Granskning av polisens hantering av behörighet till IT-system

Internrevisionen

2018-04-16

INNEHÅLL

BILAGOR

BESLUTSPROTOKOLL RIKSPOLISCHEFEN 2018-04-13
SAMMANSTÄLLNING AV INKOMNA SVAR (FULLSTÄNDIGA)

1 Sammanfattning

Internrevisionen har i enlighet med revisionsplanen för 2016-2017 granskat polisens hantering av behörighet till it-system. Granskning och rapportskrivning har genomförts under perioden maj-oktober 2017.

Granskningen har omfattat processen för hantering av it-behörigheter. Platsbesök med intervjuer har genomförts på behörighetscenter (BC) i Göteborg, Stockholm och med personal tillhörande BC i Örnsköldsvik och Halmstad. Intervjuer har också genomförts med vissa informationsägare, personuppgiftsombudet samt processägare på it-säkerhet. I granskningen ingick även att via slumpmässigt urval granska ett större antal medarbetares it-behörigheter.

Internrevisionen anser att det finns förbättringsmöjligheter i den interna styrningen och kontrollen beträffande hanteringen av it-behörigheter.

Internrevisionen gör den övergripande bedömningen att processen för tilldelning och revision av it-behörigheter inte är tillräcklig för att säkerställa kraven på att behörighet till polisens it-system endast ska ske på grundval av lämplighet, kunskap och behov i sitt arbete. Chefer, med bäst kunskap om detta, är normalt inte är involverade i samband med tilldelning och revision av medarbetarnas it-behörigheter. Fördelningen av ansvar och roller inte är tillräckligt tydlig vad gäller hur processägarens/informationsägarens ansvar och roll förhåller sig till övriga chefers ansvar och roll.

I flertalet fall saknas riktlinjer från informationsägare som reglerar tilldelning av it-behörigheter. Dessa riktlinjer skulle kunna ge stöd till BC:s bedömningar i samband med tilldelning av it-behörigheter. De riktlinjer som tagits fram under senare tid har heller inte fullt ut införts inom BC.

Utfallet från stickprovsgranskningen visade att många anställda har onödigt många it-behörigheter och i vissa fall högre it-behörigheter än nödvändigt för tjänsten. Detta kan medföra en ökad risk att anställda använder behörigheterna på ett otillbörligt sätt, t.ex. genom att göra slagningar i systemen. Det finns även en kostnadsaspekt att beakta.

Internrevisionen gör bedömningen att effektivitetsförbättringar kan åstadkommas genom att all behörighetshantering så långt möjligt styrs till BC, att alla ansökningar går via Polisens administrationsportal (PAP), att fler it-system blir helintegrerade, genom att vidareutveckla utformningen av ansökningsförfarandet samt utarbeta fler behörighetsprofiler.

Granskning har resulterat i totalt sju rekommendationer, fördelade enligt nedan utifrån internrevisionens modell för bedömning av brister.

		Antal
	Mycket väsentlig brist	1
	Väsentlig brist	4
	Mindre väsentlig brist	2

2 Inledning

Granskningen har utförts i enlighet med revisionsplanen för 2016-17.

2.1 Bakgrund

Behörighet till polisens it-system ska endast ges till anställd eller konsult som bedöms vara lämplig ur säkerhetssynpunkt, som har erforderliga kunskaper och har behov av uppgifterna i sitt arbete. Det är högst väsentligt för den enskilde medarbetaren och för Polismyndigheten att behörigheterna är korrekta.

Innan reformen 2015 fanns ingen nationell enhetlighet för polisens behörighetshantering. Processer och system var lokalt anpassade.

Genomförandekommittén arbetade 2014 fram riktlinjer för ett nationellt arbetssätt gällande behörighetshantering. Detta gjordes för att säkerställa att polisens behörighetshantering (via systemstödet PAP) hanterades på ett enhetligt sätt.

Behörighetscenter (BC) som organisatoriskt sorterar under enheten it-kundservice har därefter fått ansvaret för att den nationella processen för behörighetshantering ska fungera i det dagliga linjearbetet och att alla som arbetar inom polisen får tillgång till de it-system som deras arbetsuppgifter kräver.

Enligt vision 2017[1] är målet att medarbetares närmaste chef ska godkänna/avslå behörighetsansökan samt utföra revision av sina medarbetares behörigheter. Fram till 2018-12-31 under en övergångsperiod, eller till dess annat beslut tas, beslutas och revideras behörigheter i PAP av behörighetshandläggare vid BC.

2.2 Syfte

Syftet med granskningen har varit att bedöma om den interna styrningen och kontrollen av polisens hantering av it-behörigheter är ändamålsenlig.

Målet med granskningen med utgångspunkt i myndighetsförordningens (2007:515) 3 § har varit att bl.a. bedöma om verksamheten bedrivs effektivt.
Granskningen har syftat till att bedöma följande frågeställningar:

- Finns det en ändamålsenlig och effektiv process för hantering av it-behörigheter?
- Hur säkerställs att medarbetarna har rätt it-behörigheter?
- Är ansvar och roller för behörighetshantering tydliga?

2.3 Omfattning och avgränsning

Granskningen har omfattat behörighetstilldelning till medarbetare i samtliga polisregioner och nationella avdelningar via stickprov. Granskningen har inte omfattat behörighetstilldelning i utvecklingsmiljö, behörighetstilldelning till det it-baserade inpasseringssystemet samt fysisk åtkomst till it-utrustning.

[1] Genomförandekommittén för nya Polismyndigheten, PM 2013-12-17.

2.4 Metod och tillvägagångssätt

Informationsinsamling och metoden för granskningen har varit platsbesök med intervjuer på BC i Göteborg, Stockholm och personal tillhörande BC i Örnsköldsvik och Halmstad, dataanalys/registeranalys samt stickprov. Internrevisionen har också varit i kontakt med vissa informationsägare, personuppgiftsombudet samt processägare på it-säkerhet.

Beträffande stickprovet fick internrevisionen hjälp av PAP förvaltningen med att ta fram ett slumpmässigt urval på 50 personer i varje polisregion och nationell avdelning, totalt 750 personer[2]. Ur denna lista valde internrevisionen ut var femte person för granskning. I granskningen ingick att bedöma om behörigheterna var rimliga med beaktande av funktion, framtagna behörighetsprofiler och informationsägarnas riktlinjer avseende ansvar för personuppgiftsbehandling. I tveksamma fall har internrevisionen muntligen kontaktat berörda personer beträffande deras behörigheter. Avstämning av tveksamma behörigheter har i vissa fall även skett med BC.

Granskningen har utförts under perioden maj – september, 2017 av internrevisorerna Carl Ygge och Stefan Carp.

Rapporten sakgranskades under perioden 2017-10-17 till 2017-11-15 av samtliga nationella avdelningar. Begäran om inhämtande av åtgärdsförslag skickades till RPC kansli 2017-12-06. Svar med förslag på åtgärder med anledning av internrevisionens rekommendationer lämnades under perioden 2018-01-15 fram till 2018-02-15. Förslag på åtgärder har lämnats av IT-avdelningen, Ekonomiavdelningen, HR-avdelningen, Nationellt Forensiskt Centrum, Rättsavdelningen, Nationella Operativa Avdelningen samt Kommunikationsavdelningen. Svaren i sin helhet har sammanställts i bilaga till rapporten, *Internrevisionens granskning av polisens hantering av behörighet till it-system - Sammanställning av inkomna svar.* Nya beredningsrutiner som införts i myndigheten i början av 2018 har medfört en viss fördröjning av expedieringen av rapporten.

2.5 Bedömningsgrunder

Internrevisionens iakttagelser, bedömningar och grunder för lämnade rekommendationer framgår av den löpande texten i rapporten. För respektive rekommendation har internrevisionen bedömt bristen vid tidpunkten för granskningen. Internrevisionens bedömning följer nedanstående mall.

Bedömning	Beskrivning
Röd - Mycket väsentlig brist	Brist som allvarligt påverkar Polismyndighetens måluppfyllelse enligt instruktion eller regleringsbrev och/eller medför stora negativa konsekvenser för Polismyndighetens verksamhet och/eller innebär att Polismyndigheten inte uppfyller myndighetsförordningens krav på effektivitet, lagenlighet, redovisning och hushållning.
Orange - Väsentlig brist	Brist som påverkar den granskade verksamheten så att uppställda mål inte nås och/eller medför betydande negativa konsekvenser för verksamheten.

