Omsorg och äldreförvaltningen
Enheten för IT och e-Hälsa
John Fristedt

2017-03-05

Diarie nr

Socialtjänster i molnet

E-hälsa utvecklar vård och omsorg, socialtjänst. Genom att ta vara på digitaliseringens möjligheter kan vi öka kvaliteten för patienter och brukare och få en mer jämlik socialtjänst samt använda resurserna mer effektivt.
Som en del i att möta den enskildes individuella behov på ett mer mångfacetterat sätt har Linköpings kommun beslutat att införa välfärdsteknik-tjänster som ett komplement till traditionella insatser.

Tillsyn på annat sätt kan vara att erbjuda den enskilde tillsynen via sensorer eller via en trygghetskamera. För att säkerställa att kvalitén och att den enskildes trygghet och säkerhet prioriteras, har ett flertal kriterier identifierats. Omsorgskontoret har vidtagit ett flertal åtgärder innan den nya välfärds-tekniken blir tillgänglig för den enskilde och verksamheterna.

Åtgärderna bedrivs på flera olika strukturella nivåer, dessa är:

Ledning och styrning samt metodutveckling

- Testbäddar – vård och omsorgsverksamhet som provar och utvärderar olika tjänster och arbetssätt är basen i utvecklingsarbetet
- Utvecklingen och införandet - nya arbetssätt styrs av projektledaren och metoderna baseras på ett processorienterat förhållningssätt
- Delaktig – patienter och brukare samt verksamheter har beskrivit behoven av välfärdsteknik som komplement till befintliga insatser
- Riktlinje för användande av välfärdsteknik - har framställts tillsammans med biståndsbedömare och verksamhet

Informationssäkerhet och riskanalys

- Linköpings kommun säkerhetsgrupp har definierat metoder för informationsklassificering och riskanalys. Omsorgskontoret använder dessa verktyg för att kunna göra bedömningar av informationens känslighet och värna om den enskildes integritet på ett systematiskt sätt.
- Den nya dataskyddsförordningen kommer att ställa särskilda krav på kommunerna avseende information som har bäring på personuppgifter och den beaktas därför särskilt.
- Leverantörernas ansvar och åtaganden är långtgående avseende hantering av känsliga uppgifter i våra verksamheter och regleras därför tydligt i avtal.

För att säkerställa att ovanstående åtgärder har rätt innehåll och kvalité har omsorgskontoret anlitat välrenommerad leverantör i form av Certezza.

Bilaga – Socialtjänster i molnet.

Titel & kund-/projektnamn Linköpings kommun; Socialtjänster i molnet		
Skapad 2017-03-07	**Senast ändrad** 2017-03-07	**Version** 1.0
Författare Thomas Nilsson, Conny Balazs, Magnus Hûbner	**Dokumentansvarig/Godkänd** Thomas Nilsson	**Säkerhetsklass** Intern

Socialtjänster i molnet

Linköpings kommun, Omsorgskontoret

Titel & kund-/projektnamn Linköpings kommun; Socialtjänster i molnet		CERTEZZA
Skapad 2017-03-07	**Senast ändrad** 2017-03-07	**Version** 1.0
Författare Thomas Nilsson, Conny Balazs, Magnus Hûbner	**Dokumentansvarig/Godkänd** Thomas Nilsson	**Säkerhetsklass** Intern

Innehållsförteckning

Titel & kund-/projektnamn Linköpings kommun; Socialtjänster i molnet		
Skapad 2017-03-07	**Senast ändrad** 2017-03-07	**Version** 1.0
Författare Thomas Nilsson, Conny Balazs, Magnus Hûbner	**Dokumentansvarig/Godkänd** Thomas Nilsson	**Säkerhetsklass** Intern

Saken

Socialtjänsten i Linköpings kommun genomför en granskning av PUB-avtal i ett PUA perspektiv. Syftet är att granska molntjänster samt använda vedertagna metoder för riskanalys kopplat till tidigare genomförd informationsklassning. Uppdraget till Certezza omfattar metodstöd och bistå med expertkunskaper avseende värlfärdsteknologi, PuA´s åtagande, PuB-avtal, riskanalys samt genomförande av dessa.

Bakgrund

Socialtjänsten står inför nyttjande av molntjänster. Syftet är att lagra informationsmängder hos externa leverantörer. Linköpings kommun har tidigare genomfört en informationsklassning av de informationsmängder som kommunen hanterar i sina processer (bifogas separat).

Mål

Sammanfatta kommunens arbete avseende informationsklassning ur ett KLASSA-perspektiv, genomföra riskanalys samt säkerställa att det ligger i linje med EUs dataskyddsförordning.

Beställare

John Fristedt, Omsorgskontoret, Linköpings kommun.

Leveransobjekt

Underlag som utgör stöd i samband med att kommunen planerar att lagra informationsmängder i olika molntjänster.

Metodik

I allt informationssäkerhetsarbete ska:

- Informationstillgången identifieras
- Ägandeskap fastställas
- Externa och interna krav tydliggöras
    - Ex regulatoriska krav, verksamhetskrav

- Klassificering minst utifrån perspektiven konfidentialitet, riktighet och spårbarhet
    - Med fördel med dem av SIS/MSB/SKL föreslagna konsekvensnivåerna allvarlig, betydande, måttlig eller försumbar (se nedan)
- Återkommande riskanalyser genomföras, med särskilt fokus på behandling av personuppgifter
    - Med fördel används samma konsekvensnivåer som vid informationsklassning
- Tillämpning av resultaten från informationsklassning och riskanalys ska leda till:
    - Att rätt tekniska och organisatoriska skyddsåtgärder påförs. För resultatet av informationsklassning kan KLASSAv2 användas för att få förslag på tekniska och organisatoriska skyddsåtgärder (se bilaga)

Förklaring av konsekvensnivåer

- Försumbar skada
- Måttlig skada - ex minskad förmåga att genomföra verksamhetens uppgifter, men effektiviteten är påvisbart reducerad
- Betydande skada - ex tillgänglighetsstörningar, brott mot regelverk, rättsliga krav och avtal, eller förlust av skapat förtroende
- Allvarlig skada - ex massiv informationsförlust, verksamhetsförlust, oöverskådliga konsekvenser, eller fara för liv och hälsa

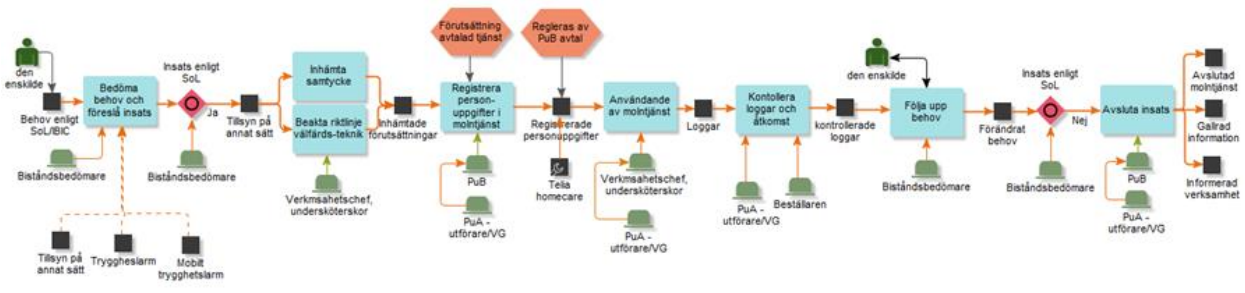
Fokusobjekt

Fokus är i första hand digital tillsyn, men metodiken ska kunna tillämpas på andra digitala välfärdssatsningar

Processbeskrivning

Processen beskriver individens behov av tillsyn. Tjänsten digitaltillsyn utgör i detta fall den beslutade SoL insatsen och tillgodoser den enskildes behov av trygghet.

Processen synliggör också personuppgiftsansvarig respektive personuppgiftsbiträdets roller i samband med att personuppgifter hanteras i samband med att tjänsten tas i bruk hos den enskilde.



