkerhetsnivå.

Pensionsmyndighetens säkerhetsarbete styrs genom ett säkerhetsledningssystem som består av ett antal processer och rutiner, organisation och ett säkerhetsregelverk. Ledningssystemet är baserat på internationella standarder, *ISO/IEC 27001 Ledningssystem för informationssäkerhet - krav* och *ISO/IEC 27002 Riktlinjer för informationssäkerhetsåtgärder*.

Pensionsmyndigheten arbetar aktivt med styrning och uppföljning inom informationssäkerhet och anpassar våra processer för att fungera i det agila arbetssätt som myndigheten infört. Genom att delta i Myndigheten för samhällsskydd och beredskaps (MSB) uppföljningsmodell Infosäkkollen[1] kan myndigheten följa upp det systematiska informationssäkerhetsarbetet.

Idag arbetar 70 % av myndighetens medarbetare på distans vanligast 3 dagar per vecka, så kallat hybridarbete. Myndigheten har tekniska lösningar och tydliga säkerhetsregler som möjliggör hybridarbete med motsvarande säkerhetsnivå.

Med anledning av Rysslands invasion av Ukraina 2022 fick området civilt försvar mycket uppmärksamhet både internt och i samhället samt inom politiken. Sedan den 1 oktober 2022 är Pensionsmyndigheten beredskapsmyndighet[2] vilket innebär att myndigheten har särskild betydelse för samhällets civila beredskap och ska ha god förmåga att motstå hot och risker, förebygga sårbarheter, hantera fredstida krissituationer och kunna genomföra sina uppgifter vid höjd beredskap.

Pensionsmyndigheten har en grundläggande beredskap och förmåga att hantera incidenter, störningar, kriser och höjd beredskap. Myndigheten vidareutveckla arbetet med civil beredskap genom att vidta ett antal riskreducerande åtgärder exempelvis utbildningar och övningar som stärker myndighetens krishanteringsförmåga, robusthöjande åtgärder för kritiska it-tjänster och åtgärder för säkra kommunikationer.

[1] https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/infosakkollen/

[2] Förordning (2022:524) om statliga myndigheters beredskap

1. Inledning

Säkerhet är viktigt för det offentliga Sverige och en förutsättning för att kunna fullt ut tillvarata de effekter som digitaliseringen kan ge vårt samhälle. Pensionsmyndigheten stödjer en bredare samverkan inom säkerhetsområdet som kan skapa långsiktiga förutsättningar för att höja nivån av säkerhet inom statsförvaltningen.

Pensionsmyndigheten har sedan en längre tid ett fungerande systematiskt informationssäkerhetsarbete. Processer är på plats med definierade roller och ansvar samt tydliga rapporteringsvägar som även anpassas för att fungera i det agila arbetssättet, vilket är en förutsättning för att lyckas med informationssäkerheten.

Pensionsmyndigheten utvecklar och prövar innovativa lösningar för att effektivisera vår verksamhet och förbättra vår service till medborgare.

1.1. Uppdraget

Pensionsmyndigheten ska redogöra för hur myndigheten har arbetat för att förvalta och utveckla sin informationssäkerhet och hur myndigheten planerar för att möta framtida behov. Pensionsmyndigheten ska särskilt redogöra för:

- åtgärder som myndigheten har vidtagit för att utveckla den interna styrningen och uppföljningen av informationssäkerhetsarbetet,
- hur medarbetarnas arbete på distans påverkar informationssäkerheten och om åtgärder för att hantera identifierade risker har vidtagits,
- om en analys har gjorts av om hot och sårbarheter för myndigheten har förändrats i och med det rådande omvärldsläget, samt om åtgärder har vidtagits eller planerats för att minska eventuella identifierade risker med anledning av detta.

1.2. Avgränsningar

Redovisningen innehåller inte analyser eller åtgärder som våra leverantörer eller samverkansparter har vidtagit, utan redovisningen avser det arbete som sker inom Pensionsmyndigheten.

2. Förvaltning och utveckling av informationssäkerhet

Pensionsmyndigheten förvaltar och utvecklar informationssäkerheten och planerar för att möta framtida behov. Pensionsmyndigheten har funnits i tretton år och bildandet av myndigheten föregicks av Pensionsmyndighetsutredningen (S 2008:05). Från myndighetens start har

det funnits ett beslutat säkerhetsledningssystem, bestående av internt styrande dokument för säkerhet och en genomförd säkerhetsskyddsanalys. Ett systematiskt arbetssätt för säkerhet som inkluderar informationssäkerhet inleddes vid myndighetens bildande.

En god informationssäkerhet är en förutsättning för att Pensionsmyndigheten ska kunna utföra sitt uppdrag vilket i huvudsak är att administrera och betala ut den allmänna pensionen, att ge pensionssparare och pensionärer en samlad bild av och korrekt information om hela pensionen samt att stärka pensionssparares och pensionärers ställning som konsumenter.

Myndighetens verksamhet är helt beroende av digitala lösningar och verksamhetssystemen lagrar och behandlar information om drygt 8 miljoner personer.

Målet för säkerhetsarbetet är att Pensionsmyndigheten ska ha en väl avvägd och riskbaserad säkerhetsnivå. Myndigheten värnar om kundernas förmåner och integritet, medarbetarnas trygghet samt skyddar våra tillgångar.