[2] Internrevisionen har inte lyckats få kontakt med samtliga personer i stickprovsurvalet och har i dessa fall valt att utelämna dessa från granskningen.

Gul - Mindre väsentlig brist	Brist som inte påverkar den granskade verksamhetens måluppfyllelse men som medför negativa konsekvenser för verksamheten.

3 Granskning av polisens hantering av behörighet till IT-system

3.1 Processen för behörighetshantering

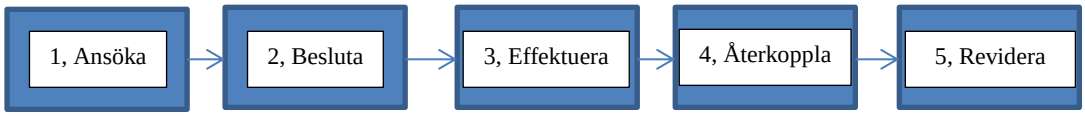
Iakttagelser

Styrdokument
Processen för behörighetshantering finns beskriven i ett arbetsdokument som tagits fram av it-avdelningen/it-säkerhetsenheten och som är i behov av att formaliseras. Som komplement finns en mer detaljerad instruktion för BC som beskriver hur BC ska arbeta i den nationella processen för behörighetshantering. Vissa avsnitt i denna instruktion som är daterad 2016-12-21 är under arbete och behöver färdigställas.

BC har även anvisningar, instruktioner och lathundar för bl.a. effektuering av behörigheter i respektive system och i vissa fall som stöd för bedömningar. Lathundar för bedömningar är inte heltäckande. De riktlinjer som vissa informationsägare tagit fram och som bl.a. reglerar behörighetstilldelningar har enligt uppgift inte kommit BC till del och har således inte införts och används inte som stöd för BC:s bedömningar, se vidare 3.2, säkerställande av rätt it-behörigheter.

De riktlinjer som reglerar området, Polismyndighetens riktlinjer för säkerhet vid informationsbehandling med stöd av it, blev i november (2017) formellt beslutade.

Processen
Den nationella behörighetsprocessen omfattar följande aktiviteter:



Enligt den nationella behörighetsprocessen hanteras it-behörigheterna av BC. I intervjuer framkom dock att det finns ett flertal it-system där godkännande och/eller effektuering av behörighet inte sker av BC. Exempelvis godkänns vissa it-system av BC men effektueras av andra funktioner. Några it-system godkänns och effektueras av förvaltningen eller motsvarande. En anledning till att vissa behörigheter administreras av andra än BC kan vara att informationsägare/systemansvarig vill ha kontroll över vilka personer som tilldelas behörigheter till känsliga system. En annan anledning kan vara tekniska svårigheter t.ex. att behörigheter endast kan effektueras från vissa datorer.

1, Ansöka
Beställaren (i normalfallet slutanvändaren) ansöker om ny behörighet via PAP alternativt via formulär (PM 174.2). För vissa behörigheter ska motivering anges. Även om de flesta ansökningar om it-behörigheter inkommer via PAP så görs en del via formulär och i vissa fall via mejl.
Enligt intervjuer med medarbetare inom BC borde alla ansökningar inkomma via PAP för att säkra en bättre spårbarhet. De intervjuade lyfte även fram att en bättre utformning

av ansökan i PAP skulle kunna effektivisera behörighetsadministrationen genom att minska antalet ansökningar som behöver returneras för kompletteringar. Vidare skulle det ge ett bättre stöd till beställare av mer komplexa system som t.ex. PÄr. Om tvingande motivering införs vid behörighetsansökan till känsliga system skulle även detta minska antalet ansökningar som returneras.

Tilldelningen av it-behörigheter till studenter vid polisutbildningen har också lyfts fram som ett område med en omfattande behörighetshantering då de först får en studentbehörighet, sedan aspirantbehörighet och tillbaka till student (under 8 veckor), för att sedan få behörighet som polisassistent.

Ett flertal behörighetsprofiler har tagits fram (16) vilket uppges underlätta BC:s arbete. Internrevisionens stickprovsgranskning visade dock exempel där befintliga behörighetsprofiler behöver ses över pga att funktionen har fått utökade arbetsuppgifter, t.ex. för PKC operatör. Det finns också utrymme att ta fram fler behörighetsprofiler.

2, Besluta
BC utför kontroll av informationen i behörighetsansökan samt fattar beslut. Kontroll avser huvudsakligen anställningsinformation i PAP och information i ansökan inklusive eventuell motivering. Godkänns ansökan går den vidare till effektuering, i annat fall skickas avslag med motivering till sökande (beställaren). För vissa behörigheter krävs s.k. tvåhandsfattning vilket innebär att ansökan behöver godkännas (sanktionera ansökan) av systemansvarig enligt PAP och sedan godkännas (besluta ansökan) av behörighetshandläggare inom BC.

För övriga iakttagelser relaterade till beslut se avsnitt 3.2, säkerställande av rätt it-behörigheter.

3, Effektuera
Effektuering av behörighet utförs i huvudsak av BC, efter godkännande och kan antingen ske automatiskt via PAP för integrerade it-system eller att BC effektuerar behörigheten direkt i målsystemet.

Medarbetare inom BC har lyft fram möjligheten till effektivitetsvinster om fler it-system blir helintegrerade. Enligt intervjuer är majoriteten av it-systemen helintegrerade men de största it-systemen, d.v.s de som har flest användare t.ex. Agresso, Palasso och DurTvå, är inte helintegrerade.

4, Återkoppla
BC meddelar användaren om ansökan har godkänts och behörigheten är tilldelad, alternativt om ansökan avslagits eller behöver kompletteras.

I likhet med punkt 1 ansöka ovan, har medarbetarna inom BC lyft fram att en bättre utformning av behörighetsansökan via PAP och formulär skulle minska andelen ansökningar som skickas tillbaka för kompetteringar.

5, Revidera
BC utför behörighetsrevisioner senast var 13:e månad. Behörighetsrevisionen initieras tidigare vid förändringar såsom byte av tjänst/avdelning/enhet, förändrade arbetsuppgif-

ter eller förändrade arbetsförhållanden eller till följd av disciplinära åtgärder. För att BC ska kunna genomföra behörighetsrevisioner tidigare än var 13:e månad måste BC få denna information.
För övriga iakttagelser relaterade till beslut se avsnitt 3.2, säkerställande av rätt it-behörigheter.

Bedömning
Internrevisionen gör bedömningen att effektivitetsförbättringar skulle kunna åstadkommas genom att all behörighetshantering så långt möjligt styrs till BC och inte som idag då flera funktioner sköter hanteringen. En bättre effektivitet kan också uppnås genom att alla ansökningar går via PAP, att fler it-system blir helintegrerade samt vidareutveckla utformningen av själva ansökansförfarandet i PAP för att på så sätt minska andelen ansökningar som måste returneras för komplettering. En effektivare och enhetligare process kan också uppnås genom att utarbeta fler behörighetsprofiler i myndigheten. Internrevisionen konstaterar att ett antal styrdokument inte är uppdaterade och beslutade vilket kan leda till oklarheter kring behörighetsprocessen.

Rekommendationer

Gul – Mindre väsentlig brist
Internrevisionen rekommenderar att: IT-avdelningen - Vidtar åtgärder för att så långt möjligt all behörighetshantering lyfts över till BC - Så långt möjligt få fler it-system att bli integrerade med PAP - Färdigställer och formaliserar processdokument och instruktion för BC - I samråd med informationsägarna förbättrar utformningen av ansökan om it-behörigheter i PAP, t.ex. tvingande motivering vid ansökan om känsliga system, underlätta ansökan, bättre hjälp vid ansökan till it-system med många olika behörigheter såsom t.ex. PÄr - Skapar behörighetsprofiler för flera funktioner inom myndigheten samt gör översyn av befintliga behörighetsprofiler.