Informationsmängder

Om brukare

- För och Efternamn
- Personnummer
- Brukarens adress
- Brukarens mail (i förekommande fall)
- Telefonnummer
- Videoström (under strömning)
- Anteckningar (dessa skall dock inte betecknas som SOL-information)
- Schemat (konfiguration av tillsynstider)
- Namn på kameror
- Status på Tillsyn (utförd eller inte)

Om personal

- Användarnamn på personal
- Organisation
- Suborganisation
- Slutanvändargrupp

Användarrelaterade loggar

- En användare uppdaterar tillsynstider
- Tillsynstid påbörjas
- Tillsynstid avslutas
- Ingen tillsyn genomförd inom föregående Tillsynsintervall
- Användare som tittar på video (genomför tillsyn)
- Användare som markerar att tillsyn är genomförd, detta genom att hon / han klickat på knappen "Tillsyn utförd"
- Kameran förlorar nätverksanslutning
- Kameran återupprättade nätverksanslutning
- En användare misslyckades att starta video
- En användare har försökt titta på video utanför tillsynstider

Tekniska loggar

- User owning the camera
- Camera identifier
- When content was accessed
- Accessed content type (here: video)
- Who accessed the content (here: personnel, only id)
- Start time of accessed content
- Stop time of accessed content

Titel & kund-/projektnamn Linköpings kommun; Socialtjänster i molnet		CERTEZZA
Skapad 2017-03-07	**Senast ändrad** 2017-03-07	**Version** 1.0
Författare Thomas Nilsson, Conny Balazs, Magnus Hûbner	**Dokumentansvarig/Godkänd** Thomas Nilsson	**Säkerhetsklass** Intern

Regulatoriska krav

Skyddade personuppgifter

Personer med skyddad identitet kommer inte inledningsvis att erbjudas välfärdsteknologiska tjänster under pilotverksamheten varför den informationsmängden avgränsas från detta arbete.

Personuppgiftsbehandling

All personuppgiftsbehandling innebär att följande tydliggörs:

- Specifika ändamål för behandlingen
- Typ av uppgifter
- Tillåten behandling
- Tidsfrister för radering/gallring

Ändamålet

Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

1. Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.
2. Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.
3. Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.
4. Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.
5. Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.
6. Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn. Första stycket ska inte gälla för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter, intresseavvägning får inte användas vid myndighetsutövning.

I fallet välfärdsteknologi är det sannolikt samtycke som är vägen fram. Här är det viktigt att separera olika typer av samtycken så att det tydligt framgår vad som kan relateras till Personuppgiftslagen, sedermera Dataskyddsförordningen, och vad som relateras till andra lagrum såsom SOL, HSL mfl.

Dataskyddsförordningen ställer högre krav på samtycket än vad Personuppgiftslagen gör, exempelvis tydligheten i samtycket, vilket bör beaktas redan från start.

Typ av uppgifter

I fallet välfärdsteknologi är det högst sannolikt att personuppgifter som hanteras ät känsliga i enlighet med §13 i Personuppgiftslagen. Det leder till att det ställs höga krav på de tekniska och organisatoriska skyddsåtgärderna för att skydda personuppgifterna.

I tillsynsärenden från Datainspektionen framgår exempelvis att åtkomst över öppna nät ska föregås av stark autentisering. Exempel på öppna nät är Internet och Sjunet men även större interna nät som återfinns i kommuner och landsting är att betrakta som öppna nät. Med stark autentisering menas autentisering med minst två faktorer (ex något man har i kombination med något man vet) samt att processen för tilldelning av identitet och utfärdande av identitetshandling är rigorös. Exempelvis ska inte en person ensam kunna tilldela en identitet och därefter utfärda en identitetshandling. Rollseparering och distribution av aktiveringsdata ska särskilt beaktas.

Idealt levererar inte varje molntjänsteleverantör en autentiseringslösning. Det blir ett ohållbart scenario. Istället kravställs med fördel öppna gränssnitt i tjänsten som SAML (Secure Assertion Markup Langrue) och OIC (Open ID Connect) och kommunens befintliga lösningar för stark autentisering används. På samma sätt kan en privat utfärdare använda sin lösningar och slipper därigenom en lösning per uppdragsgivare.

Tillåten behandling

Behandling är något av följande insamling, registrering, organisering, strukturering, lagring, bearbetning, ändring, framtagning, läsning, användning, utlämning genom överföring, spridning, justering, sammanförande, begränsning, radering eller förstöring

Personuppgiftsansvar och biträden

Utföraren är alltid personuppgiftsansvarig och i Linköpings kommun kan det röra sig om upp till 20-25 privata utförare. Molntjänsteleverantören är alltid personuppgiftsbiträde Även rollen som underbiträde kan diskuteras för molntjänsteleverantören (se nedan).

Det personuppgiftsbiträdesavtal som presenterats för Telia HomeCare är formulerat som att kommunen är personuppgiftsansvarig. Det måste justeras så att varje utförare kan vara personuppgiftsansvarig. Det bör också klargöras huruvida kommunen i det fallet har ett behov av att vara biträde och vad det i så fall skulle vara för ändamål med behandlingen.

I personuppgiftsbiträdesavtal omnämns att parterna ska överenskomma krypteringsmetoder, krypton etc. Kommunen bör upprätta riktlinjer för kryptografiska algoritmer, nyckelhantering samt nyckelegenskaper som varje part ska förhålla sig till. Detta ska biläggas varje separat avtal.

Underbiträde

Personuppgiftsbiträdesavtal upprättas normalt genom att teckna ett separat avtal med varje leverantör som behandlar personuppgifter för den personuppgiftsansvariges räkning. Man kan också ge biträdet mandat att ingå avtal med underbiträden. Om man ger ett sådant mandat

måste det framgå i avtalet att varje underbiträde har samma skyldigheter som huvudleverantören av tjänsten, som är den personuppgiftsansvariges avtalspart.

Ett önskvärt scenario i sammanhanget är att utförare är personuppgiftsanvarig som upprättar ett biträdesavtal med kommunen som i sin tur upprättar underbiträdesavtal med molntjänsteleverantören.

Tidsfrister för radering

För att säkerställa att personuppgifter inte sparas längre än nödvändigt bör den personuppgiftsansvarige införa tidsfrister för radering, gallring samt för regelbunden kontroll.

För välfärdsteknologin har konstaterats ett behov att vid avslutat åtagande gallra uppgifterna när de inte längre behövs. En tids bevarande för t.ex. uppföljning kring incidenter kan vara motiverat.. Detta behöver beaktas i sammanhang likt "rätten att bli glömd" i de fall det inte rör sig om myndighetsutövning.

Uppföljningskravet för den personuppgiftsansvarige måste åtkomstbegränsas per utförare för att säkerställa behandlingen av personuppgifterna.

Annan författningsreglering

I sammanhanget digital tillsyn kan kameraövervakningslagen bli tillämpningsbar. Rättsläget är ännu något oklart avseende digital tillsyn med kamera. Praxis är på väg att växa fram och kommunen rekommenderas följa det arbetet.

Klassificiering

Sammanfattande klassningsresultat av de informationsmängder som hanteras i den tjänst som levereras av Telia HomeCare:

- Förlust av konfidentialitet kan ge betydande skada
- Förlust av riktighet kan ge allvarlig skada
- Förlust av tillgänglighet kan ge måttlig skada (enstaka kameror).

Vid tillgänglighetsförlust till lösningen som helhet bedöms skadan som betydande till allvarlig.

Ovanstående klassningsresultat ligger i linje med resultaten från MFD's workshop våren 2015 med fokus nattillsyn.

Vad gäller logginformation är kravbilden

- Konfidentialitet - Betydande
- Riktighet - Betydande
- Tillgänglighet - Måttlig

Noterbart är att varje informationsägare (personuppgiftsansvarig) torde göra sin egen informationsklassificering och efterföljande riskanalys.

Riskanalys

I Datainspektionens informationsskrift om molntjänster och i de tillsynsbeslut gällande molntjänster som har meddelats, finns krav på att den personuppgiftsansvarige ska genomföra en risk- och sårbarhetsanalys. Något som också stärks i kommande Dataskyddsförordning.

Syftet med riskanalysen är att kartlägga vilka eventuella risker som är förenad med tjänsten och hur riskerna kan hanteras på ett sätt som visar att verksamheten kan använda tjänsten. Den personuppgiftsansvarige ska, med bland annat detta som grund, kunna göra bedömningen att behandlingen av personuppgifter i tjänsten uppfyller de krav som följer av PuL och sedermera Dataskyddsförordningen.