2.1. Säkerhetsledningssystemet

Säkerhetsarbetet vid Pensionsmyndigheten är riskbaserat och utgår från verksamhetens behov, författningskrav, avtal, interna regler och rådande hotbilder. Säkerhetsarbetet är en viktig del i Pensionsmyndighetens övergripande arbete med intern styrning och kontroll. Grunden i Pensionsmyndighetens systematiska säkerhetsarbete är att sträva efter ständig förbättring, vilket sker genom att årligen följa upp, mäta effekterna av säkerhetsledningssystemet och rapportera till ledningen läget samt föreslå och implementera förbättringar.

Pensionsmyndigheten styr och leder säkerhetsarbetet genom ett säkerhetsledningssystem som innefattar alla aspekter av säkerhet inklusive informationssäkerhet. Det ger myndigheten en sammanhållen bild av säkerhetsarbetet och de processer och rutiner inom säkerhetsarbetet som ingår i en större helhet. Säkerhetsledningssystemet omfattar alla organisatoriska delar vid alla myndighetens verksamhetsorter och är en del av myndighetens totala ledningssystem. I myndighetens strategiska plan[3] beskrivs att *Pensionsmyndigheten ska ha en god myndighetsförvaltning och vara en välskött, rättssäker och effektiv myndighet med högt förtroende och starkt medborgarfokus.* En del av det uppdraget är att *vår verksamhet har en väl avvägd och riskbaserad säkerhetsnivå.*

Säkerhetsledningssystemet baseras på standarderna *ISO/IEC 27001 Ledningssystem för informationssäkerhet – krav* och *ISO/IEC 27002 Riktlinjer för informationssäkerhetsåtgärder*. Pensionsmyndigheten följer MSB:s föreskrifter (MSBFS 2020:6) och allmänna råd om statliga myndigheters informationssäkerhet.

[3] Pensionsmyndighetens strategiska plan 2023 och framåt, PID283284

2.2. Ansvar inom säkerhet

Alla medarbetare har ett ansvar för säkerheten i Pensionsmyndigheten. För att nå målen för säkerhet är engagemang från myndighetens ledningsgrupp, chefer och medarbetare en förutsättning.

- Styrelsen beslutar den övergripande inriktningen för säkerhetsarbetet genom myndighetens säkerhetspolicy. Styrelsen ska hålla sig informerad om säkerheten vid myndigheten.
- Generaldirektören har det yttersta ansvaret för säkerheten i den löpande verksamheten inom myndigheten. I övrigt följer ansvaret för säkerheten det ordinarie verksamhetsansvaret.
- Verksamhetsansvarig chef ansvarar för att
    - den beslutade säkerhetsnivån som anges i säkerhetsregelverket införs och upprätthålls inom den egna verksamheten
    - korrigera brister som påverkar säkerheten inom den egna verksamheten. Det kan till exempel vara brister i informations-hantering, förändringar av behörigheter för medarbetare
    - hantera säkerhetsincidenter.
- En del roller inom myndigheten ingår säkerhetsansvar med tillhörande arbetsuppgifter, exempelvis för vissa roller inom det agila arbetssättet.
- Medarbetare på alla nivåer har ett ansvar för att följa regler, genomgå läraktiviteter i säkerhet samt att vara uppmärksamma på och rapportera säkerhetsbrister och säkerhetsincidenter till närmaste chef eller säkerhetsenheten.
- Vid Pensionsmyndigheten finns särskilda befattningar som inrättats till följd av lag eller annan förordning. Pensionsmyndighetens säkerhetsskyddschef är en sådan befattning. Säkerhetsskyddschefen lyder administrativt under avdelningen för myndighetsstyrning och stöd, men rapporterar i säkerhetsskyddsärenden direkt till generaldirektören.

2.2.1. Organisation av säkerhetsarbetet

I myndighetens arbetsordning[4] framgår att det finns två avdelningar med bestämmande ansvar inom säkerhet, avdelningen för myndighetsstyrning och stöd samt it-avdelningen. På dessa respektive avdelningar finns enheter med specialistkompetens inom säkerhetsområdet.

Säkerhetsenheten (avdelningen för myndighetsstyrning och stöd)

Chefen för säkerhetsenheten är Pensionsmyndighetens säkerhetschef och säkerhetsskyddschef. Enheten har det övergripande ansvaret för styrningen av säkerhetsarbetet, säkerhetsledningssystemet och rapporterar säkerhetsläget till myndighetens ledning.

[4] Arbetsordning för Pensionsmyndigheten, VER 2021-126

Säkerhetsenheten ansvarar för informationssäkerhet, personsäkerhet, fysisk säkerhet, internutredningar, säkerhetsskydd, kontinuitetsplanering samt civil beredskap på Pensionsmyndigheten.

It-säkerhetsenheten (it-avdelningen)

It-säkerhetsenheten ansvarar för att ta fram, etablera och underhålla det regelverket inom it-säkerhet. Enheten ansvarar även för att säkerställa att it-säkerhetskraven beaktas och upprätthålls inom ramen för Pensionsmyndighetens säkerhetsledningssystem, till exempel inom utvecklingsprojekt, förvaltning och servicenivåavtal. It-avdelningen har ett bestämmande, samordnade och uppföljande ansvar inom löpande behörighetshantering, identitets- och åtkomsthantering (IAM), samt it-säkerhet. Chefen för it-säkerhetsenheten är Pensionsmyndighetens it-säkerhetschef.

Även om det bestämmande ansvaret är fördelat mellan de två avdelningarna med tillhörande enheter, finns ett samarbete som sker på strategisk nivå i frågor som rör styrning av säkerhet, samverkan och ansvarsfördelning, på taktisk nivå exempelvis vid utformning av styrande dokument, processer och rutiner samt även på operativ nivå där representanter från båda enheterna deltar i upphandlingar, riskanalyser, konsekvensbedömningar, informationsklassning, utvecklingsinsatser med mera.