Konsekvenserna av om rekommendationerna inte följs är en ineffektiv och ej enhetlig behörighetshantering. Detta kan medföra negativa konsekvenser för verksamheten.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Chefen för IT-säkerhetsenheten, Josefine Östfeldt i samråd med chefen för IT-kundserviceenheten Petra Marcusson.
Åtgärder	- För varje systemanslutning görs en bedömning om all behörighetshantering ska ligga hos BC, vilket är utgångspunkten. Det kan dock finnas tillfällen då det inte är möjligt tex pga att behörigheter endast kan läggas upp på en specifik dator eller att det är mycket känsliga uppgifter. Det är därför inte möjligt att lyfta över all behörighetshantering till BC. - För varje systemanslutning görs en bedömning om systemet ska helintegreras med PAP, vilket är intentionen. Det kan dock finnas tekniska skäl till att en integration inte är möjlig, eller att

	det är mycket få användare av ett system och det inte är ekonomiskt försvarbart att integrera. - Processdokument för den nationella behörighetsprocessen ska färdigställas och beslutas. För övriga instruktioner för BC uppdateras dessa kontinuerligt av process- och dokumentansvarig på BC. - Förbättringar i PAP hanteras löpande i Behörighetsforum som leds av IT-säkerhetsenheten. - Fler och förbättrade behörighetsprofiler förbättras löpande i den sk MUG gruppen (MetodUtvecklingsGruppen) inom BC och beslutas av IT-säkerhetsenheten.
Ansvarig	Chefen för IT-säkerhetsenheten, Josefine Östfeldt.
Tidsplan	Den nationella behörighetsprocessen ska vara beslutad senast 2018-09-30. Övriga punkter utförs löpande och förbättringsarbetet under 2018 kommer att följas upp med avstämning senast 2019-02-28.

Gul – Mindre väsentlig brist
Internrevisionen rekommenderar att: HR-avdelningen - Ser över möjligheter till förändrad behörighetshantering av polisstudenter.

Konsekvenserna av om rekommendationen inte följs är en ineffektiv och ej enhetlig behörighetshantering. Detta kan medföra negativa konsekvenser för verksamheten.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	HR-avdelningen, avdelningskansli, analytikern Oscar Lundin.
Åtgärder	HR-avdelningen vidtar åtgärder för förändrade administrativa rutiner som möjliggör att samlade underlag kan lämnas i så god tid som möjligt till behörighetscenter.
Ansvarig	HR-avdelningen, Kompetensutveckling, enhetschefen Anna Orhall.
Tidsplan	Genomfört 1 oktober 2018

Kommentarer till lämnad rekommendation eller planerade åtgärder:
Studenter är i behov av vissa behörigheter under polisutbildningen vid lärosätena. Under aspirantutbildningen som genomförs vid polisregionerna är studenterna tillfälligt an-

ställda i Polismyndigheten och har då behov av utökade behörigheter. Vid anställning som polisassistenter förändras återigen behovet av behörigheter.

3.2 Säkerställande av rätt it-behörigheter

Iakttagelser

Ny behörighetsansökan
Ansökan om behörighet till de flesta it-systemen godkänns av behörighetshandläggare inom BC. För vissa it-system krävs så kallad tvåhandsfattning vilket innebär att ansökan ska godkännas (sanktioneras) av systemansvarig enligt PAP och sedan godkännas (beslutas) av behörighetshandläggare inom BC. Ansökan fylls i normalfallet i av slutanvändaren och skickas direkt till BC utan att passera slutanvändarens chef. Säkerställandet av rätt it-behörighet görs således huvudsakligen av BC. För att fullgöra denna uppgift kontrollerar BC anställningsinformationen i PAP samt informationen i ansökan inklusive eventuell motivering. Även om BC är bemannat med personal som har god verksamhetskunskap så upplever personalen enligt intervjuer emellanåt svårigheter med bedömningen av behovet av behörigheter. Vissa ansökningar kontrolleras av BC genom kontakt med berörd eller närmaste chef. Om slutanvändare motiverar behov så kan detta vara svårt för BC att ifrågasätta.

I intervjuer med BC framkom erfarenheter av brister i tillförlitligheten till anställningsinformationen i PAP. Informationen som initialt kommer från Palasso och överförs till PAP stämmer inte alltid och detta medför att kontroller som BC genomför och som ligger till grund för BC:s bedömning och beslut kan baseras på felaktig/ej uppdaterad information. Internrevisionens stickprovsgranskning visade också flera exempel där anställningsinformationen var felaktig. Enligt uppgift har HR genomfört en omfattande rättning av anställningsuppgifter efter sommaren 2017. Detta har lett till betydligt bättre kvalitet gällande källdata i Palasso. Det kvarstår dock en brist som hänger samman med ett fritextfält i Palasso från vilket PAP hämtar information om vilka som är chefer. Fritextfältet återfinns inte i blankett ”ändrade anställningsuppgifter”, utan måste fyllas i under övrig information, vilket leder till att uppgiften om chef lätt missas att fyllas i.

En annan faktor som försvårar BC bedömningar och beslut är att polisregioner har organiserat sitt arbete på olika sätt vilket leder till att vissa anställda söker högre behörigheter jämfört med andra polisregioner även om personen har samma funktion.

BC har som stöd för sina bedömningar och beslut ett antal lathundar och PM. Dessa är enligt intervjuer inte fullständiga och leder till viss osäkerhet i samband med bedömningarna. Enligt uppgift pågår arbete inom BC med att förbättra stödet för att göra bedömningar.

De riktlinjer som vissa informationsägare tagit fram (se vidare 3.3, informationsägares roll och ansvar) för att bl.a. reglera till vem och hur it-behörigheter får tilldelas har enligt uppgift inte kommit BC till del och har således inte införts och används inte som stöd av BC i samband med behörighetsbedömningar.

Behörighetsrevision
BC utför behörighetsrevisioner senast var 13:e månad. Behörighetsrevisionen kan initieras tidigare vid förändringar såsom byte av tjänst/avdelning/enhet, förändrade arbetsuppgifter eller förändrade arbetsförhållanden eller till följd av disciplinära åtgärder.
En förutsättning för att BC ska kunna genomföra behörighetsrevisioner tidigare är att BC får information om detta, vilket inte alltid sker enligt uppgift. Felaktig/ej uppdaterad information i PAP har också observerats i internrevisionens stickprovsgranskning, t.ex. felaktig uppgift om chef enligt PAP. Internrevisionens stickprov visade i ett stort antal fall där medarbetare hade kvar it-behörigheter som inte längre fanns behov av och i vissa fall högre behörigheter än nödvändigt. I stickproven fanns ett flertal exempel där tidigare poliser bytt tjänst till nationella avdelningar men där behörighet till de polisiära it-systemen fanns kvar. I vissa fall hade medarbetare it-behörigheter som man inte kände till och inte aktivt ansökt om.

I intervjuer har personal inom BC fört fram att det vid behörighetsrevisioner skulle underlätta om möjlighet fanns att se om slutanvändaren varit inaktiv i ett it-system i t.ex. 6 månader.

Bedömning
Internrevisionen gör den övergripande bedömningen att processen för tilldelning och revision av it-behörigheter inte är tillräcklig för att säkerställa kraven på att behörighet till polisens it-system endast ska på grundval av lämplighet, kunskap och behov i sitt arbete. Internrevisionen konstaterar att chefer normalt inte är involverade i samband med tilldelning och revision av medarbetarnas it-behörigheter. Internrevisionen anser att detta är en brist/nackdel då cheferna är de som har bäst kunskap om sina medarbetares lämplighet, kunskap och behov i sina arbetsuppgifter.

Information om förändrade anställningsförhållanden når inte alltid BC, vilket kan leda till felaktiga behörighetsbedömningar. Internrevisionen anser också att det är en brist att riktlinjer från informationsägare inte införts av BC som stöd för sina bedömningar. Detta då riktlinjerna bl.a. reglerar vilka verksamheter och funktioner som ska vara behöriga att ta del av och registrera uppgifter i respektive it-system. Det är av vikt att lathundar och PM som används av BC för sina bedömningar är tydliga och heltäckande för att kunna eftersträva en så enhetlig bedömning som möjligt. Utfallet från stickprovsgranskningen visade att många anställda har onödigt många it-behörigheter och i vissa fall högre it-behörigheter än nödvändigt för tjänsten. Detta anser internrevisionen kan medföra en ökad risk att anställda använder behörigheterna på ett otillbörligt sätt, t.ex. genom att göra slagningar i systemen. Det finns även en kostnadsaspekt att beakta.