Riskanalysen görs exempelvis med stöd av MSB's modell https://www.informationssakerhet.se/siteassets/metodstod-for-lis/2.-analysera/riskanalys.pdf

Exempel på risker som bör analyseras i tjänster som behandlar personuppgifter:

1. Leverantör får del av personuppgifter
2. Leverantören visar sig inte kunna etablera eller upprätthålla tillräcklig informationssäkerhet
3. Leverantören går i konkurs, köps upp av intressent som inte respekterar ingånget avtal eller att tjänsten avvecklas
4. Leverantören förmår inte upprätthålla tillgängligheten av tjänsten
5. Skadlig kod kan via tjänsten hota kommunens övriga IT-miljö
6. Information och personuppgifter raderas inte när tjänsten avslutats
7. Leverantören behandlar personuppgifterna för egna ändamål
8. Leverantören förändrar innehållet i tjänsten
9. Data och metadata kan inte överföras från en leverantör till en annan vid avslutande av tjänsten

Riskanalys digital tillsyn

Inom ramen för uppdraget har en riskanalys genomförts av digital tillsyn med Telia HomeCare. I riskanalysen deltog följande personer:

- John Fristedt, Linköpings kommun, Omsorgskontoret, IT-utvecklingschef
- Marie Gunhardsson, Linköpings kommun, Omsorgskontoret , tjänsteutvecklare
- Daniel Karlsson, Linköpings kommun, Säkerhetssamordnare
- Jonas Wiman, Linköpings kommun, LKDATA, Modererar av riskanlysen
- Jakob Dumky, Telia Healthcare team, kvalitetsansvarig
- Thomas Nilsson, Certezza AB, Säkerhetskonsult

Identifierade risker och bedömningen av dem bifogas. Det kvarstår därefter att behandla riskerna och fatta beslut om eventuella åtgärder..

Följande identifierade risker med högt riskvärde behöver särskild beaktas.

- Fel uppgifter registreras om ett nytt eller ändrat konto (fel uppgift, saknad uppgift, behörighet). Tillsynen genomförs med fel förutsättningar (riskvärde 45 enligt LKDATA's modell för riskanalys, där riskvärdet kan vara 1-100)
- Utföraren förstår inte sitt ansvar för uppgifter i tjänsten. Tar inte sitt ansvar för att hantera uppgifter och de riskerar att spridas felaktigt (riskvärde 36).
- Personal reagerar negativt på kameror. Tjänsten används inte (riskvärde 30).
- Personal reagerar negativt på kameror. Personalen uppfattar det som ett arbetsmiljöproblem (riskvärde 30).
- Personal inom delar av verksamheten väljer att inte erbjuda tjänsten. Omsorgen blir inte jämlik (riskvärde 30).

Efter förslag på behandling och beslut om eventuella åtgärder bör en ny riskanalys göras för att säkerställa att riskerna med hög riskvärde är hanterade.

Riskanalyser avseende välfärdsteknologi bör göras återkommande, förslagsvis årligen och vid större förändringar .

Vägen fram

Linköpings kommun står i begrepp att göra en pilot med Telia HomeCare. Det är inte helt säkerställt att lösningen uppfyller kraven som följer av klassificeringen (se bilaga) men det är å andra sidan inte lätt att verifiera kraven förrän tjänsten faktiskt tillämpas. Vi rekommenderar därför Linköping kommun att inleda en mindre pilot (20 tal brukare) för att bekanta sig med teknologin och successivt tillse tillräcklig kravuppfyllnad inför ett bredare införande.

Riskanalys ska ske minst årligen eller vid större förändringar. Förslagsvis genomförs dessa med lite tätare intervall under utvärderingsperioden för att säkerställa att identifierade risker hanteras.

Titel & kund-/projektnamn Linköpings kommun; Socialtjänster i molnet		CERTEZZA
Skapad 2017-03-07	**Senast ändrad** 2017-03-07	**Version** 1.0
Författare Thomas Nilsson, Conny Balazs, Magnus Hûbner	**Dokumentansvarig/Godkänd** Thomas Nilsson	**Säkerhetsklass** Intern

Bilaga - Tillämpning KLASSAv2

Klassificering

Sammanfattande klassningsresultat av de informationsmängder som hanteras i den tjänst som levereras av Telia HomeCare:

- Tillgänglighetskrav är av måttlig vikt för enstaka kameror, men av betydande/allvarlig vikt för lösningen som helhet.
- Konfidentialitskravet är av betydande vikt
- Riktighetskravet är av allvarlig vikt

Kravbild - Leverantör

Följande är den kravbild (leverantör) som KLASSAv2 ger givet klassificeringen ovan.

Krav	ISO kapitel	ISO kravområde
Leverantören ska för de delar av verksamheten som berörs i leveransen ha ett ledningssystem för informationssäkerhet (LIS) som baseras på ISO/IEC 27001 eller motsvarande. Ledningssystemet ska omfatta bland annat att samtliga säkerhetskritiska administrativa och tekniska processer är dokumenterade och vilar på en formell grund där roller, ansvar och befogenheter finns tydligt definierade.	A.6.1 Intern organisation	A.6.1.1 Informationssäkerhetsroller och ansvar

Krav	ISO kapitel	ISO kravområde
Leverantören ska ha en policy som beskriver hur de anställda får arbeta på distans avseende drift, förvaltning och support av de levererade tjänsterna. Leverantören ska regelbundet kontrollera att den efterlevs.	A.6.2 Mobila enheter och distansarbete	A.6.2.2 Distansarbete
Leverantören ska ha processer och rutiner på plats för relevant bakgrundskontroll av personal.	A.7.1 Före anställning	A.7.1.1 Bakgrundskontroll
Leverantören ska ha avtal om tystnadsplikt med sina anställda. Tystnadsplikten ska omfatta information om leverantörens kunder. Via avtal ska leverantören även säkerställa tystnadsplikt för underleverantörer.	A.7.1 Före anställning	A.7.1.2 Anställningsvillkor
Leverantören ska ha dokumenterade regler, rutiner och roller som beskriver tillåten användning av de resurser som berörs i leveransen.	A.8.1 Ansvar för tillgångar	A.8.1.3 Tillåten användning av tillgångar
Leverantören ska ha rutiner och funktioner för att permanent radera information som är relaterad till leveransen.	A.8.1 Ansvar för tillgångar	A.8.1.4 Återlämnande av tillgångar

Krav	ISO kapitel	ISO kravområde
Leverantören ska genomföra regelbundna risk- och sårbarhetsanalyser för systemet minst årligen. Identifierade brister ska åtgärdas omgående enligt en dokumenterad plan och ska kunna redovisas för beställaren.	A.8.2 Informationsklassning	A.8.2.1 Klassning av information
Leverantören ska ha fastställda rutiner för hur information relaterad till systemet får hanteras. Efterlevnad ska följas upp	A.8.2 Informationsklassning	A.8.2.3 Hantering av tillgångar
Om ansvar för användarregisterering och behörighetstilldelning ingår i leveransen ska Leverantören ha en dokumenterad process för hur detta sker.	A.9.2 Hantering av användaråtkomst	A.9.2.1 Registrering och avregistrering av användare
Leverantören ska följa en överenskommen rutin som möjliggör för Beställaren att godkänna hantering (skapande, borttag, ändring) av utpekade behörighetsroller t ex avseende högre behörigheter. Hanteringen ska vara spårbar.	A.9.2 Hantering av användaråtkomst	A.9.2.2 Tilldelning av användaråtkomst

Krav	ISO kapitel	ISO kravområde
Leverantören ska använda särskilda personliga användaridentiteter, som godkänns av Beställaren för höga behörigheter som används för systemadministration. Dessa konton ska vara spårbara och lätta att skilja från vanliga användare.	A.9.2 Hantering av användaråtkomst	A.9.2.3 Hantering av privilegierade åtkomsträttigheter
Leverantören ska tillhandahålla ett sätt att distribuera och återställa lösenord utan att lösenordet kan röjas till obehöriga. Behörighetsinformation som t.ex. lösenord får ej lagras i klartext (gäller även systemkonton i källkod). Motsvarande krav gäller även för temporära filer som skapas i användarens arbetsstation när systemet används.	A.9.2 Hantering av användaråtkomst	A.9.2.4 Hantering av användares konfidentiella autentiseringsinformation
Behörighetssystemet ska logga information om när användare skapades, togs bort eller förändrades samt senaste inloggning.	A.9.2 Hantering av användaråtkomst	A.9.2.5 Granskning av användares åtkomsträttigheter
Leverantören ska ha en rutin för att både avaktivera användarkonton och permanent ta bort konton från systemet.	A.9.2 Hantering av användaråtkomst	A.9.2.6 Borttagning eller justering av åtkomsträttigheter