Pensionsmyndighetens internrevision har under 2022 genomfört en granskning ”Säkerhet i it-nätverk”[5] som bland annat har identifierat att ansvarsfördelningen mellan säkerhetsenheten och it-säkerhetsenheten behöver tydliggöras ytterligare. Myndigheten har inlett arbetet för att tydliggöra ansvarsfördelningen.

2.3. Säkerhetsregelverket

Pensionsmyndigheten har styrande dokument som reglerar verksamheten och

- preciserar myndighetens uppdrag och de externa regler och krav som myndigheten ska förhålla sig till och reglerar utförandet av verksamheten
- säkerställer att verksamheten bedrivs effektivt och rättssäkert
- klargör vem som gör vad och vem som ska fatta vilka beslut, samt
- ser till att vi hushåller med statens medel.

De styrande dokumenten ska tillsammans bilda en sammanhängande struktur för styrning och uppföljning av myndighetens verksamhet. Inom Pensionsmyndigheten delas de styrande dokumenten in i styrande regeldokument (verksamhetsregler och rättsliga regler) och styrande planeringsdokument.

[5] Internrevisionens granskning av säkerhet i it-nätverk, VER 2022-290

Pensionsmyndighetens säkerhetsregelverk, där den beslutade säkerhetsnivån och säkerhetsregler framgår, är en del myndighetens regelverk.

Säkerhetsegelverket består av i huvudsak styrande regeldokument (verksamhetsregler) på fyra nivåer policy, riktlinjer, anvisningar och rutinbeskrivningar indelade efter syfte. I dagsläget finns ca 30 styrande regeldokument (verksamhetsregler) inom områdena informationssäkerhet, it-säkerhet, krisberedskap, civilt försvar, personsäkerhet och fysisk säkerhet. De styrande regeldokumenten är utgivna av antingen avdelningen för myndighetsstyrning och stöd (säkerhetsenheten) eller it-avdelningen (it-säkerhetsenheten).

Genom att ha ett strukturerat säkerhetsregelverk kan myndigheten arbeta mer effektivt med säkerhet. Det är transparent för organisationen vilken nivå av säkerhet som gäller vid myndigheten och återkommande frågor inom säkerhetsområdet kan ofta besvaras genom att beskriva säkerhetsnivån i regelverket.
Säkerhetsregelverket uppdateras och anpassas löpande exempelvis för att hantera myndighetens säkerhetsrisker, förändringar i hotbild och omvärld, lagstiftning eller uppdrag, verksamhetsbehov och för att säkerställa att myndigheten har en väl avvägd säkerhetsnivå. Myndigheten har en väl fungerande process för att genomföra förändringar i regelverket.

2.4. Säkerhetsmedvetande

Säkerhetsarbetet är inriktat mot att skapa ett högt allmänt säkerhetsmedvetande inom hela Pensionsmyndigheten. Myndigheten genomför olika aktiviteter som syftar till att öka medarbetarnas säkerhetsmedvetande för att skapa en god säkerhetskultur. Med säkerhetskultur menas ett gemensamt tanke-, beteende- och värderingsmönster som kan påverka myndighetens säkerhet. Säkerhetsmedvetande i sig är en ständigt pågående lärandeprocess.

Pensionsmyndigheten har ett övergripande program för ökat säkerhetsmedvetande[6] som knyter ihop aktiviteterna och som syftar till att säkerställa att alla väsentliga områden täcks. Genom programmet kan myndigheten mäta och få en samlad bild av medarbetarnas nivå av säkerhetsmedvetande. Några exempel på aktiviteter som genomförs är säkerhetsutbildningar, föreläsningar, artiklar på intranätet, krisberedskapsveckan (v39) och cybersäkerhetsmånaden (oktober).

Under senaste åren har Pensionsmyndigheten haft stort fokus på att öka säkerhetsmedvetenhet hos medarbetarna. Det har myndigheten gjort genom kommunikation, utbildningar och cybersäkerhetmånaden, där vi blandar föreläsningar, artiklar och tävlingar.

Som en bas i programmet för ökat säkerhetsmedvetande har Pensionsmyndigheten en webbaserad läraktivitet inom säkerhet som består av fem delar, där den första grundläggande läraktiviteten ”säkerhet för alla”

[6] Program för ökat säkerhetsmedvetande, SÄK 2019-99

är obligatorisk för samtliga medarbetare. Det finns också en it-säkerhetsutbildning som lanserades 2022 och även den är obligatorisk för samtliga medarbetare. Båda dessa läraktiviteter är återkommande och medarbetare ska genomföra dem minst vartannat år. Arbete pågår även med att lansera en utbildning kring it-säkerhet kopplat till applikationsutveckling.

Utöver basutbildningarna finns även rollspecifika påbyggnadsdelar för exempelvis chefer och SID-handläggare (Skyddad Identitet-handläggare).

Pensionsmyndigheten genomför också anpassade utbildningar och aktiviteter för särskilda målgrupper exempelvis inom it-avdelningen, bland annat

- en återkommande mognadsmätning som omfattar förmågor inom it-säkerhetsarkitektur. Detta är tänkt som stöd kring framtida investeringar och riskminimeringar.
- fortsatta insatser för att höja säkerheten i vår utvecklingsprocess (DevSecOps).
- riktad kommunikation kring exempelvis förändrad hotbild, patchning med mera.