Rekommendationer

Röd – Mycket väsentlig brist
Internrevisionen rekommenderar att: IT-avdelningen - I samråd med informationsägarna genomför riskbedömning och ser över i vilka situationer ytterligare kontrollmoment (chefsinvolvering) bör införas, t.ex. genom godkännande av avvikelser från behörighetsprofiler, vid ansökan om högre behörigheter till känsliga system och i samband med revision av personalens it-behörigheter - Efter genomförd riskbedömning införa relevanta kontroller (chefsinvolvering).

Konsekvenserna av om rekommendationerna inte följs är att det finns risk att känslig information används och sprids. Detta kan medföra stora negativa konsekvenser för Polismyndighetens verksamhet och innebära att Polismyndigheten inte uppfyller myndighetsförordningens krav på effektivitet, lagenlighet, redovisning och hushållning.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Chefen för IT-säkerhetsenheten, Josefine Östfeldt i samråd med chefen för IT-kundserviceenheten Petra Marcusson.
Åtgärder	Utredning pågår redan kring hur kontroller ska ske framöver, bl.a. genom att genomföra piloter för behörighetsrevision i verksamheten. Efter genomförda piloter och annan utredning kommer även en riskbedömning att göras. Därefter kommer beslut att fattas om vilka kontroller som ska införas.
Ansvarig	Chefen för IT-säkerhetsenheten, Josefine Östfeldt.
Tidsplan	2018-12-31

Orange – Väsentlig brist
Internrevisionen rekommenderar att: IT-avdelningen Säkerställer att det finns tydliga och fullständiga lathundar och PM för BC:s behörighetsbedömningar baserade på informationsägarnas riktlinjer för personuppgiftsbehandlingar samt att de redan befintliga riktlinjerna används som stöd för BC:s behörighetsbedömningar.

Konsekvensen av om rekommendationen inte följs är att det finns risk att känslig information används och sprids. Detta kan leda till att uppställda mål inte nås och/eller medför betydande negativa konsekvenser för verksamheten.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Chefen för IT-säkerhetsenheten, Josefine Östfeldt i samråd med chefen för IT-kundserviceenheten Petra Marcusson.
Åtgärder	Riktlinjer lämnas av respektive informationsägare på nationella avdelningar. Riktlinjer som berör behörighetshantering införs och följs skyndsamt av BC.
Ansvarig	Chefen för IT-kundserviceenheten Petra Marcusson.
Tidsplan	Åtgärdat avseende befintliga riktlinjer från informationsägare. Löpande arbete avseende kommande riktlinjer från informationsägare.

Orange – Väsentlig brist
Internrevisionen rekommenderar att: HR-avdelningen med stöd av IT-avdelningen Utreder möjligheten att PAP hämtar information gällande vilka som är chefer från BESTA-koden, i stället för från fritextfältet.

Konsekvensen av om rekommendationen inte följs är att det finns risk för att it-behörighetsbedömningar baseras på felaktiga uppgifter, att känslig information används och sprids. Detta kan leda till att uppställda mål inte nås och/eller medför betydande negativa konsekvenser för verksamheten.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	HR-avdelningen, avdelningskansli, analytikern Oscar Lundin.
Åtgärder	HR-avdelningen initierar en dialog med produktgruppen för Palasso i samråd med PAP-Förvaltningen i syfte att se över möjligheten att ändra från vilket fält i Palasso som PAP hämtar information från.
Ansvarig	HR-avdelningen, avdelningskansli, analytikern Oscar Lundin.
Tidsplan	Dialogen slutförd senast under våren (2018-05-31) med förhoppning om verkställande av ändring i PAP under 2018 (2018-12-31).

3.3 Ansvar och roller

Iakttagelser

Generellt
Ett flertal funktioner i myndigheten har ansvar och roller för olika delar i den nationella processen för tilldelning och revidering av it-behörigheter. Det råder dock otydlighet kring vem/vilken funktion som ytterst är ansvarig för slutanvändarnas it-behörigheter.

IT-avdelningens ansvar och roll
Enligt arbetsordningen[3] har it-avdelningen verksamhetsansvar för och chefen för avdelningen är tillika processägare för att bl.a. tillhandahålla it-tjänster till Polismyndighetens olika enheter och att införskaffa it-stöd och it-applikationer och införa dem i Polismyndighetens verksamhet.

I it-avdelningens handläggningsordning[4] framgår att enheten it-säkerhet har processansvaret för Polismyndighetens identitets- och åtkomsthantering samt att sektionen BC ansvarar för att genomföra löpande behörighetsförändringar.

[3] Arbetsordning för Polismyndigheten, PM 2017:43, 3 kap. 21§.
[4] Dnr A.010.199/2016

Enligt instruktion för BC har sektionen ansvar för att den nationella processen för behörighetshantering skall fungera i det dagliga linjearbetet och att alla som arbetar inom polisen får tillgång till de it-system som deras arbetsuppgifter kräver.
IT-avdelningens BC har enligt beslut[5] (2016-12-09) mandat att besluta om behörigheter till polisens system t.o.m. 2018-12-31.

Processägarens/informationsägarens ansvar och roll
En processägare har ett nationellt ansvar för en viss process inom hela myndigheten och för att processen säkerställer att resultat uppnås inom verksamheten. Processägare är också ansvarig för Polismyndighetens personuppgiftsbehandling inom sitt ansvarsområde, enligt arbetsordningen 3 kap. 3 §.

Avdelningarna ska enligt 3 kap. 16 § vara informationsägare och kravställare av it-system inom avdelningens ansvarsområde. Polismyndighetens informationsägare är ansvariga för den information som behandlas i ett it-system och för att information hanteras i enlighet med gällande författningar och Polismyndighetens styrdokument.

Enligt Polismyndighetens riktlinjer[6] har informationsägaren ett övergripande ansvar för att verksamheten behandlar information i enlighet med lag och förordning. Detta ska säkerställas bl.a. genom att ta fram styrdokument och andra verksamhetsrutiner som skapar förutsättningar för att behandlingen av personuppgifter ska kunna ske i enlighet med lag. I riktlinjen framgår bl.a. processansvariges skyldighet att besluta om styrdokument, omfattning och nyttjande av information, t.ex. regler kring i vilka verksamhetsdelar som information från it-system får nyttjas. Det ges i riktlinjerna även exempel på fördelning av arbetsuppgifter såsom att inom uppsatta ramar besluta om behörigheter samt att följa upp tilldelning av behörigheter. Det kan även ges instruktioner för bl.a. begränsningar av hur och till vem behörigheter får tilldelas.

Enligt intervjuer har de nationella avdelningarna kommit olika långt med arbetet att ta fram riktlinjer för personuppgiftsbehandlingar. Noa har kommit längst i detta arbete och det finns nu riktlinjer för de mest väsentliga it-systemen som Noa ansvarar för. Enligt uppgift återstår dock arbete med att ta fram motsvarande riktlinjer för de it-system som övriga nationella avdelningar ansvarar för.

Rättsavdelningens ansvar
Enligt 3 kap. 23 § arbetsordningen ska rättsavdelningen ha verksamhetsansvar för och chefen för avdelningen är tillika processägare för personuppgiftsfrågor. Hur långt rättsavdelningens ansvar med anledning av detta sträcker sig i behörighetsfrågorna är inte helt klart. Sett till att rättsavdelningen enligt samma bestämmelse ansvarar för den rättsliga styrningen och det juridiska stödet generellt i Polismyndigheten ligger det nära till hands att utgå från att frågor som rör en enhetlig tillämpning av behörighetskraven som ställs ur ett personuppgiftsperspektiv faller inom avdelningens ansvar.