Krav	ISO kapitel	ISO kravområde
Leverantörens behörigheter ska tilldelas enligt principen där minsta möjliga behörighet tilldelas utifrån användares roll och arbetsuppgifter. Detta gäller även konton som används vid kommunikation mellan systemkomponenter, exempelvis mellan applikation och databas samt privilegierade konton.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.1 Begränsning av åtkomst till information
Systemet ska ha stöd för stark autentisering alternativt kunna anslutas till Beställarens behörighetskontrollsystem.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.2 Säkra inloggningsrutiner
Systemet ska ha funktioner för att kunna kravställa lösenordslängd, komplexitet och livslängd.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.3 System för lösenordshantering
Leverantören ska skydda och tillse att det finns spårbarhet i de verktyg som avses för underhåll av systemet, dess säkerhetskonfiguration och information.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.4 Användning av privilegierade verktygsprogram

Krav	ISO kapitel	ISO kravområde
Källkod framtagen i egen utveckling ska skyddas för obehöriga förändringar gentemot den godkända och fastställda versionen. Källkod ska deponeras på ett sådant sätt att beställaren garanteras tillgång om leverantören inte uppfyller sina avtalade förpliktelser.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.5 Åtkomstkontroll till källkod för program
Leverantören ska ha rutiner för kryptering där val av algoritmer, protokoll och nyckellängder samt hantering av krypteringsnycklar framgår.	A.10.1 Kryptografiska säkerhetsåtgärder	A.10.1.1 Regler för användning av kryptografiska säkerhetsåtgärder
Datahallen uppfyller minst skyddsnivå 3 ("datahall" enligt MSB "Vägledning för fysisk informationssäkerhet i it-utrymmen")	A.11.1 Säkra områden	A.11.1.1 Fysiska säkerhetsavgränsningar
Samtliga rutiner som berör leveransen ska följas upp minst årligen och redovisas för Beställaren.	A.12.1 Driftsrutiner och ansvar	A.12.1.2 Ändringshantering
Leverantören ska ha ett skydd mot skadlig kod som uppdateras kontinuerligt för de delar som ingår i leveransen.	A.12.2 Skydd mot skadlig kod	A.12.2.1 Säkerhetsåtgärder mot skadlig kod

Krav	ISO kapitel	ISO kravområde
Leverantören ska ha funktioner för återställande av information enligt överenskomna tillgänglighetskrav med Beställaren. Säkerhetskopior ska skyddas enligt samma skyddsnivåer som, och förvaras åtskilt från, originalinformationen.	A.12.3 Säkerhetskopiering	A.12.3.1 Säkerhetskopiering av information
Leverantören ska skydda loggningsfunktioner och loggningsverktyg mot manipulation och obehörig åtkomst. Detta ska även omfatta leverantörens personal.	A.12.4 Loggning och övervakning	A.12.4.2 Skydd av logginformation
Systemet och relaterad infrastruktur ska använda tidssynkronisering mot samma tidskälla (GPS eller svenska UTC (SP)).	A.12.4 Loggning och övervakning	A.12.4.4 Synkronisering av tid
Leverantören ska verifiera och begränsa den mjukvara som får exekveras inom den levererade tjänsten	A.12.5 Styrning av driftsystem	A.12.5.1 Installation av program på driftsystem
Leverantören ska utan dröjsmål informera beställaren om sårbarheter i levererade komponenter. Upptäckta sårbarheter ska åtgärdas omgående.	A.12.6 Hantering av tekniska sårbarheter	A.12.6.1 Hantering av tekniska sårbarheter

Krav	ISO kapitel	ISO kravområde
All kommunikation till och från systemet ska vara skyddad mot obehörig åtkomst eller förvanskning. Det gäller både kommunikation mellan klient och server och mellan olika systemkomponenter. Skyddet ska uppdateras löpande utifrån kända sårbarheter.	A.13.1 Hantering av nätverkssäkerhet	A.13.1.1 Säkerhetsåtgärder för nätverk
Leverantören ska tillhandahålla en (logisk eller fysiskt) separerad miljö inklusive behörighetskontrollsystem, loggar och lagring för varje kund.	A.13.1 Hantering av nätverkssäkerhet	A.13.1.3 Separation av nätverk
Beställaren ska godkänna alla informationsutbyten som sker med andra system	A.13.2 Informationsöverföring	A.13.2.1 Regler och rutiner för informationsöverföring
Leverantören ska ha fastlagda och dokumenterade principer och metoder för utveckling av säkra system. Vid webbutveckling ska OWASP:s (www.owasp.org) rekommendationer följas.	A.14.1 Säkerhetskrav på informationssystem	A.14.1.1 Analys och specifikation av informationssäkerhetskrav

Krav	ISO kapitel	ISO kravområde
Endast av Beställaren utpekade roller får publicera publik information på allmänt åtkomliga informationssystem.	A.14.1 Säkerhetskrav på informationssystem	A.14.1.2 Säkerställande av programtjänster på publika nätverk
Leverantörens ansvar omfattar även underleverantörer. Underleverantörer ska godkännas av beställaren.	A.15.1 Informationssäkerhet i leverantörsrelationer	A.15.1.1 Informationssäkerhetsregler för leverantörsrelationer
Leverantören ska ha dokumenterade rutiner för övervakning, upptäckt, analys, rapportering, eskalering och hantering av säkerhetshändelser och säkerhetsincidenter.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.1 Ansvar och rutiner
Leverantören ska tillsammans med utpekad roll hos Beställaren samråda kring hantering av sårbarheter, säkerhetshändelser eller säkerhetsincidenter.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.4 Bedömning av och beslut om informationssäkerhetshändelser
Leverantören ska ha rutiner för att hantera utredningar av säkerhetsincidenter enligt gällande lagar och förordningar och samtidigt tillse att känsliga personuppgifter inte röjs till obehöriga.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.5 Hantering av informationssäkerhetsincidenter

Krav	ISO kapitel	ISO kravområde
Leverantören ska ha reservrutiner, reservlösningar och återstartsplaner som uppfyller beställarens krav på tillgänglighet (SLA).	A.17.1 Kontinuitet för informationssäkerhet	A.17.1.2 Införa kontinuitet för informationssäkerhet
Leverantören ska ha reservrutiner, reservlösningar och återstartsplaner som uppfyller beställarens krav på tillgänglighet (SLA)	A.17.1 Kontinuitet för informationssäkerhet	A.17.1.3 Styra, granska och utvärdera kontinuitet för informationssäkerhet
Leverantören ska löpande och i samråd med beställaren arbeta för att leveransen i alla lägen följer de aktuella lagar, förordningar, regler och föreskrifter som ställs på beställarens verksamhet	A.18.1 Efterlevnad av juridiska och avtalsmässiga krav	A.18.1.1 Identifiering av tillämplig lagstiftning och avtalsmässiga krav
Vid behandling av personuppgifter i systemet ska beställaren upprätta biträdesavtal med leverantören avseende personuppgiftsbiträde innan avtalet träder i kraft.	A.18.1 Efterlevnad av juridiska och avtalsmässiga krav	A.18.1.4 Skydd av personlig integritet och personuppgifter
Beställaren ska i samråd med leverantören ha rätt att genomföra säkerhetsrevisioner av ingående delar i leveransen.	A.18.2 Granskningar av informationssäkerhet	A.18.2.3 Granskning av teknisk efterlevnad

Kravbild - Systemförvaltare

Följande är den kravbild (systemförvaltare eller motsvarande) som KLASSAv2 ger givet klassificeringen ovan.