Som en del i uppföljningen genomför myndigheten årligen en enkät om medarbetarnas säkerhetsmedvetande.

2.5. Hantering av säkerhetsrisker

Pensionsmyndigheten bedriver ett riskbaserat säkerhetsarbete, där hantering av säkerhetsrisker är en central del. Myndigheten har definierat säkerhetsrisk som möjligheten att ett givet hot utnyttjar sårbarheten hos en tillgång (information, produkt eller person) eller en grupp av tillgångar och därigenom påverkar Pensionsmyndighetens säkerhetsmål negativt.

Pensionsmyndigheten har en beslutad process för riskhantering[7] som är gemensam för samtliga riskkategorier och säkerhetsrisker är en delmängd av operativa risker. Enligt den processen är det riskägaren som tar ställning till om en risk ska accepteras eller om den ska hanteras. Beslutet om acceptans eller hantering av risk dokumenteras. Observera att när det gäller acceptans av säkerhetsrisker, eller vilken nivå av säkerhetsrisk myndigheten vill exponera sig för, inom verksamhet som omfattas av säkerhetsskydd ska riskägaren och säkerhetskyddschef vara överens. Om riskägaren och säkerhetsskyddschef inte är överens ska frågan om riskacceptans eller nivå av risk eskaleras till generaldirektören för beslut.

Riskhanteringsprocessen används för att identifiera, värdera, analysera, hantera och rapportera säkerhetsrisker inom hela verksamheten.

I myndighetens årliga verksamhetsplanering genomför varje avdelning riskanalyser för att identifiera risker inom ansvarsområdet samt risker utifrån de mål som definieras i samband med verksamhetsplaneringen.

[7] Riktlinje riskhantering VER 2020-350

Identifiering och bedömning av säkerhetsrisker ingår i avdelningarnas riskanalyser. Åtgärder för att hantera säkerhetsriskerna omhändertas i avdelningarnas verksamhetsplaner och följs upp i de fördjupande verksamhetsuppföljningarna.

2.6. Hantering av incidenter

Incidenthantering handlar om att identifiera svagheter och brister i myndighetens verksamhet som ger underlag till förbättringar. Hanteringen innefattar att rapportera, åtgärda och följa upp incidenter. Att förebygga att incidenter inträffar och mildra de potentiella konsekvenserna utgör en viktig del av Pensionsmyndighetens riskhantering och säkerhetsarbete.

Pensionsmyndigheten har fungerande verktygsstöd och processer för att hantera incidenter inom ramen för informationssäkerhet på myndigheten. En incident kan beröra flera områden i verksamheten och förutsätter intern samverkan vid hanteringen. Säkerhetsenheten har bestämmande ansvar för incidenthantering, men alla myndighetens avdelningar är delaktiga i hanteringen av incidenterna.

Pensionsmyndigheten har fungerande rutiner för hur vi rapporterar it-incidenter till MSB och följer MSB:s föreskrifter (MSBFS 2020:8) om statliga myndigheters rapportering av it-incidenter. Under 2023 har myndigheten uppdaterat styrande dokument inom incidenthantering och tagit fram informationsmaterial för de roller som agerar backup för myndighetens incident managers.

2.7. Informationstillgångar

Pensionsmyndighetens tillgångar ska vara identifierade, dokumenterade och det ska finnas en ansvarig chef eller funktion för respektive tillgång.

Information som en tillgång finns i alla delar av myndighetens verksamhet och kan beskrivas och förtecknas på olika sätt.

1. Pensionsmyndighetens arkiv utgörs av våra allmänna handlingar. Inköps-, fastighets- och arkivenheten ansvarar för myndighetens arkivredovisning och dokumenthanterings- och arkivbildningsplanen[8], som utgör en del av förteckningen över myndighetens informationstillgångar.
2. Pensionsmyndighetens registerförteckning[9] innehåller beskrivningar av de personuppgiftsbehandlingar som utförs och de databaser och register som används vid myndigheten. Förteckningen utgår huvudsakligen från de processer som finns i myndighetens klassificeringsstruktur och inkluderar även personuppgiftsbehandlingar som inte ingår i allmänna handlingar.

[8] Anvisning med bilaga, Dokumenthanterings- och arkivbildningsplan Dnr VER 2021-128

[9] Registerförteckning, VER 2023-26

Dataskyddsfunktionen ansvarar för utformning och förvaltning av myndighetens registerförteckning enligt dataskyddsförordningen.

3. Myndighetens diarieförda handlingar hanteras i ett ärende- och dokumenthanteringssystem, där inkomna och upprättade allmänna handlingar registreras i enlighet med offentlighets- och sekretesslagen (2009:400). I arkivbildnings- och dokumenthanteringsplanen framgår vilka handlingar som ska diarieföras. Inköps-, fastighets- och arkivenheten ansvarar för detta system.
4. Myndighetens centrala ärendehanteringssystem för handlingar i försäkringsärenden, vilka genom en bestämmelse i offentlighets- och sekretessförordningen (2009:641) är undantagna från registreringsskyldigheten i offentlighets- och sekretesslagen (2009:400).
5. I myndighetens gemensamma mappstruktur, samarbetsportal med mera lagras och behandlas information och handlingar som inte ska diarieföras i myndighetens diarieföringssystem. Närmaste chef ansvarar för att medarbetare behandlar information på korrekt sätt i de olika dokumenthanteringssystemen. Närmaste chef är ägare av de mappar och sidytor som deras medarbetare har skapat eller beställer.
6. Övrig information som lagras och hanteras i it-miljön

De största informationsmängderna inom Pensionsmyndigheten lagras och behandlas i it-system. Vissa av dem är förvaltade av Försäkringskassan. Myndighetens använder ett agilt arbetssätt inom verksamhetsutveckling med it, vilket även inkluderar förvaltning. Det agila arbetssättet bygger på ramverket Scaled Agile Framework (SAFe). Arbetet sker i en tvärfunktionell virtuell organisation, där medarbetare från olika delar av linjeorganisationen samarbetar över avdelningsgränser i agila leveranståg och team. Tågen är bestående grupperingar som ansvarar för både ny- och vidareutveckling och förvaltning av it-miljön.