Personuppgiftsombudets ansvar och roll
Enligt arbetsordningen, 4 kap. 5 § ska personuppgiftsombudet självständigt utöva tillsyn över personuppgiftsbehandlingar i myndigheten. I tillsynen ingår bl.a. att granska behö-

[5] Dnr.848.897/2016
[6] Polismyndighetens riktlinjer för den processansvariges styrdokument avseende ansvar för personuppgiftsbehandling, PM 2016:37.

righetstilldelningar. Enligt intervju med personuppgiftsombudet genomförs detta på ett övergripande sätt genom att granska anmälningar om personuppgiftsbehandlingar, processägares riktlinjer om personuppgiftsbehandlingar samt genom att aktivt delta vid extern tillsyn och omhänderta synpunkter och iakttagelser från dessa.

Medarbetarens chefs ansvar och roll
I arbetsordningen, 5 kap. 8 §, Allmänt för chefer, framgår att ”Varje chef ska ha ansvar för att arbetet bedrivs enligt gällande författningar, avtal och styrdokument”. Därutöver framgår det i Noa:s riktlinjer avseende ansvar för personuppgiftsbehandlingar för de flesta it-system, som de är informationsägare för, vem som ansvarar för behörighetstilldelningen. För de it-system som annan avdelning än Noa har ansvar för saknas dock motsvarande reglering.

Bedömning
Internrevisionen anser att den nuvarande fördelningen av ansvar och roller inte är tillräckligt tydlig vad gäller processägares/informationsägares ansvar och roll i förhållande till övriga chefers roll och ansvar för medarbetares it-behörigheter. Chefers ansvar för detta borde utökas i enlighet med rekommendation 3.2 och ansvaret att informera om förändrade arbetsförhållanden borde tydliggöras. Internrevisionen anser att detta skulle leda till en mer rättssäker tilldelning och revision av behörigheter. Det är för internrevisionen oklart om det t.ex. finns ett ansvar för chef att meddela förändrade arbetsuppgifter för sin personal. Internrevisionen konstaterar att det finns brister vad gäller processägares/informationsägares ansvar för att verksamheten behandlar information i enlighet med lag och förordning. Avsaknad av riktlinjer för personuppgiftsbehandlingar där bl.a. regler kring behörighetstilldelning och uppföljning av behörigheter ingår ökar risken för en alltför extensiv behörighetstilldelning.

Rekommendationer

Orange - Väsentlig brist
Internrevisionen rekommenderar att: IT-avdelningen - Tar fram en övergripande riktlinje eller motsvarande som beskriver ansvar och roller, och specifikt tydliggör hur processägarens/informationsägarens ansvar och roll förhåller sig till övriga chefers ansvar och roll för säkerställande av personalens it-behörigheter.

Konsekvensen av om rekommendationen inte följs är en fortsatt otydlighet kring ansvar för medarbetares it-behörigheter vilket negativt påverkar säkerställandet av en korrekt behörighetstilldelning och revision av densamma. Detta kan leda till att uppställda mål inte nås och medför betydande negativa konsekvenser för verksamheten.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Chefen för IT-säkerhetsenheten, Josefine Östfeldt.
Åtgärder	Polismyndighetens riktlinjer för säkerhet avseende informationsbehandling med stöd av IT beskriver i kapitel 4 Roller och ansvar vad som gäller för informationsägarens ansvar gällande behörigheter. Rollen processansvarig beskrivs i Polismyndighetens arbets-

	ordning. Processdokument för den nationella behörighetsprocessen, där en utförligare beskrivning av ansvar och roller framgår, är under framtagande och ska beslutas.
Ansvarig	Chefen för IT-säkerhetsenheten, Josefine Östfeldt.
Tidsplan	2018-09-30.

Orange - Väsentlig brist
Internrevisionen rekommenderar att: Nationella avdelningar (i form av informationsägare) -Tar fram riktlinjer för personuppgiftsbehandlingar som bl.a. reglerar till vem och hur tilldelning av it-behörigheter ska ske samt uppföljning av detta.

Konsekvensen av om rekommendationen inte följs är en fortsatt otydlighet kring ansvar för medarbetares it-behörigheter vilket negativt påverkar säkerställandet av en korrekt behörighetstilldelning och revision av densamma. Detta kan leda till att uppställda mål inte nås och medför betydande negativa konsekvenser för verksamheten.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Liselott Ringborg, enhetschef rättsavdelningen.
Åtgärder	Rättsavdelningen säkerställer att det finns riktlinjer för personuppgiftsbehandlingar kopplat till system rättsavdelningen är ansvarig för. Detta med undantag av de system som ska termineras under 2018.
Ansvarig	Ansvarig rättsavdelningen, Liselott Ringborg.
Tidsplan	2018-12-31.

Kommentarer till lämnad rekommendation eller planerade åtgärder:
Rättsavdelningen rekommenderar att it-avdelningen även får ansvara för att upprätthålla en aktuell förteckning över informationsägare och produktägare. Finns en förteckning med informationsägare från 2015 som börjar bli inaktuell.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Nationellt forensiskt centrum
Åtgärder	Skapa en nationell riktlinje där ansvaret för personuppgiftsbehandlingen i hela den forensiska verksamheten inom polisen beskrivs. I dokumentet kommer det att framgå vilka funktioner som får ha tillgång till olika forensiska system, uppföljande

	åtgärder och vidare vem som svarar för uppföljande åtgärder.
Ansvarig	Liselotte Nielsen Sundberg
Tidsplan	Vi har för avsikt att färdigställa riktlinjen under 2018.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Ekonomiavdelningen/Finansiell styrning/Gruppen för utvecklings-samordning och informationsägarskap, Malin Löfström Nord
Åtgärder	Ekonomiavdelningen kommer att påbörja arbetet med att ta fram riktlinjer för personuppgiftsbehandlingar och aktuella mallar för arbetet (inkl reglering och tilldelning av it-behörigheter och uppföljning) kopplade till avdelningens verksamhet. Dock är ekonomiavdelningen, precis som övriga nationella avdelningar beroende av it-avdelningens övergripande riktlinje (som är under framtagande).
Ansvarig	Ekonomiavdelningens grupp för utvecklingssamordning och informationsägarskap, tillsammans med aktuella verksamhets-ansvariga inom avdelningen.
Tidsplan	Tidsplanen är att det ska göras under 2018 och vara klart senast 31 december 2018.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	HR-avdelningen, avdelningskansli, analytikern Oscar Lundin
Åtgärder	HR-avdelningen ser över vilka befintliga riktlinjer och rutiner som finns för de system som avdelningen, i egenskap av informationsägare, ansvarar för. Befintliga riktlinjer och rutiner kompletteras vid behov och i de fall befintliga riktlinjer och rutiner saknas tas sådana fram.
Ansvarig	HR-avdelningen, avdelningskansli, kanslichefen Jenny Hedqvist.
Tidsplan	Genomgång av befintliga riktlinjer och rutiner senast den 30 april 2018. Framtagande av eventuellt nya eller komplettering av befintliga riktlinjer och rutiner slutförs senast den 29 juni 2018.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	KA, Produktionsenheten, tf chef enhet, Susanne Hammarberg
Åtgärder	Riktlinjer ska tas fram för de it-system som KA är information-sägare för.
Ansvarig	Anders Vessman
Tidsplan	Uppdraget ska vara genomfört senast 2018-12-30, delrapportering ska ske senast 2018-06-30 till chefen för produktionsenheten.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Patrick Cordner, Utredningsenheten/Noa Karin Elmström, Beredningsenheten/Noa
Åtgärder	Utredningsenheten ska snarast revidera sina riktlinjer och komplettera med de delar som saknas utifrån tidigare beslut av C Noa. I övrigt finns inom Noa riktlinjer för det framtagna och beslutade.
Ansvarig	Samtliga enhetschefer för sina respektive system
Tidsplan	2018-12-31.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Chefen för IT-säkerhetsenheten, Josefine Östfeldt
Åtgärder	Att se över behovet av riktlinjer för de it-system där it-avdelningen är informationsägare, samt tillse att riktlinjer tas fram i relevanta fall.
Ansvarig	Berörd produktägare inom IT-avdelningen.
Tidsplan	2019-06-30.