Krav	ISO kapitel	ISO kravområde
Ansvar och ansvarsområden som står i konflikt med varandra är tekniskt eller organisatoriskt åtskilda, exempelvis genom rollseparering, för att minska möjligheterna för obehörig eller oavsiktlig ändring eller missbruk av organisationens tillgångar.	A.6.1 Intern organisation	A.6.1.2 Åtskillnad av ansvar
Det är dokumenterat vilka tillsynsorgan och myndigheter som ska informeras vid säkerhetsincidenter. Efterlevnad följs upp årligen.	A.6.1 Intern organisation	A.6.1.3 Kontakt med myndigheter
Sekretessförbindelse är tecknad med samtliga som har åtkomst till information i systemet. T ex som del av anställningsavtal eller leverantörsavtal.	A.7.1 Före anställning	A.7.1.2 Anställningsvillkor
Utbildning avseende informationssäkerhet för användare och i förekommande fall leverantörer genomförs regelbundet samt vid större förändringar	A.7.2 Under anställning	A.7.2.2 Medvetenhet, utbildning och fortbildning vad gäller informationssäkerhet.
Det finns tydliga och kommunicerade disciplinära åtgärder för överträdelse av informationssäkerhetsregler. Dessa har stöd i lag eller anställningsavtal. Exempel på åtgärder är förlust av behörigheter, muntlig eller skriftlig varning, avstängning eller uppsägning	A.7.2 Under anställning	A.7.2.3 Disciplinär process.

Ansvar och skyldigheter som gäller före och efter tillgång till systemet är definierade och kommunicerade till användare. Användare skriver under ansvarsförbindelse i samband med tillgång till systemet. I samband med avslut av tillgång till systemet repeteras ansvar och skyldigheter för användaren.	A.7.3 Uppsägning eller ändring av anställning	A.7.3.1 Uppsägning eller ändring av anställds ansvar
Systemägare, systemförvaltare och driftansvarig är utsedd.	A.8.1 Ansvar för tillgångar	A.8.1.2 Ägarskap av tillgångar
Dokumentation för användning av systemet finns tillgängligt för användare och revideras årligen.	A.8.1 Ansvar för tillgångar	A.8.1.3 Tillåten användning av tillgångar
Information tillhörande systemet som lagras på externa molntjänster eller på flyttbar lagringsmedia, exempelvis mobiltelefoner, USB-minnen och externa hårddiskar, hanteras och skyddas på motsvarande sätt som övrig information tillhörande systemet.	A.8.3 Hantering av lagringsmedia	A.8.3.1 Hantering av flyttbara lagringsmedia
I samband med avveckling eller återanvändning förstörs, avmagnetiseras eller överskrivs information så att information inte kan återläsas.	A.8.3 Hantering av lagringsmedia	A.8.3.2 Bortskaffande av lagringsmedia
En dokumenterad bedömning av informationens skyddsvärde genomförs innan åtkomst till systemet och tillhörande nätverk tillåts. Bedömningen ligger till grund för regler kring hur åtkomst ska styras. Uppföljning av efterlevnad av reglerna sker regelbundet och dokumenteras.	A.9.1 Verksamhetskrav för styrning av åtkomst	A.9.1.1 Regler för styrning av åtkomst

Användare ska endast ges tillgång till nätverk och nätverkstjänster som systemet kräver och som de specifikt beviljats tillstånd för.	A.9.1 Verksamhetskrav för styrning av åtkomst	A.9.1.2 Tillgång till nätverk och nätverkstjänster
Användare tilldelas personliga och unika användaridentiter efter att identiteten verifierats mot officiellt register. Identiteterna är unika över tid. Användare inaktiveras omgående då åtkomst inte längre behövs.	A.9.2 Hantering av användaråtkomst	A.9.2.1 Registrering och avregistrering av användare
När behörigheter tilldelas, ändras eller fråntas bedöms dessa aktiviteter utifrån användarens tilltänkta roll i systemet och med utgångspunkt i "minsta möjliga behörighet". Dokumentation över beslut och tilldelning arkiveras i 5 år (preskriptionstiden för dataintrång).	A.9.2 Hantering av användaråtkomst	A.9.2.2 Tilldelning av användaråtkomst
För höga behörigheter (privilegierade) i systemet nyttjas separata, personliga och spårbara användaridentiteter som godkänns av systemägare. Behörigheterna är tidbegränsade. Förnyelse sker efter förnyad bedömning.	A.9.2 Hantering av användaråtkomst	A.9.2.3 Hantering av privilegierade åtkomsträttigheter

Följande är uppfyllt gällande tilldelning av inloggningsuppgifter: a) Tilldelade personliga inloggningsuppgifter, så som lösenord och PIN-kod, ändras vid första användningen. b) Elektroniska meddelanden, t.ex. e-post, innehållandes inloggningsuppgifter i klartext (okrypterat) undviks. c) Identiteten på en användare säkerställs innan inloggningsuppgifter tilldelas, oavsett om informationen är ny, förnyad eller tillfällig. d) Tillfälliga inloggningsuppgifter är unika för en användare och går inte att gissa. e) Användare bekräftar mottagandet av inloggningsuppgifter.	A.9.2 Hantering av användaråtkomst	A.9.2.4 Hantering av användares konfidentiella autentiseringsinformation
Stickprov av användares behörigheter granskas minst kvartalsvis avseende att de är korrekta. Hänsyn tas särskilt till användare med privilegierade behörigheter.	A.9.2 Hantering av användaråtkomst	A.9.2.5 Granskning av användares åtkomsträttigheter
Behörigheter inaktiveras omgående vid avslutande av anställning, avslut av avtal eller i överenskommelse med externa parter.	A.9.2 Hantering av användaråtkomst	A.9.2.6 Borttagning eller justering av åtkomsträttigheter
Användare informeras och utbildas regelbundet om sitt eget ansvar att skydda inloggningsuppgifter (lösenord, PIN-kod etc). Det finns underskriven ansvarsförbindelse.	A.9.3 Användaransvar	A.9.3.1 Användning av konfidentiell autentiseringsinformation

Det finns hög tillit till identiteten (motsvarande tillitsnivå 3 - LoA3). Identiteten verifieras med godkänd ID-handling eller en annan LoA3 identitet och ett officiellt register (t ex folkbokföringsregistret). Inloggningen är flerfaktorsbaserad (ex BankID, smart kort, hård eller mjuk dosa för engångskod eller engångslösenord via SMS). Inloggning sker endast via flerfaktor. Aktiveringskod, PIN-kod eller andra personliga inloggningsuppgifter är minst 6 tecken långa.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.2 Säkra inloggningsrutiner
Det finns åtkomstbegränsningar och spårbarhet i användning av verktyg för underhåll av systemet. Uppföljning av efterlevnad sker årligen och dokumenteras.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.4 Användning av privilegierade verktygsprogram
Källkod skyddas från åtkomst och obehöriga förändringar gentemot fastställd version. Förändringar i källkod kan härledas genom versionshantering och spårning.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.5 Åtkomstkontroll till källkod för program
Regelverk för kryptering och kryptonycklar uppfylls av systemet. Efterlevnad följs upp minst årligen.	A.10.1 Kryptografiska säkerhetsåtgärder. Mål: Att säkerställa korrekt och effektiv användning av kryptering för att skydda informationens konfidentialitet, äkthet och/eller riktighet.	A.10.1.1 Policy för användning av kryptografiska säkerhetsåtgärder
Fysisk åtkomst till systemet är begränsad endast till endast behörig personal	A.11.1 Säkra områden	A.11.1.2 Fysiska tillträdesbegränsningar.

Kablage och annan utrustning avsedd för strömförsörjning och nätverksöverföring är skyddade mot otillbörlig åtkomst samt avsiktlig och oavsiktlig skada. Skyddet följer MSB:s vägledning "MSB629 Vägledning för fysisk informationssäkerhet i it-utrymmen"	A.11.2 Utrustning	A.11.2.3 Kablagesäkerhet.
Det finns driftsrutiner	A.12.1 Driftsrutiner och ansvar	A.12.1.1 Dokumenterade driftsrutiner
Processen för ändringhantering är dokumenterad och tillämpas vid behov.	A.12.1 Driftsrutiner och ansvar	A.12.1.2 Ändringshantering
Informationen i systemet skyddas mot skadlig kod genom säkerhetsuppdateringar. Skyddet mot skadlig kod uppdateras kontinuerligt.	A.12.2 Skydd mot skadlig kod	A.12.2.1 Säkerhetsåtgärder mot skadlig kod
Säkerhetskopiering sker regelbundet med övervakning och loggning. Frekvensen av säkerhetskopior baseras på överenskommelse med verksamheten. Återläsning av säkerhetskopior testas minst årligen och förvaras minst 500 meter från systemet eller om så inte är möjligt i annan brandcell.	A.12.3 Säkerhetskopiering	A.12.3.1 Säkerhetskopiering av information
Systemet loggar information som berör fel, användaraktiviteter och säkerhetshändelser. Logginformationen sparas och granskas vid behov.	A.12.4 Loggning och övervakning	A.12.4.1 Loggning av händelser
Logginformation och verktyg för loggning skyddas mot obehörig åtkomst och förändring.	A.12.4 Loggning och övervakning	A.12.4.2 Skydd av logginformation

