

För kännedom  
Enligt sändlista

Regionstyrelsen

### **Granskning av hantering av eTjänstekort**

Region Sörmlands revisionskontor har på uppdrag av regionens revisorer genomfört en granskning av hanteringen av eTjänstekort (inklusive nyckelkort/taggs). Granskningens syfte är att bedöma om regionstyrelsen säkerställer att hanteringen av eTjänstekort, sker med en tillräcklig intern styrning och kontroll.

Region Sörmland tillhandahåller olika lösningar för behörigheter IT-system och/eller lokaler till medarbetare och personer med uppdrag i regionen. Regionens eTjänstekort har Inera AB som leverantör där identifieringstjänsten ställer höga krav på hanteringen och på identitetshandlingar.

Den sammanfattande bedömningen är att regionstyrelsen inte helt säkerställt att hanteringen av eTjänstekort sker med en tillräcklig intern styrning och kontroll.

Bedömningen är att intern styrning och kontroll kan utvecklas. Bilden som förmedlats i granskningen är att uppföljning av tilldelade behörigheter för åtkomst till system om lokaler, sker sporadiskt, inte samlat och systematiskt i enlighet med styrande dokument. Bedömningen är att det finns behov av att säkerställa att ansvarig chef ges förutsättningar att systematiskt genomföra uppföljningar. Det saknas styrande dokument för inpassering i lokaler. Granskningen visar att det inte är tydliggjort vad som gäller vid medarbetares långtidsfrånvaro och för förtroendevalda.

Flera förändringar planeras på området från 2025, vilket är positivt.

Revisorerna ställer sig bakom de rekommendationer som framförs i rapporten.

Revisionen

Datum  
2024-12-12

Dokumentnummer  
RE-REV24-0040-1

I granskningen har vi också följt upp rekommendationer på området som lämnades till nämnden för kultur, utbildning och friluftsvksamhet år 2019. Uppföljningen visar att det som kvarstår är att den årliga utvärderingen av säkerhetsplanen sker muntligt, vilket gör att den inte är spårbar. Granskningsrapporten lämnas för kännedom till nämnden för kultur, utbildning och friluftsvksamhet.

Vi begär svar från regionstyrelsen med uppgifter om verkställda och planerade åtgärder senast 10 april 2025.

Catharina Fredriksson  
ordförande

Gustaf Wachtmeister  
vice ordförande

Sändlista

Nämnden för kultur, utbildning och friluftsvksamhet  
Magnus Johansson, regiondirektör  
Helena Söderquist, verksamhetsområdeschef regionservice  
Urban Petré, IT-direktör  
Hanna Rasmussen, verksamhetsområdeschef Kultur & Utbildning  
Sörmland  
Sofia Stenlund Wretling, utvecklingsdirektör, staben för demokrati och insyn

# UNDERSKRIFTSSIDA

---

**Detta dokument har undertecknats med avancerade elektroniska  
underskrifter:**



REGION  
SÖRMLAND

*Revisionen*

# Hantering av eTjänstekort

---

Granskningsrapport

**Åsa Forsman**

**2024-12-12**

Revisionen

## Innehåll

Sammanfattning .....	2
Bakgrund .....	4
Syfte och revisionsfrågor .....	5
Omfattning och avgränsning .....	5
Metod .....	5
Revisionskriterier .....	6
Granskningens resultat .....	6
Organisation, roller och ansvar .....	9
Styrande dokument, riktlinjer och rutiner .....	10
Utbildning och information .....	14
Uppföljning .....	15
Inpassering i lokaler/passagebehörighet .....	18
Sörmlands museum .....	24
Sörmlands museum- uppföljning av granskning av säkerhetsarbetet på Sörmlands museum .....	25
Framtida arbete .....	26

## Sammanfattning

Region Sörmlands revisionskontor har på uppdrag av regionens revisorer genomfört en granskning för att bedöma om regionstyrelsen säkerställer att hanteringen av eTjänstekort (SITHS-kort/reservkort) inklusive nyckelkort/taggs sker med en tillräcklig intern styrning och kontroll.

Regionen tillhandahåller olika lösningar för behörighet till IT-system och/eller lokaler, för medarbetare och personer med uppdrag i regionen.

Den sammanfattande bedömningen är att regionstyrelsen inte helt säkerställt att hanteringen av eTjänstekort inklusive nyckelkort/taggs sker med tillräcklig intern styrning och kontroll.