För respektive tåg finns det en roll som har ett huvudansvar för säkerhet och även har ett risk- och informationsägarskap. Denna huvudansvariga roll ska, enligt arbetsordningen, antingen innehas av en avdelningschef (linje-organisation) eller av en särskild utsedd Business Owner (roll i det agila arbetssättet) där avdelningschefen har fördelat ansvar till Business Owner.

Pensionsmyndighetens internrevision har i granskningen ”säkerhet i it-nätverk” konstaterat att inget av myndighetens agila tåg hittills har utsett någon business owner som ansvarig för risk- och informationsägarskap. Det har påbörjats ett arbete för att genomföra och dokumentera delegering av ansvar gällande risk- och informationsägarskap

2.7.1. Informationsklassning av tillgångar i it-miljön

Informationsklassning är en metod[10] som myndigheten använder för att säkerställa att information har ett korrekt skydd i it-systemen i förhållande till dess värde för verksamheten. Om skyddet är fel dimensionerat kan det

[10] Anvisning informationsklassning, SÄK 2016-37

exempelvis leda till onödigt höga kostnader eller att information utsätts för en för hög risk.

Informationsklassning är en viktig del i att upprätthålla myndighetens beslutade säkerhetsnivå och myndigheten har arbetat systematiskt med informationsklassning sedan 2012. Metoden för informationsklassning består av fyra steg, värdering, avvikelseanalys, riskanalys och åtgärdsanalys som genomförs i workshopform.

Genom metoden kontrolleras att ett enskilt it-system har rätt nivå av säkerhet i förhållande till värdet hos informationen som behandlas i systemet. Myndigheten kan via metoden följa upp att de säkerhetsåtgärder som är tillämpbara är införda och fungerar. Att upprätthålla rätt nivå av säkerhet över lång tid är en utmaning och det finns nästan alltid en eller flera avvikelser som behöver åtgärdas. Utifrån genomförd informationsklassning identifieras dessa avvikelser med tillhörande risker och en åtgärdsplan upprättas för att korrigera avvikelserna och hantera riskerna. Under 2023 pågår ett arbete med att anpassa metoden för informationsklassning till det agila arbetssättet.

2.7.2. Hanteringsregler för information och utrustning

Ett viktigt kompletterande skydd för informationen, utöver det skydd som finns i it-miljön och våra lokaler, är hanteringsregler[11] som beskriver hur medarbetarna får hantera information och arbetsutrustning.

Hanteringsreglerna beskriver vilka säkerhetsbestämmelser som gäller för information i en viss informationsklass vid exempelvis användning av e-post, videomötestjänst, chattverktyg, mobila enheter med mera. Myndigheten har även särskilda bestämmelser för hur utrustning och information ska hanteras vid distansarbete, eller när medarbetare är på tjänsteresa.

Pensionsmyndigheten ser löpande över och anpassar hanteringsreglerna då det ständigt sker förändringar i verksamheten och omvärlden som påverkar hur våra medarbetare ska hantera information och utrustning.

2.8. Säkerhet i it-miljön

All verksamhet vid myndigheten är beroende av it-lösningar och myndigheten utvecklar och prövar innovativa lösningar för att effektivisera verksamheten och förbättra myndighetens service till medborgare. De senaste åren har myndighetens it-avdelning vuxit och förändrat arbetssätt, vilket har lett fram till en omorganisation som trädde i kraft första mars. I den nya organisationen flyttas it-säkerhetsenheten en nivå närmare it-chefen.

I Pensionsmyndighetens strategi för it[12] identifieras nio strategiska inriktningar för arbetet med it inom myndigheten. Inriktningarna utgör ett

[11] Riktlinje säkerhet för medarbetare, SÄK 2020-62

[12] Strategi för it 3.0, VER 2018-133

fundament för hur myndigheten arbetar med it för att maximera nyttan för pensionärer och pensionssparare och är i linje med myndighetens övergripande inriktning för kundcentrerad digitalisering.

Den första av de nio inriktningarna är ”Säker leverans”. Där framgår bland annat att it-säkerhet och driftstabilitet ska vara i fokus och prägla myndighetens it-leverans i alla avseenden.

Eftersom Pensionsmyndigheten är en beredskapsmyndighet och bedriver samhällsviktig verksamhet har myndigheten höga krav på tillgänglighet och god it- och informationssäkerhet. Detta innebär att

- it-leveransen ska bedrivas utan störningar och i de fall sådana inträffar ska myndigheten kunna hantera dem på ett kontrollerat och effektivt sätt.
- it-avdelningen prioriterar arbetet med robusthet och redundans samt ett fungerande kontinuitetsarbete då tillgängligheten för informationssystem är central för myndighetens verksamhet.
- myndighetens säkerhetsarbete ska följa lagar och förordningar och vara riskbaserat, med säkerhetsåtgärder som anpassas till risknivå och kostnadseffektivitet i lösningarna.
- myndigheten ska ha ett högt kvalitets- och säkerhetsmedvetande inom hela myndigheten.