Logginformation som härrör från konton med högre behörigheter (privilegierade) granskas vid behov.	A.12.4 Loggning och övervakning	A.12.4.3 Administratörs- och operatörsloggar
Systemet och kringliggande infrastruktur använder den svenska nationella tidsskalan UTC(SP) som källa för tid.	A.12.4 Loggning och övervakning	A.12.4.4 Synkronisering av tid
Systemförvaltare ansvarar för att hålla sig uppdaterad kring tekniska sårbarheter. Återkommande riskanalyser genomförs och åtgärder vidtas för att minska risken att sårbarheter kan utnyttjas.	A.12.6 Hantering av tekniska sårbarheter	A.12.6.1 Hantering av tekniska sårbarheter
I nätverket har åtgärder genomförts i syfte att skydda: - systemet från obehörig åtkomst - systemets informationen som transporteras i nätverket - systemets konfiguration och administration.	A.13.1 Hantering av nätverkssäkerhet. Mål: Att säkerställa skyddet för information i nätverk och dess stödjande informationsbehandlingsresurser.	A.13.1.1 Säkerhetsåtgärder för nätverk
Nätverkssegmentet där systemet är placerat motsvarar skyddsnivån för allvarlig påverkan. Det finns en förteckning av systemets samtliga beroenden och kopplingar till andra nätverk.	A.13.1 Hantering av nätverkssäkerhet. Mål: Att säkerställa skyddet för information i nätverk och dess stödjande informationsbehandlingsresurser.	A.13.1.3 Separation i nätverk

Systemägaren eller informationsägaren har godkänt informationsutbyten som sker med andra system och externa parter. Informationsutbytet är dokumenterat, avtalat och spårbart.	A.13.2 Informationsöverföring. Mål: Att upprätthålla säkerheten hos information som överförs inom en organisation, eller till en extern enhet.	A.13.2.1 Policyer och rutiner för informationsöverföring
Säker överföring av information mellan systemet och externa parter är reglerad genom överenskommelser.	A.13.2 Informationsöverföring. Mål: Att upprätthålla säkerheten hos information som överförs inom en organisation, eller till en extern enhet.	A.13.2.2 Överenskommelser om informationsöverföring
Vid informationsöverföring skyddas informationen mot manipulation och avlyssning. Skyddet gäller oberoende av på vilket sätt informationen kommuniceras och omfattar hela kedjan oavbrutet från avsändaren till mottagaren.	A.13.2 Informationsöverföring. Mål: Att upprätthålla säkerheten hos information som överförs inom en organisation, eller till en extern enhet.	A.13.2.3 Elektronisk meddelandehantering
Avtal med extern part reglerar åtkomst, vidareutnyttjande, ägande och tillåten behandling av systemets information. I det fall personuppgifter behandlas är ett personuppgiftsbiträdesavtal upprättat. Leverantörens skyldighet att anmäla och rapportera obehörigt röjande eller läckage av sekretessbelagd information är reglerad i avtal. Villkor för hur information returneras eller förstörs vid avtalets upphörande är reglerad. Efterlevnad följs upp minst årligen.	A.13.2 Informationsöverföring. Mål: Att upprätthålla säkerheten hos information som överförs inom en organisation, eller till en extern enhet.	A.13.2.4 Sekretessförbindelser

Informationssäkerhetskrav beaktas vid upphandling, utveckling, drift, stora förändringar och avveckling via avtal och överenskommelser. Uppföljning av att kraven efterlevs sker minst årligen.	A.14.1 Säkerhetskrav på informationssystem	A.14.1.1 Analys och specifikation av informationssäkerhetskrav
Publicering av information, från systemet till platser som är allmänt åtkomliga, är begränsad till utpekade roller.	A.14.1 Säkerhetskrav på informationssystem	A.14.1.2 Säkerställande av programtjänster på publika nätverk
Riskanalys genomförs i samband med förändring och utveckling. Risker dokumenteras, följs upp och hanteras.	A.14.2 Säkerhet i utvecklings- och supportprocesser	A.14.2.2 Rutiner för hantering av systemändringar
En reservplan (roll-back) för återställning av systemets funktionalitet ska finnas vid varje större uppgradering.	A.14.2 Säkerhet i utvecklings- och supportprocesser	A.14.2.3 Teknisk granskning av tillämpningar efter ändringar i driftsmiljö
Vid utveckling och större förändringar finns det krav på säkerhetstester. Avvikelser och resultat dokumenteras och sparas.	A.14.2 Säkerhet i utvecklings- och supportprocesser	A.14.2.5 Principer för utveckling av säkra system
Vid extern systemutveckling efterlevs metoder för utveckling av säkra system. Vid webbutveckling ska OWASP:s (www.owasp.org) rekommendationer följas.	A.14.2 Säkerhet i utvecklings- och supportprocesser	A.14.2.7 Outsourcad utveckling
Acceptanstester omfattar även säkerhetstester.	A.14.2 Säkerhet i utvecklings- och supportprocesser	A.14.2.9 Acceptanstestning av system
Utvecklings- och testsystem skyddas antingen på likvärdigt sätt som produktionssystemet, alternativt innehåller inte konfidentiell eller känslig information.	A.14.3 Testdata	A.14.3.1 Skydd av testdata

Säkerhetskrav för leverantörens åtkomst till systemet är överenskomna och avtalade. Efterlevnad följs upp minst årligen.	A.15.1 Informationssäkerhet i leverantörsrelationer	A.15.1.1 Informationssäkerhetsregler för leverantörsrelationer
Det finns avtal med krav på att driftsleverantör skyndsamt ska hantera informationssäkerhetsrisker. Efterlevnad följs upp minst årligen.	A.15.1 Informationssäkerhet i leverantörsrelationer	A.15.1.3 Försörjningskedja för informations- och kommunikationsteknologi
Leverantörens tjänsteleverans med avseende på informationssäkerhetskrav följs upp minst årligen.	A.15.2 Hantering av leverantörers tjänsteleverans	A.15.2.1 Övervakning och granskning av leverantörers tjänster
En rutin eller process för genomförande av förändringar i systemet finns framtagen och som säkerställer att systemförvaltare godkänner förändringen innan den genomförs. Eventuella undantag är överenskomna. Efterlevnad av rutiner följs upp efter genomförd förändring.	A.15.2 Hantering av leverantörers tjänsteleverans	A.15.2.2 Ändringshantering av leverantörers tjänster
Ansvar, rutiner, kontaktvägar och kommunikationsplan vid säkerhetsincidenter finns dokumenterade och är inövade.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.1 Ansvar och rutiner
Användare, driftspersonal och leverantörer informeras om sitt ansvar att rapportera avvikelser, risker och incidenter som kan påverka systemet, samt känner till på vilket sätt detta ska ske. Ovanstående är inövat och dokumenterat.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.3 Rapportering av svagheter gällande informationssäkerhet
Säkerhetsincidenter dokumenteras och utvärderas inom en månad för att minska sannolikheten för liknande framtida händelser.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.6 Att lära av informationssäkerhetsincidenter

Vid en incident har organisationen fastställt hur identifiering, insamling, kopiering och bevarande av information kan användas som bevis.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.7 Insamling av bevis
Lagar och avtal som påverkar systemet identifieras, dokumenteras och kommuniceras. Det finns dokumentation som beskriver hur kraven efterlevs. (Till exempel: information som överförs till arkivering följer Riksarkivets föreskrifter av bevaring av information.)	A.18.1 Efterlevnad av juridiska och avtalsmässiga krav	A.18.1.1 Identifiering av tillämplig lagstiftning och avtalsmässiga krav
Dokumenterad information som processer, rutiner, systemdokumentation, resultat från granskningar, tester, riskanalyser mm skyddas från obehöriga. Dessa dokument har en ägare som förvaltar, versionshanterar och uppdaterar dokumenten.	A.18.1 Efterlevnad av juridiska och avtalsmässiga krav	A.18.1.3 Skydd av dokumenterad information