INTERNREVISIONEN

Carl Ygge Stefan Carp

Polisen

Beslutsprotokoll

Datum
2018-04-13

Diarienr, ärende	Saknr	Protokoll nr/år
A105.760/2017	977	RPC1/2018

Beslutande	Föredragande
Rikspolischefen Anders Thornberg	Enhetschefen Petra Marcusson

Övriga som deltagit i den slutliga handläggningen
Avdelningschefen Martin Valfridsson
Internrevisionschefen Stina N Kristiansson
Kanslichefen Liselotte Nielsen Sundberg
Biträdande avdelningschefen Britt Rehnberg
Kanslichefen Jenny Hedqvist
Tf. enhetschefen Susanne Hammarberg
Enhetschefen Christer Nilsson
Enhetschefen Liselott Ringborg

Ärende
Beslut om åtgärder med anledning av internrevisionens granskning av polisens hantering av behörighet till it-system, rapportutkast 2018-02-26.

Beslut
Internrevisionen har genomfört en granskning av polisens hantering av behörighet till it-system. Granskningen har resulterat i ett antal iakttagelser och rekommendationer. Verksamheten har lämnat förslag till åtgärder i anledning av rekommendationerna.

Polismyndigheten beslutar avseende internrevisionens
rekommendationer i avsnitt 3.1 att
It-avdelningen (IT) ska vidta följande åtgärder: Den nationella behörighetsprocessen ska vara beslutad senast 2018-09-30. Övriga punkter utförs löpande och förbättringsarbetet under 2018 kommer att följas upp med avstämning senast 2019-02-28. IT, chefen för it-säkerhetsenheten ansvarar för åtgärdernas genomförande.

HR-avdelningen (HR) ska vidta åtgärder för förändrade administrativa rutiner som möjliggör att samlade underlag kan lämnas i så god tid som möjligt till behörighetscenter. Åtgärderna ska vara genomförda 2018-10-01. HR, Kompetensutveckling, enhetschefen ansvarar för åtgärdernas genomförande.

rekommendationer i avsnitt 3.2 att
IT ska vidta följande åtgärder: Utredning pågår redan kring hur kontroller ska ske framöver, bl.a. genom att genomföra piloter för behörighetsrevision i verksamheten. Efter genomförda piloter och annan utredning kommer även en riskbedömning att göras. Därefter kommer beslut att fattas om vilka kontroller som ska införas. Åtgärdernas ska vara genomförda 2018-12-31. IT, chefen för it-säkerhetsenheten ansvarar för åtgärdernas genomförande. (IT har åtgärdat avseende befintliga riktlinjer från informationsägare. Löpande arbete avseende kommande riktlinjer från informationsägare. IT, chefen för it-kundserviceenheten ansvarar för åtgärdernas genomförande).

HR ska vidta följande åtgärder: initierar en dialog med produktgruppen för Palasso i samråd med PAP-Förvaltningen i syfte att se över möjligheten att ändra från vilket fält i Palasso som PAP hämtar information från. Dialogen slutförd senast under våren (2018-05-31) med förhoppning om verkställande av ändring i PAP under 2018 (2018-12-31). HR, avdelningskansli ansvarar för åtgärdernas genomförande.

rekommendationer i avsnitt 3.3 att

IT ska vidta följande åtgärder: Processdokument för den nationella behörighetsprocessen, där en utförligare beskrivning av ansvar och roller framgår, är under framtagande och ska beslutas. Åtgär-

den ska vara genomförd 2018-09-30. It, chefen för it-säkerhetsenheten ansvarar för åtgärdens genomförande.

IT ser över behovet av riktlinjer för de it-system där it-avdelningen är informationsägare, samt tillse att riktlinjer tas fram i relevanta fall. Åtgärder ska vara genomförda 2019-06-30. Berörda produktägare inom IT-avdelningen ansvarar för åtgärdernas genomförande.

Rättsavdelningen (RA) ska vidta följande åtgärder: RA säkerställer att det finns riktlinjer för personuppgiftsbehandlingar kopplat till system rättsavdelningen är ansvarig för. Detta med undantag av de system som ska termineras under 2018. Åtgärderna ska vara genomförda 2018-12-31. RA, enhetschefen för informationsförvaltningen ansvarar för åtgärdernas genomförande.

Nationellt Forensiskt Centrum (NFC) ska vidta följande åtgärder: NFC skapar en nationell riktlinje där ansvaret för personuppgiftsbehandlingen i hela den forensiska verksamheten inom polisen beskrivs. I dokumentet kommer det att framgå vilka funktioner som får ha tillgång till olika forensiska system, uppföljande åtgärder och vidare vem som svarar för uppföljande åtgärder. Åtgärden ska vara genomförd under 2018. NFC, kanslichefen ansvarar för åtgärdens genomförande.

Ekonomiavdelningen (EA) ska vidta följande åtgärder: EA påbörjar arbetet med att ta fram riktlinjer för personuppgiftsbehandlingar och aktuella mallar för arbetet (inklusive reglering och tilldelning av it-behörigheter och uppföljning) kopplade till avdelningens verksamhet. Åtgärden ska vara genomförd senast 2018-12-31. EA:s grupp för utvecklingssamordning och informationsägarskap, tillsammans med aktuella verksamhetsansvariga inom avdelningen är ansvariga för åtgärdernas genomförande.

HR ska vidta följande åtgärder: HR ser över vilka befintliga riktlinjer och rutiner som finns för de system som avdelningen, i egenskap av informationsägare, ansvarar för. Befintliga riktlinjer och rutiner kompletteras vid behov och i de fall befintliga riktlinjer och rutiner saknas, tas sådana fram. Genomgång av befintliga riktlinjer och rutiner senast 2018-04-30. Framtagande av eventuellt nya eller komplettering av befintliga riktlinjer och rutiner slutförs senast 2018-06-29. HR, kanslichefen ansvarar för åtgärdernas genomförande.

Kommunikationsavdelningen (KA) ska vidta följande åtgärder: KA tar fram riktlinjer för de it-system som KA är informationsägare för. Uppdraget ska vara genomfört senast 2018-12-30, delrapportering ska ske senast 2018-06-30 till chefen för produktionsenheten. KA, enhetschefen för produktion ansvarar för åtgärdernas genomförande.

Nationella operativa avdelningen (Noa), Utredningsenheten reviderar snarast sina riktlinjer och komplettera med de delar som saknas utifrån tidigare beslut. I övrigt finns inom Noa riktlinjer för det framtagna och beslutade. Åtgärderna ska vara genomförda 2018-12-31. Noa, samtliga enhetschefer vid utredningsenheten ansvarar för åtgärdernas genomförande för sina respektive system.

Kostnad	Finansiering
Inom budget	Inom budget

Vid protokollet

Petra Marcusson

Justeras

Anders Thornberg

Sändlista	Kopia till

Bilaga till

Internrevisionens granskning av polisens hantering av behörighet till it-system

Sammanställning av inkomna svar

2018-04-16

Internrevisionens granskning av polisens hantering av behörighet till it-system

Förslag på åtgärder m.a.a. internrevisionens granskning har i huvudsak inhämtats av Rikspolischefens kansli. Förslag har inhämtats från nationella avdelningar (it-avdelningen samt nationella avdelningar i rollen som informationsägare).

Denna sammanställning innehåller inkomna förslag på åtgärder. Sammanställningen följer rapportens huvudrubriker och förslagen återfinns under respektive rekommendation.

INNEHÅLL

3 Granskning av polisens hantering av behörighet till it-system

3.1 Processen för behörighetshantering

Rekommendationer

Gul – Mindre väsentlig brist
Internrevisionen rekommenderar att: IT-avdelningen - Vidtar åtgärder för att så långt möjligt all behörighetshantering lyfts över till BC - Så långt möjligt få fler it-system att bli integrerade med PAP - Färdigställer och formaliserar processdokument och instruktion för BC - I samråd med informationsägarna förbättrar utformningen av ansökan om it-behörigheter i PAP, t.ex. tvingande motivering vid ansökan om känsliga system, underlätta ansökan, bättre hjälp vid ansökan till it-system med många olika behörigheter såsom t.ex. PÄr - Skapar behörighetsprofiler för flera funktioner inom myndigheten samt gör översyn av befintliga behörighetsprofiler.