Pensionsmyndigheten har en fungerande styrning och systematiskt arbetssätt och det finns ett antal processer och rutiner inom it-säkerhet.

Regelverk för it-säkerhet består av 11 anvisningar inom området. I regelverket anges vilka säkerhetsåtgärder som är beslutade inom it-säkerhet, hur ansvar fördelas inom området samt beskrivningar av processer och rutiner.

It-säkerhetsenheten arbetar aktivt med olika former av uppföljning och sammanställer rapporter över it-säkerhetsläget. Det finns också ett samarbete inom it-avdelningen där it-säkerhetsspecialister deltar i olika beslutsfora för att säkerställa att it-säkerheten upprätthålls.

2.9. Leverantörsrelationer

Delar av Pensionsmyndighetens verksamhet utförs av eller hos andra aktörer, såväl offentliga och privata. Myndighetens verksamhet ska ha rätt nivå av säkerhet oavsett om utförandet sker inom Pensionsmyndigheten eller för myndighetens räkning hos en extern part. Pensionsmyndigheten har etablerade processer och rutiner för inköp där säkerhet ingår och myndighetens krav på säkerhet ska specificeras i avtal eller överenskommelser. Myndigheten har fungerande leverantörsrelationer där bland annat säkerhetskraven, hantering av incidenter med mera följs upp.

Några exempel på delar av myndighetens verksamhet som utförs av eller hos andra myndigheter är

- Statens Servicecenter som ansvarar för servicekontorsverksamheten, där Pensionsmyndigheten ingår. Inom ramen för servicekontoren samverkar alla deltagande myndigheter och diskuterar vilken nivå av säkerhet som ska gälla inom servicekontorsverksamheten.
- Försäkringskassan levererar datahallstjänster och förvaltning av vissa verksamhetssystem till Pensionsmyndigheten. Pensionsmyndigheten och Försäkringskassan har löpande samverkan där bland annat säkerheten följs upp och olika säkerhetslösningar i leveranserna diskuteras.

3. Framtida behov

Informationssäkerhetsarbetet behöver ständigt utvecklas. Det för att på bästa sätt stötta verksamheten och ge förutsättningar för att skydda den samhällsviktiga funktionen inom myndigheten.

Mycket arbete genomförs för att skapa medvetenhet och kunskap om informationssäkerhet i hela myndigheten och särskilt inom it och systemutveckling. Där tas nya utbildningar fram för att stärka informationssäkerheten.

Flera initiativ har tagits för att öka förmågan att identifiera sårbarheter och angrepp i it-miljön. Arbete med att etablera ytterligare lösningar för att kunna återställa Pensionsmyndighetens data på alternativa sätt har initierats.

Det systematiska säkerhetsledningssystemet utvecklas kontinuerligt för att hantera nya eller förändrade risker för pensionsmyndighetens it-miljö.

Pensionsmyndigheten är medlemmar i eSam[13]. Genom medlemskapet verkar myndigheten för att bättre ta tillvara digitaliseringens möjligheter, för att underlätta för privatpersoner och företag och för att använda gemensamma resurser på ett effektivt sätt. Pensionsmyndigheten deltar i olika arbetsgrupper inom eSam, till exempel Moln, Juridik och Säkerhet. Genom att verka i dessa grupper arbetar Pensionsmyndigheten för digitala tjänster som är tekniskt ändamålsenliga, säkra och lagenliga.

Utöver eSam deltar Pensionsmyndigheten även i andra former av extern samverkan inom säkerhetsområdet för att utbyta erfarenheter med exempelvis andra myndigheter. I samverkan får myndigheten en möjlighet att kvalitetssäkra säkerhetsarbetet genom att utbyta erfarenheter med andra och jämföra metoder och arbetssätt. Att dela med sig av kunskap och erfarenheter är en framgångsfaktor i arbetet med säkerhet inom det offentliga Sverige.

[13] eSam är ett medlemsdrivet program för samverkan mellan 34 myndigheter, www.esamverka.se

4. Intern styrning och uppföljning av informationssäkerhet

Pensionsmyndigheten arbetar kontinuerligt med att vidareutveckla styrningen och uppföljningen av informationssäkerhetsarbetet inom ramen för myndighetens säkerhetsledningssystem. Nedan redogörs för de åtgärder myndigheten har vidtagit för att utveckla den interna styrningen och uppföljningen av informationssäkerhetsarbetet.

Styrning av informationssäkerhet

Informationssäkerhetsarbetet påverkar hela myndighetens verksamhet och behöver kontinuerligt anpassas efter de styrmodeller och ramverk som används inom myndigheten. De senaste åren har myndigheten infört ett agilt arbetssätt för it-utveckling och förvaltning. Styrningen av informationssäkerhetsarbetet har vidareutvecklats och anpassningar pågår så styrningen fungerar både i den traditionella linjeverksamheten och i det agila arbetssättet.

Säkerhetsregelverket har exempelvis kompletterats med två nya riktlinjer, riktlinje för agil styrning[14] och riktlinjen styrning av säkerhet och säkerhetsansvar[15] (en uppdatering och sammanslagning av de tidigare riktlinjerna säkerhet för chefer och styrning och ledning av säkerhet).