Om systemet innehåller personuppgifter genomförs: - Laglighetsbedömning av behandling (ex. avtal, samtycke, allmänt intresse) - Separat register uppförs där kategorier av behandling, syfte, ändamål, omfattning, vidareutlämning och skydd av personuppgifter dokumenteras. - Om personuppgifterna är känsliga göra en konsekvensbedömning ur ett integritetsperspektiv. - Biträdesavtal tecknas med alla berörda parter. - Personuppgifts- och/eller dataskyddsombud notifieras om behandlingen. Skyddet av personuppgifter är i enlighet med dataskyddsförordningen prioriterat vid utveckling och förändring av systemet, så kallat inbyggt dataskydd och dataskydd som standard.	A.18.1 Efterlevnad av juridiska och avtalsmässiga krav	A.18.1.4 Skydd av personuppgifter
Oberoende part granskar informationssäkerheten minst vartannat år.	A.18.2 Granskningar av informationssäkerhet	A.18.2.1 Oberoende granskning av informationssäkerhet
Granskning och kontroll av efterlevnad av informationssäkerhetskrav ska rapporteras till systemägaren minst årligen. Resultatet finns dokumenterat.	A.18.2 Granskningar av informationssäkerhet	A.18.2.2 Efterlevnad av säkerhetspolicy, regler och standarder

Genomgång av säkerhetsinställningar som påverkar systemet (t. ex. brandväggsregler och systemkonfiguration) genomförs minst årligen, sammanställs och rapporteras till berörda parter.	A.18.2 Granskningar av informationssäkerhet	A.18.2.3 Teknisk granskning av efterlevnad

Titel & kund-/projektnamn Linköpings kommun; Socialtjänster i molnet		
Skapad 2017-03-07	**Senast ändrad** 2017-03-07	**Version** 1.0
Författare Thomas Nilsson, Conny Balazs, Magnus Hûbner	**Dokumentansvarig/Godkänd** Thomas Nilsson	**Säkerhetsklass** Intern

Bilaga - Riskanalys Telia HomeCare

Riskanalysen är genomförd enligt LKDATA's metodik under ledning av Jonas Wikman, Linköpings kommun. Nedan är ett extrakt från rapporten.

Definiera objekt för analys

Hårdvara

- N/A ingår Telia's tjänst

Programvara

- N/A ingår Telia's tjänst

Tjänster (externa eller interna från andra verksamhetsområden)

- Telia HomeCare tjänst
- Personal från en eller flera utförare
- Larmcentral (en eller flera från olika företag)

Integrationer

- N/A

Processer

- Process för tillsyn via kamera

Information (data som lagras eller behandlas)

- Personuppgifter men inte om skyddade personer
- Känslig personuppgift (PUL)
- Videoström (behandlas, lagras ej)

Roller

- Omsorgskontoret (beställare)
- Utförare Personuppgiftsansvariga. (kommunen och privata)
- Telia
- Brukare
- Anhöriga
- Larmteam (kommunens personal som gör installationer)

Intressenter

- Tillsyns organ
- Politisk ledning
- Kommunledning
- Media

Beroenden (ingår inte riskanalysen, men bör vara kända)

- Datakommunikation
- Acceptans från brukare

Avgränsning

- Omfattar enbart personer som inte har skyddade personuppgifter
- Omfattar enbart personer som har valt tjänsten och samtyckt till hanteringen av information
- Generella frågor runt hemtjänst ingår inte i analysen. Enbart sådant som är unikt för tillsyn via kamera

Slutsats - Rekommendation

Analysobjektet har fått många risker med mycket höga bedömningar för konsekvens, och få med hög sannolikhet. Det är kopplat till höga krav enligt informationsklassning, samt att den tänkta funktionen redan är designad för att minimera negativa händelser.

Vissa risker bedöms kunna leda till vårdskador.

Bland de risker som placerar sig högst är flertalet kopplade till handhavandefel hos personal, främst inom förvaltning och utförare. Det leder till att stor omsorg bör läggas på utformning av rutiner och uppföljning av användningen.

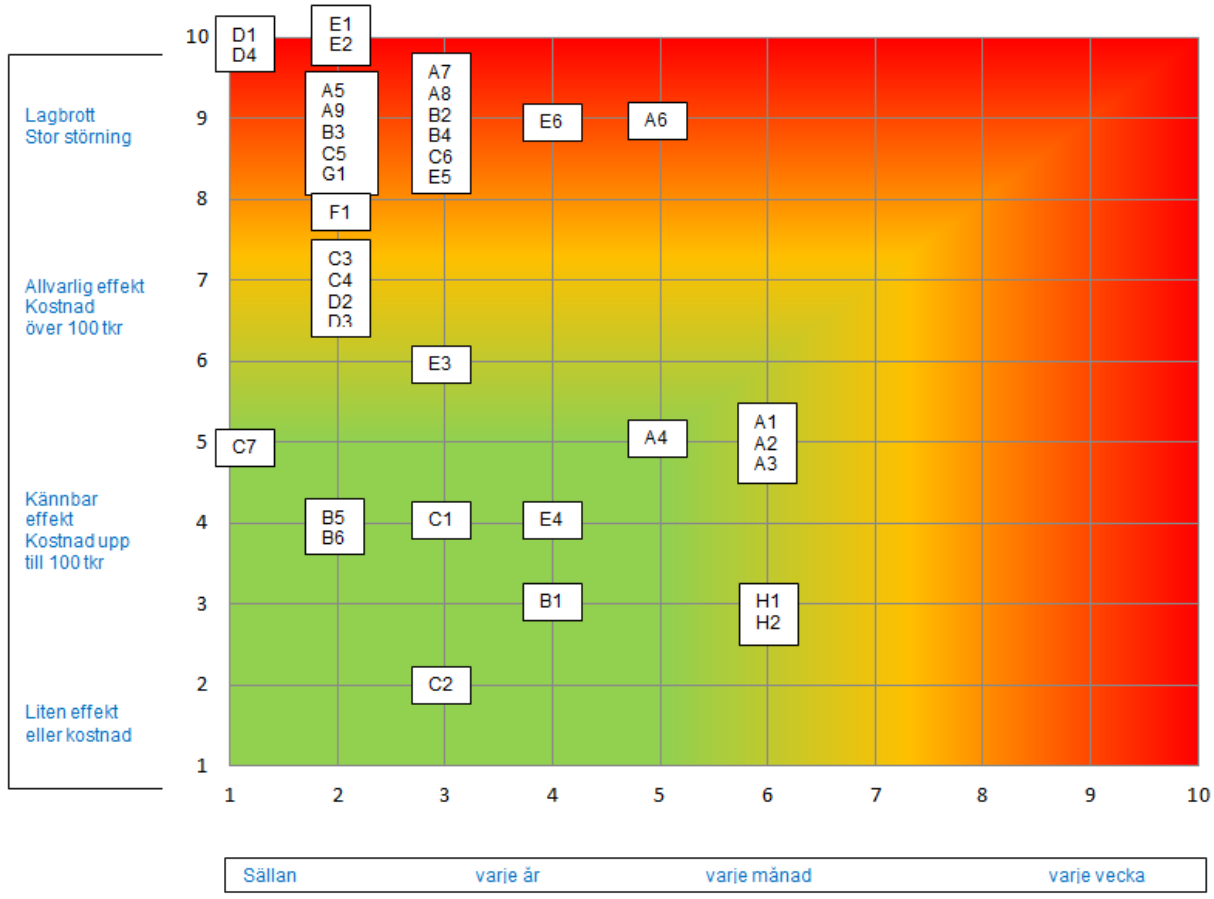
Risker kopplade till leverantör handlar i första hand om tillgänglighetsstörningar trots lägre informationsklassning inom det området.
Leverantören kommer att agera Personuppgiftsbiträde för information som faller under både PUL och särskild sekretesslagstiftning. Tjänsten som erbjuds bedöms vara konstruerad utifrån sådana krav. PUB avtal och uppföljning av efterlevnad enligt PUB-avtal är ändå viktiga.

Analysen är ett underlag för mottagarens beslut om åtgärder. Det är en rekommendation att dokumentera vilka beslut som tas för samtliga risker, även de som lämnas utan åtgärd. Vidare rekommenderas att minst alla risker med röd markering bemötas med någon form av åtgärd.

Riskanalysen bör upprepas inom två år då mer är känt om hur funktionen används och fungerar. Alternativt om nya typer av sensorer, utöver kameror, ska börja användas.