Konsekvenserna av om rekommendationerna inte följs är en ineffektiv och ej enhetlig behörighetshantering. Detta kan medföra negativa konsekvenser för verksamheten.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Chefen för IT-säkerhetsenheten, Josefine Östfeldt i samråd med chefen för IT-kundserviceenheten Petra Marcusson.
Åtgärder	- För varje systemanslutning görs en bedömning om all behörighetshantering ska ligga hos BC, vilket är utgångspunkten. Det kan dock finnas tillfällen då det inte är möjligt tex pga att behörigheter endast kan läggas upp på en specifik dator eller att det är mycket känsliga uppgifter. Det är därför inte möjligt att lyfta över all behörighetshantering till BC. - För varje systemanslutning görs en bedömning om systemet ska helintegreras med PAP, vilket är intentionen. Det kan dock finnas tekniska skäl till att en integration inte är möjlig, eller att det är mycket få användare av ett system och det inte är ekonomiskt försvarbart att integrera. - Processdokument för den nationella behörighetsprocessen ska färdigställas och beslutas. För övriga instruktioner för BC uppdateras dessa kontinuerligt av process- och dokumentansvarig på BC. - Förbättringar i PAP hanteras löpande i Behörighetsforum som leds av IT-säkerhetsenheten. - Fler och förbättrade behörighetsprofiler förbättras löpande i den sk MUG gruppen (MetodUtvecklingsGruppen) inom BC och beslutas av IT-säkerhetsenheten.

Ansvarig	Chefen för IT-säkerhetsenheten, Josefine Östfeldt.
Tidsplan	Den nationella behörighetsprocessen ska vara beslutad senast 2018-09-30. Övriga punkter utförs löpande och förbättringsarbetet under 2018 kommer att följas upp med avstämning senast 2019-02-28.

Gul – Mindre väsentlig brist
Internrevisionen rekommenderar att: HR-avdelningen - Ser över möjligheter till förändrad behörighetshantering av polisstudenter.

Konsekvenserna av om rekommendationen inte följs är en ineffektiv och ej enhetlig behörighetshantering. Detta kan medföra negativa konsekvenser för verksamheten.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	HR-avdelningen, avdelningskansli, analytikern Oscar Lundin.
Åtgärder	HR-avdelningen vidtar åtgärder för förändrade administrativa rutiner som möjliggör att samlade underlag kan lämnas i så god tid som möjligt till behörighetscenter.
Ansvarig	HR-avdelningen, Kompetensutveckling, enhetschefen Anna Orhall.
Tidsplan	Genomfört 1 oktober 2018

Eventuella kommentarer till lämnad rekommendation eller planerade åtgärder:
Studenter är i behov av vissa behörigheter under polisutbildningen vid lärosätena. Under aspirantutbildningen som genomförs vid polisregionerna är studenterna tillfälligt anställda i Polismyndigheten och har då behov av utökade behörigheter. Vid anställning som polisassistenter förändras återigen behovet av behörigheter.

3.2 Säkerställande av rätt it-behörigheter

Rekommendationer

Röd – Mycket väsentlig brist
Internrevisionen rekommenderar att: IT-avdelningen - I samråd med informationsägarna genomför riskbedömning och ser över i vilka situationer ytterligare kontrollmoment (chefsinvolvering) bör införas, t.ex. genom godkännande av avvikelser från behörighetsprofiler, vid ansökan om högre behörigheter till känsliga system och i samband med revision av personalens it-behörigheter - Efter genomförd riskbedömning införa relevanta kontroller (chefsinvolvering).

Konsekvenserna av om rekommendationerna inte följs är att det finns risk att känslig information används och sprids. Detta kan medföra stora negativa konsekvenser för Polismyndighetens verksamhet och innebära att Polismyndigheten inte uppfyller myndighetsförordningens krav på effektivitet, lagenlighet, redovisning och hushållning.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Chefen för IT-säkerhetsenheten, Josefine Östfeldt i samråd med chefen för IT-kundserviceenheten Petra Marcusson.
Åtgärder	Utredning pågår redan kring hur kontroller ska ske framöver, bl.a. genom att genomföra piloter för behörighetsrevision i verksamheten. Efter genomförda piloter och annan utredning kommer även en riskbedömning att göras. Därefter kommer beslut att fattas om vilka kontroller som ska införas.
Ansvarig	Chefen för IT-säkerhetsenheten, Josefine Östfeldt.
Tidsplan	2018-12-31

Orange – Väsentlig brist

Internrevisionen rekommenderar att:

IT-avdelningen

Säkerställer att det finns tydliga och fullständiga lathundar och PM för BC:s behörighetsbedömningar baserade på informationsägarnas riktlinjer för personuppgiftsbehandlingar samt att de redan befintliga riktlinjerna används som stöd för BC:s behörighetsbedömningar.

Konsekvensen av om rekommendationen inte följs är att det finns risk att känslig information används och sprids. Detta kan leda till att uppställda mål inte nås och/eller medför betydande negativa konsekvenser för verksamheten.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Chefen för IT-säkerhetsenheten, Josefine Östfeldt i samråd med chefen för IT-kundserviceenheten Petra Marcusson.
Åtgärder	Riktlinjer lämnas av respektive informationsägare på nationella avdelningar. Riktlinjer som berör behörighetshantering införs och följs skyndsamt av BC.
Ansvarig	Chefen för IT-kundserviceenheten Petra Marcusson.
Tidsplan	Åtgärdat avseende befintliga riktlinjer från informationsägare. Löpande arbete avseende kommande riktlinjer från informationsägare.

Orange – Väsentlig brist
Internrevisionen rekommenderar att: HR-avdelningen med stöd av IT-avdelningen Utreder möjligheten att PAP hämtar information gällande vilka som är chefer från BESTA-koden, i stället för från fritextfältet.

Konsekvensen av om rekommendationen inte följs är att det finns risk för att it-behörighetsbedömningar baseras på felaktiga uppgifter, att känslig information används och sprids. Detta kan leda till att uppställda mål inte nås och/eller medför betydande negativa konsekvenser för verksamheten.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	HR-avdelningen, avdelningskansli, analytikern Oscar Lundin.
Åtgärder	HR-avdelningen initierar en dialog med produktgruppen för Palasso i samråd med PAP-Förvaltningen i syfte att se över möjligheten att ändra från vilket fält i Palasso som PAP hämtar information från.
Ansvarig	HR-avdelningen, avdelningskansli, analytikern Oscar Lundin.
Tidsplan	Dialogen slutförd senast under våren (2018-05-31) med förhoppning om verkställande av ändring i PAP under 2018 (2018-12-31).

3.3 Ansvar och roller

Rekommendationer

Orange - Väsentlig brist
Internrevisionen rekommenderar att: IT-avdelningen - Tar fram en övergripande riktlinje eller motsvarande som beskriver ansvar och roller, och specifikt tydliggör hur processägarens/informationsägarens ansvar och roll förhåller sig till övriga chefers ansvar och roll för säkerställande av personalens it-behörigheter.

Konsekvensen av om rekommendationen inte följs är en fortsatt otydlighet kring ansvar för medarbetares it-behörigheter vilket negativt påverkar säkerställandet av en korrekt behörighetstilldelning och revision av densamma. Detta kan leda till att uppställda mål inte nås och medför betydande negativa konsekvenser för verksamheten.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Chefen för IT-säkerhetsenheten, Josefine Östfeldt.
Åtgärder	Polismyndighetens riktlinjer för säkerhet avseende informationsbehandling med stöd av IT beskriver i kapitel 4 Roller och ansvar vad

	som gäller för informationsägarens ansvar gällande behörigheter. Rollen processansvarig beskrivs i Polismyndighetens arbetsordning. Processdokument för den nationella behörighetsprocessen, där en utförligare beskrivning av ansvar och roller framgår, är under framtagande och ska beslutas.
Ansvarig	Chefen för IT-säkerhetsenheten, Josefine Östfeldt.
Tidsplan	2018-09-30.

Orange - Väsentlig brist

Internrevisionen rekommenderar att:

Nationella avdelningar (i form av informationsägare)

-Tar fram riktlinjer för personuppgiftsbehandlingar som bl.a. reglerar till vem och hur tilldelning av it-behörigheter ska ske samt uppföljning av detta.