En viktig fråga som har klarlagts är riskägarskap för säkerhetsrisker samt informationsägarskap inom de delar av verksamheten som omfattas av det agila arbetssättet. Pensionsmyndigheten har fastställt en mall för hur ett beslut om fördelning av riskägarskap och informationsägarskap från avdelningschef (linje-organisationen) till Business Owner (agilt arbetssätt) ska dokumenteras. Som tidigare nämnts pågår ett arbete för att genomföra och dokumentera delegering av ansvar gällande risk- och informationsägarskap.

Uppföljning av informationssäkerhet

Pensionsmyndigheten genomför bland annat regelbundna kontroller och uppföljningar enligt beslutade kontrollplaner och analyserar inträffade incidenter för att identifiera brister och avvikelser inom säkerhet. Det bidrar till att ständigt förbättra myndighetens säkerhetsarbete och myndighetens säkerhetsnivå.

Pensionsmyndighetens ledningsgrupp är engagerade i säkerhetsfrågor och en gång per år genomförs ledningens genomgång i enlighet med standarderna ISO/IEC 27001 och 27002. Vid senaste genomgången bedömdes att myndighetens säkerhetsledningssystem är lämpligt, tillräckligt och effektivt.

---

[14] Riktlinje Agil Styrning, VER 2022-266

[15] Riktlinje Styrning av säkerhet och säkerhetsansvar, SÄK 2021-45

En del av Pensionsmyndighetens interna kontroll består i att kontrollera efterlevnaden av säkerhetsregelverket. Verksamhetsansvarig chef genomför kontroll gällande efterlevnaden av säkerhetsregelverket inom sitt verksamhetsområde samt att medarbetarna har kunskap om och efterlever säkerhetsregelverket.

I den fördjupande verksamhetsuppföljningen som genomförs två gånger per år rapporterar avdelningschef status för avdelningens säkerhetsrisker.

Under 2023 har Pensionsmyndigheten vidareutvecklat arbetsprocessen och metoden för uppföljning. En del i arbetet har varit att kartlägga och beskriva de olika typer av uppföljning som görs inom informationssäkerhet. Pensionsmyndigheten har också tagit fram metoder och underlag för riktade uppföljningar inom specifika områden eller till specifika målgrupper. Tidigare i år genomfördes en riktad uppföljning om säkerhet till myndighetens chefer. Resultatet var på det stora hela väldigt positivt, även om det finns delar som kan förbättras.

Pensionsmyndigheten genomförde en uppföljning enligt MSB:s uppföljningsmodell Infosäkkollen under 2021. Modellen utgår från det systematiska informationssäkerhetsarbetet som det beskrivs i MSB:s föreskrifter och stöd, som i sin tur bygger på standardserien ISO/IEC 27000. Modellen ger stöd till uppföljning på en strategisk nivå. MSB gav återkoppling till de organisationer som skickade in sina svar. I återkopplingen ingår en jämförelse med snittet för andra, liknande organisationer. Jämförelsen utgår från det samlade underlaget.

Den återkoppling och jämförelse som MSB presenterar visar att Pensionsmyndighetens systematiska informationssäkerhetsarbete befinner sin över medelvärdet för de 30 bästa myndigheterna. Återkopplingen, som sker i form av värden för olika områden och totalt, från MSB pekar på att Pensionsmyndigheten överlag har ett bra informationssäkerhetsarbete, men självklart finns det områden där informationssäkerhetsarbetet behöver förbättras och vidareutvecklas.

Resultatet visar i vilken utsträckning Pensionsmyndigheten bedriver ett systematiskt informationssäkerhetsarbete, det vill säga har förutsättningar att bygga ett gott skydd för sin information. Modellen mäter inte om den enskilda organisationens skydd är tillräckligt.

Myndigheten har en handlingsplan, som togs fram efter det att Infosäkkollen genomförts, med ett antal åtgärder som myndigheten arbetar med att införa. Myndigheten planerar att genomföra Infosäkkollen igen under 2023.

5. Hur arbete på distans påverkar informationssäkerheten

Nedan redogörs för hur medarbetarnas arbete på distans bedöms påverka informationssäkerheten och vilka åtgärder som har vidtagits för att upprätthålla informationssäkerheten.

Under pandemin och därefter har myndighetens arbetssätt förändrats och mer arbete utförs nu på distans. Närmaste chef beslutar om möjlighet till distans/hybridarbete och medarbetare tecknar en överenskommelse om distansarbete med Pensionsmyndigheten. I dagsläget har 70% av medarbetarna tecknat överenskommelse om distansarbete vanligtvis 3 dagar på distans per vecka. I överenskommelsen framgår att medarbetaren särskilt ska informera sig om styrande dokument inom säkerhet. Myndigheten har också en särskild anvisning för distansarbete och mobilt arbete[16]. I den beskrivs de förutsättningar som gäller och det finns ett eget kapitel som reglerar säkerhet och sekretess, där framgår både vad medarbetarna ska göra samt vad medarbetarens närmsta chef ska göra. Områden som beskrivs är säker och trygg arbetsmiljö, hanteringsregler för information, risk för påtryckningar, uppföljning, regler för utrustning med mera.

Pensionsmyndigheten har säkerställt att klienterna (med klient menas den hårdvara, till exempel dator, som medarbetarna använder för att ansluta till myndighetens it-system) är skyddade bland annat genom kryptering av klienterna och kommunikationen. Klienterna är även utrustade med skydd för att upptäcka intrångsförsök, skydd mot skadlig kod samt så kallat surffilter. Utöver detta använder myndigheten alltid stark autentisering med tillhörande processer och rutiner för att livscykelhantera behörigheter.