Titel & kund-/projektnamn Linköpings kommun; Socialtjänster i molnet		CERTEZZA
Skapad 2017-03-07	**Senast ändrad** 2017-03-07	**Version** 1.0
Författare Thomas Nilsson, Conny Balazs, Magnus Hûbner	**Dokumentansvarig/Godkänd** Thomas Nilsson	**Säkerhetsklass** Intern

Riskmatris



Risker bedöms efter sannolikhet och konsekvens. Värden sätts efter en tiogradig standardiserad skala. Riskvärdet fås genom att multiplicera bedömningarna.

Riskerna delas in i ämnesområden som indikeras i RiskID enligt:

- A - Personal
- B - Teknik
- C - Produkt
- D - Sabotage
- E - Drift
- F - Projekt
- G - Leverantör
- H - Brukare

Risk ID	Riskbeskrivning	Sannolikhet	Konsekvens	Riskvärde	Föreslagen åtgärd
A6	Fel uppgifter registreras om ett nytt eller ändrat konto (fel uppgift, saknad uppgift, behörighet). Tillsynen genomförs med fel förutsättningar	5	9	45	Rutiner för verifiering av uppgifter, innan de läggs in eller efteråt tydligt underlag och gränssnitt, inte fler uppgifter än nödvändigt framtida utveckling med integration för automatisk registrering
E6	Utföraren förstår inte sitt ansvar för uppgifter i tjänsten. Tar inte sitt ansvar för att hantera uppgifter och de riskerar att spridas felaktigt.	4	9	36	avtal och uppföljning av efterlevnad
A1	Personal reagerar negativt på kameror. Tjänsten används inte	6	5	30	Utbildning och information. Teknikombud som agerar lokala ambassadörer.
A2	Personal reagerar negativt på kameror. Personalen uppfattar det som ett arbetsmiljöproblem	6	5	30	Utbildning och information. Teknikombud som agerar lokala ambassadörer.

A3	Personal inom delar av verksamheten väljer att inte erbjuda tjänsten. Omsorg blir inte jämlik	6	5	30	Utbildning och information. Teknikombud som agerar lokala ambassadörer.
A7	Information om brukare finns på flera ställen. Vid gallring tas den inte bort överallt.	3	9	27	Dataskyddsförordning en införs med höga skadestånd som följd noggrant beskrivna rutiner för gallring
A8	Fortsatt tillsyn sker trots att brukaren flyttat från boendet. Den nya brukaren har inte lämnat samtycke eller har biståndsbeslut	3	9	27	Rutiner och checklistor.
B2	Avbrott i tjänst från Telia. 1-4 timmar. Tillsyn kan inte genomföras. Hela den del av tjänsten där Telia också är nätleverantör	3	9	27	Redundans i gemensamma delar och central utrustning. Etablera dubbla kabelvägar Säkerställa att verksamheterna har upprättat kontinuitetsplaner
B4	Avbrott i datakommunikation i del av nätet. 1-4 timmar. Slår ut en andel av alla kameror	3	9	27	Redundant datakom Avtal med nätoperatörer tester och lägsta krav vid upphandling

C6	Brist i kommunikation för planerat servicefönster. Systemet stannar och personal är inte förberedd	3	9	27	
E5	Gallring misslyckas och finns kvar hos tjänsteleverantör längre tid än avsett. Personuppgifter finns där vi inte har koll på dem	3	9	27	Rutiner och riktlinjer för hantering av konton.
A4	Biståndsbedömare väljer att inte besluta om tjänsten. Omsorg blir inte jämlik	5	5	25	Utbildning och information. Teknikombud som agerar lokala ambassadörer.
E1	Kamera registreras på fel person. Personalen ser inte att en person saknas (tittar på någon annan) och åker inte ut	2	10	20	Identifierare som läggs in i själva kameran och visas i bild Dokumenterad test efter nyinstallation
E2	Kamera registreras på fel person. Personalen ser en händelse och åker till fel person. Den drabbade personen får inte hjälp	2	10	20	Identifierare som läggs in i själva kameran och visas i bild Dokumenterad test efter nyinstallation

A5	Felkonfiguration i behörighetssystem gör att fel personer får tillgång till information och videoström	2	9	18	Rutiner och stöddokumentation för hur konfigurering ska ske, Samt utbildning. Enklare handhavande i produkten cyberförsäkring mot ansvarskostnader
A9	Användare kopierar ut information från systemet och hanterar det bredvid (i syfte att effektivisera sitt jobb). Informationen kan spridas utom kontroll och/eller missa att gallras	2	9	18	
B3	Avbrott i tjänst från Telia. 1-4 timmar. Tillsyn kan inte genomföras. Hela tjänsten, ej kopplat till nätstörning	2	9	18	Säkerställa att verksamheterna har upprättat kontinuitetsplaner
C5	Störning nattetid (oavsett vilken typ) kan inte upptäckas, hanteras och avhjälpas tillräckligt snabbt.	2	9	18	
G1	Känsliga personuppgifter röjs till obehöriga hos tjänsteleverantör	2	9	18	Regleras i PUB-avtal och följs upp vid revision av oss eller tredje part

H1	Brukaren har inte uppfattat att den har gett samtycket och kommer i konflikt med oss om tjänsten.	6	3	18	Rutiner och riktlinjer
H2	Hantering av samtycke fallerar och när man vårdgivaren behöver bevisa att samtyckte finns, så kan vi inte visa det.	6	3	18	Utbildning och information. Teknikombud som agerar lokala ambassadörer.
E4	Brukare byter utförare. När data sparas i tre månader hos den gamla utföraren. Så får den nya utföraren tillgång till info som den inte ska ha. Uppgifter om SoL dok röjs	4	4	16	Rutin där Telia tömmer info som vårdgivare ser. Skickar uppgifter som ska sparas till Omsorgskontoret för att kunna göra uppföljning
F1	Få brukare väljer att använda tjänsten. Eftersökta effekter av erfarenheter av arbetssätt och välfärdsteknik uteblir	2	8	16	Utbildning och information. Teknikombud som agerar lokala ambassadörer.

E3	Information om ändrade förhållanden saknas. Ger felaktiga utryckningar och minskad trovärdighet	3	5	15	Lokala rutiner.
C3	Loggen är ändrad (medvetet eller av tekniskt fel) och kan inte användas för att spåra felaktig användning	2	7	14	Utbildning och information. Teknikombud som agerar lokala ambassadörer.
C4	Loggen är ändrad (medvetet eller av tekniskt fel) och kan inte användas för att spåra felaktig användning. Vi kan inte heller detektera att loggen är ändrad	2	7	14	Utbildning och information. Teknikombud som agerar lokala ambassadörer.
D2	Personal med behörighet att använda kamera, missbrukar den för att spionera på brukaren.	2	7	14	Loggning och loggkontroll
D3	Personal som inte ska ha behörighet att använda kamera. Använder någon annans behörighet för att spionera på brukaren.	2	7	14	Noggrann behörighetstilldelning och autentisering

B1	Avbrott i tjänst från Telia. 1-4 timmar. Tillsyn kan inte genomföras. Enskild kamera	4	3	12	Krav i avtal Kontinuitetsplanering i verksamheten
C1	Uppdatering av tjänsten leder till störning.	3	4	12	Rutiner för test och rollback vid uppdatering
D1	Angripare hackar kamera och får tillgång till bilder	1	10	10	
D4	Personal tar en skärmdump eller foto av bild från kamera och sprider den	1	10	10	
B5	Fel i enskild utrustning hos en brukare. Den brukaren kan inte få tillsyn via kamera	2	4	8	Lokala rutiner.
B6	Tekniska problem i tjänsten med fördröjning. Insats försenas	2	4	8	Lokala rutiner.
C2	Ändringar i förhållanden på plats gör att kamera inte fungerar hos enskild brukare.	3	2	6	Utbildning och information. Teknikombud som agerar lokala ambassadörer.
C7	Planerade långa servicefönster ger att extrapersonal måste kallas in och det ökar kostnaden väsentligt	1	5	5	

Titel & kund-/projektnamn Linköpings kommun; Socialtjänster i molnet		
Skapad 2017-03-07	**Senast ändrad** 2017-03-07	**Version** 1.0
Författare Thomas Nilsson, Conny Balazs, Magnus Hûbner	**Dokumentansvarig/Godkänd** Thomas Nilsson	**Säkerhetsklass** Intern