Konsekvensen av om rekommendationen inte följs är en fortsatt otydlighet kring ansvar för medarbetares it-behörigheter vilket negativt påverkar säkerställandet av en korrekt behörighetstilldelning och revision av densamma. Detta kan leda till att uppställda mål inte nås och medför betydande negativa konsekvenser för verksamheten.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Liselott Ringborg, enhetschef rättsavdelningen.
Åtgärder	Rättsavdelningen säkerställer att det finns riktlinjer för personuppgiftsbehandlingar kopplat till system rättsavdelningen är ansvarig för. Detta med undantag av de system som ska termineras under 2018.
Ansvarig	Ansvarig rättsavdelningen, Liselott Ringborg.
Tidsplan	2018-12-31.

Kommentarer till lämnad rekommendation eller planerade åtgärder:
Rättsavdelningen rekommenderar att it-avdelningen även får ansvara för att upprätthålla en aktuell förteckning över informationsägare och produktägare. Finns en förteckning med informationsägare från 2015 som börjar bli inaktuell.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Nationellt forensiskt centrum
Åtgärder	NFC har idag styrande dokument i sitt kvalitetsledningssystem som beskriver behörighetstilldelning för ärendehanteringssystemet Forum, DNA-registret och andra typer av referensregister i NFC:s verksamhet. Vi har dock påbörjat ett arbete med att i den mall som tagits fram av RA skapa en nationell riktlinje där vi beskriver ansvaret för per-

	sonuppgiftsbehandlingen i hela den forensiska verksamheten inom polisen. I dokumentet kommer det att framgå vilka funktioner som får ha tillgång till olika forensiska system, uppföljande åtgärder och vidare vem som svarar för uppföljande åtgärder.
Ansvarig	Liselotte Nielsen Sundberg
Tidsplan	Vi har för avsikt att färdigställa riktlinjen under 2018.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Ekonomiavdelningen/Finansiell styrning/Gruppen för utvecklings-samordning och informationsägarskap, Malin Löfström Nord
Åtgärder	Ekonomiavdelningen kommer att påbörja arbetet med att ta fram riktlinjer för personuppgiftsbehandlingar och aktuella mallar för arbetet (inkl reglering och tilldelning av it-behörigheter och uppföljning) kopplade till avdelningens verksamhet. Dock är ekonomiavdelningen, precis som övriga nationella avdelningar beroende av it-avdelningens övergripande riktlinje (som är under framtagande).
Ansvarig	Ekonomiavdelningens grupp för utvecklingssamordning och informationsägarskap, tillsammans med aktuella verksamhets-ansvariga inom avdelningen.
Tidsplan	Tidsplanen är att det ska göras under 2018 och vara klart senast 31 december 2018.

Kommentarer till lämnad rekommendation eller planerade åtgärder: Det är viktigt att övriga nationella avdelningars riktlinjer grundar sig på it-avdelningens övergripande riktlinje, för att skapa enhetlighet.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	HR-avdelningen, avdelningskansli, analytikern Oscar Lundin
Åtgärder	HR-avdelningen ser över vilka befintliga riktlinjer och rutiner som finns för de system som avdelningen, i egenskap av informationsägare, ansvarar för. Befintliga riktlinjer och rutiner kompletteras vid behov och i de fall befintliga riktlinjer och rutiner saknas tas sådana fram.
Ansvarig	HR-avdelningen, avdelningskansli, kanslichefen Jenny Hedqvist.
Tidsplan	Genomgång av befintliga riktlinjer och rutiner senast den 30 april 2018. Framtagande av eventuellt nya eller komplettering av befintliga riktlinjer och rutiner slutförs senast den 29 juni

	2018.
Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	KA, Produktionsenheten, tf chef enhet, Susanne Hammarberg
Åtgärder	Intrapolis. Nya riktlinjer tas fram av KA. Ny PUO-anmälan görs av KA i samband med GDPR. Polisens webbplatser: Nya riktlinjer tas fram av KA. Ny PUO-anmälan görs av KA i samband med GDPR. Polisens konton i sociala medier: Ny handbok sociala medier tas fram av KA. I handboken beskrivs bland annat vad som får publiceras, ägarskap, administration och kontohantering inklusive behörighets-hantering. Bildbanken Exigus. PUO-anmälan (motsvarande) görs av KA i samband med GDPR. Personuppgiftsbiträdesavtal (motsvarande) tecknas av KA med den leverantör som sköter driften av Exigus. KA tar fram riktlinjer för personuppgifter i Exigus. KA tar fram beskrivning av behörighetshantering och revision av behörigheter. Siteimprove. PUO-anmälan (motsvarande) i samband med GDPR. Personuppgiftsbiträdesavtal (motsvarande) tecknas av KA med den leverantör som sköter driften av Siteimprove. KA tar fram beskrivning av behörighetshantering och revision av behörigheter. Prenumerantregistret för Svensk Polis (externa prenumeranter). PUO-anmälan (motsvarande) görs av KA i samband med GDPR. KA tar fram riktlinjer för personuppgifter i prenumerantregistret. KA tar fram beskrivning av behörighetshantering och revision av behörigheter. Relationdesk. PUO-anmälan (motsvarande) görs av KA i samband med GDPR. Personuppgiftsbiträdesavtal (motsvarande) tecknas av KA med den leverantör som sköter driften av Relationdesk. KA tar fram beskrivning av behörighetshantering och revision av behörigheter.
Ansvarig	Anders Vessman
Tidsplan	Uppdraget ska vara genomfört senast 2018-12-30, delrapportering ska ske senast 2018-06-30 till chefen för produktionsenheten.

Kommentarer till lämnad rekommendation eller planerade åtgärder:
Vi håller med om att riktlinjer kan krävas för system som nationella avdelningar är informationsägare för. De system som KA ansvarar för ska inte hantera känsliga personuppgifter så tyngdpunkten i riktlinjerna kommer att vara vilka personuppgifter som får behandlas.
Vi bedömer att den revision som görs av behörighetscenter senast var 13:e månad är tillräcklig med tanke på att de system som KA är informationsägare för inte innehåller känsliga personuppgifter och KA kommer därför inte tillföra ytterligare revision av behörigheter för dessa system. För revidering i samband med att en person slutar eller byter tjänst bör HR ha en rutin för att informera behörighetscenter.
För polisens konton i sociala medier bedömer vi att PUO-anmälan inte ska göras i och med att

det är externa parter som äger och ansvarar för systemen som används.
Systemet Siteimprove används för kvalitetskontroll av innehållet på polisen.se. Det är en extern leverantör som tillhandahåller systemet och ansvarar för driften. I Siteimprove finns personuppgifter i form av namn och e-postadresser för behöriga användare
Systemet Relationdesk används för hantering av inlägg på polisens nationella Facebook-sida. Det är en extern leverantör som tillhandahåller systemet och ansvarar för driften. I Relationdesk finns personuppgifter i form av namn och e-postadresser för behöriga användare
För de externa systemen inklusive polisens konton i sociala medier sker behörighetsadministration inte via PAP utan via andra rutiner.
Google Analytics och Webtrends är två system som används av KA men det är sannolikt IT-avdelningen som är informationsägare och ska svara för åtgärderna. Google Analytics är ett externt system. I de båda systemen finns personuppgifter i form av namn och e-postadresser för behöriga användare. Dessutom hanteras IP-nummer i insamlingen av statistik.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Karin Elmström, Beredningsenheten/Noa Patrick Cordner, Utredningsenheten/Noa
Åtgärder	Inom Noa finns riktlinjer för det framtagna och beslutade. Däremot ska de löpande ses över och revideras vid förändring, vilket åligger respektive processägare enligt arbetsordning. Noa ansvarar för de brottsbekämpande systemen. Utredningsenheten ska snarast revidera sina riktlinjer och komplettera med de delar som saknas utifrån beslut av C Noa A274.991/2017 saknr 12. Ansvarig för detta är C Utredningsenheten.
Ansvarig	Samtliga enhetschefer för sina respektive system
Tidsplan	2018-12-31.

Åtgärder med anledning av internrevisionens rekommendation	
Svar lämnat av	Chefen för IT-säkerhetsenheten, Josefine Östfeldt
Åtgärder	Att se över behovet av riktlinjer för de it-system där it-avdelningen är informationsägare, samt tillse att riktlinjer tas fram i relevanta fall.
Ansvarig	Berörd produktägare inom IT-avdelningen.
Tidsplan	2019-06-30.