När myndigheten har fattat strategiska beslut om arbete på distans har informationssäkerheten beaktats. I dagsläget har nästan alla medarbetare vid myndigheten möjlighet till hybridarbete.

Pensionsmyndigheten har via uppföljningar och analyser av incidenter undersökt om myndighetens informationssäkerhet har påverkats negativt av att arbetet på distans/hybridarbetet har ökat de senaste åren. Myndigheten har hittills inte sett några negativa effekter på informationssäkerheten.

6. Analys av förändringar i omvärldsläget och påverkan för Pensionsmyndigheten

[16] Anvisning distansarbete och mobilt arbete, PSL 2021-95

[17] Anvisning för krishantering och höjd beredskap, SÄK 2021-22

avdelningar och till ledningsgrupp, hölls dialog med Socialdepartementet om vidtagna samt förmågehöjande åtgärder löpande.

Pensionsmyndigheten har förbättrat skyddet mot intrång i it-miljön och stärkt förmågan att upptäcka intrångsförsök. För att minska påverkan av överbelastningsattacker har myndigheten löpande dialog med vår leverantör för att säkerställa att det finns hög beredskap och att man följer utvecklingen.

För att validera vår säkerhet samt för att identifiera förbättringsåtgärder genomför vi löpande säkerhetsgranskningar av vår it-miljö. Under 2022 genomfördes två granskningar av externt säkerhetsföretag båda resulterade i gott betyg gällande säkerhetsnivå. Under granskningarna identifierades ett antal förbättringsförslag, dessa förslag/åtgärder har införts.

Pensionsmyndigheten har även säkerställt att rutiner och dokument kring kontinuitet är uppdaterade. Myndigheten genomför också övningar för att träna förmågan att hantera större incidenter, störningar, kriser och höjd beredskap.

Utöver ovanstående arbetar myndigheten också mycket med omvärldsbevakning för att få en god lägesbildsuppfattning och snabbt kunna agera på nya hot och händelser.

Med anledning av Rysslands invasion av Ukraina i februari 2022 fick området civilt försvar mycket uppmärksamhet internt, men också i samhället och inom politiken. Nya regeringsuppdrag tilldelades myndigheter[18], där Pensionsmyndigheten exempelvis skulle inkomma med föreslagna åtgärder inom civilt försvar för år 2023-2030.

Myndighetens övergripande riskanalys har uppdaterats som en följd av omvärldsläget där ett flertal nya åtgärder för att hantera risken har identifierats och påbörjats. Riskhanteringen och införandet av åtgärder följs upp löpande.

Myndigheten har under 2022 genomfört ett antal redovisningar inom området.

- Pensionsmyndighetens svar på hemställan del 1 och 2 avseende MSB:s regeringsuppdrag (Ju2022/01209) samt i budgetäskanden till regeringen för 2023 och framåt
- Pensionsmyndighetens svar på förmågebedömning inom ramen för regeringsuppdrag Ju2020/04658 (delvis)
- Pensionsmyndighetens risk- och sårbarhetsanalys avseende år 2022.

6.1.1. Krisberedskap och civilt försvar

Sedan den 1 oktober 2022 är Pensionsmyndigheten beredskapsmyndighet vilket i korthet innebär att myndigheten har särskild betydelse för samhällets civila beredskap och ska ha god förmåga att motstå hot och risker,

[18] MSB:s regeringsuppdrag att lämna förslag på åtgärder för att stärka det civila försvaret, Ju2022/01209

förebygga sårbarheter, hantera fredstida krissituationer och genomföra sina uppgifter vid höjd beredskap.

Pensionsmyndigheten ingår som utpekad aktör inom beredskapssektor Ekonomisk säkerhet och ska utifrån våra egna förutsättningar ha ett nära samarbete med övriga aktörer som ingår i sektorn.

Myndigheten har en grundläggande beredskap och förmåga att hantera incidenter, störningar och kriser, om de trots allt inträffar. Myndigheten fortsätter att vidareutveckla krisberedskapsarbetet och åtgärder inom civilt försvar och här redovisas exempel på genomförda och pågående riskreducerande åtgärder.

- utbildningar och övningar som stärker myndighetens krishanteringsförmåga
- översyn och planering för förbättrat skydd av, och tillgång till ledningsplatser (både fysiska och digitala)
- robusthöjande åtgärder för kritiska it-tjänster samt åtgärder för säkra kommunikationer
- fördjupat samarbete med externa aktörer, till exempel Försäkringskassan
- åtgärdsplaner från riskanalyser/risk- och sårbarhetsanalyser
- styrande dokument och uppföljning av efterlevnad av dessa
- beredskapsplanering i form av planer.

Exempel på planerade riskreducerande åtgärder inom myndigheten är

- löpande arbete med riskarbete, både på avdelningsnivå och på myndighetsnivå, inklusive arbete med åtgärdsplaner kopplat till riskhanteringsarbetet
- regelbundna krisövningar för central krisledning, avdelningar och andra relevanta medarbetare
- utbildningsinsatser för att höja medvetenheten inom säkerhet, beredskap och informationssäkerhet
- fortsatt samarbete och samverkan inom området krisberedskap, internt inom myndigheten i fastställda arbetsgrupper samt inom beredskapssektorn Ekonomisk säkerhet.

Samtliga åtgärder ovan är beslutade att genomföras. Åtgärderna prioriteras löpande inom ramen för det dagliga arbetet, utifrån tilldelade anslag och med hänsyn till omvärldssituation.

www.pensionsmyndigheten.se