Regionen är ansluten till Inera AB:s identifieringstjänst SITHS och använder SITHS e-id portalen för att utfärda eTjänstekort. Fastighetsservice hanterar behörigheter för inpassering i lokaler.

Granskningen visar att det finns förbättringsområden bland annat på området för uppföljning av behörigheter. I styrande dokument anges att ansvarig chef ska säkerställa att medarbetare endast har behörighet att komma åt uppgifter eller lokaler som behandlar information eller kan påverka informationshanteringen, som är absolut nödvändig. I granskningen har det framkommit att uppföljning av behörigheter sker sporadiskt, inte samlat och systematiskt.

Det är inte tydligt vilken skriftlig rutin som ska gälla (av de två som finns) för utgivning och hantering av eTjänstekort/reservkort och förtroendevaldas behörigheter för inpassering i lokaler. Hantering för medarbetares långtidsfrånvaro beskrivs inte i någon rutin. Området kommer enligt uppgift att ingå i utvecklingsarbeten som planeras att genomföras från 2025, vilket är positivt.

Det saknas styrande dokument som avser regelverk/hantering för behörigheter för inpassering i lokaler. För inpassering används också så kallade nyckelkort, som är lånekort och som används av personer med tillfälliga uppdrag. De är ofta personliga men det finns också opersonliga nyckelkort. Granskningen har visat att hanteringen av de opersonliga nyckelkorterna är riskfylld då det saknas koppling till eKS, manuell hantering krävs och kvittens saknas.

Det är positivt att kontroller gör av kontaktcenter, RSIT och fastighetsservice innan behörigheter läggs in och att regionservice södra inte längre ger ut opersonliga nyckelkort till medarbetare.

*Revisionen*

Efter genomförd granskning lämnar vi nedanstående rekommendationer till regionstyrelsen, att ta med i det fortsatta utvecklingsarbetet. Detta för att ytterligare säkerställa att hanteringen av eTjänstekort sker med en tillräcklig intern styrning och kontroll.

**För eTjänstekort/reservkort:**

- ✓ Säkerställ att beslutat handlingsprogram 2024–2025 genomförs
- ✓ Säkerställ att ansvarig chef ges förutsättningar att systematiskt genomföra uppföljningar av behörigheter och kontrollera åtkomst till information
- ✓ Tydliggör vilken rutin som gäller för hantering av eTjänstekort och gör den känd
- ✓ Förtydliga hantering för förtroendevalda och för utfärdande av reservkort då eTjänstekort glömts hemma
- ✓ Säkerställ att planerad rutin för långtidsfrånvaro tas fram och görs känd
- ✓ Säkerställ att verksamhetsspecifika anvisningar/rutiner tas fram
- ✓ Säkerställ att informationen om hur eTjänstekort spärras är aktuell
- ✓ Säkerställ att obligatoriska utbildningar genomförs innan eTjänstekort tilldelas
- ✓ Överväg att ha med kontrollen av medarbetare/användare som inte loggat in på länge, i internkontrollplanen.

**För inpassering i lokaler:**

- ✓ Upprätta och besluta om styrande dokument för området inpassering i lokaler
- ✓ Säkerställ att ansvarig chef ges förutsättningar att systematiskt genomföra uppföljningar av behörigheter för inpassering
- ✓ Ta fram och inför enhetlig administration av passersystemet i samtliga fastighetsdriftsområden
- ✓ Säkerställ att rutiner som upprättas är skriftligt dokumenterade
- ✓ Säkerställ att medarbetare som mottar nyckelkort undertecknar och returnerar kvittensen
- ✓ Överväg att ha med området med kontroll av behörigheter i internkontrollplanen.

I granskningen har vi också följt upp rekommendationer på området som lämnades till nämnden för kultur, utbildning och friluftsverksamhet år 2019. Uppföljningen visar att det som kvarstår är att den årliga utvärderingen av

*Revisionen*

säkerhetsplanen sker muntligt, vilket gör att den inte är spårbar. Granskningsrapporten lämnas för kännedom till nämnden för kultur, utbildning och friluftsverksamhet.

## Bakgrund

eTjänstekort används för inloggning i system som innehåller känsliga uppgifter. De används också för fysisk inpassering i lokaler. Regionens eTjänstekortsmodell bygger på en nationell modell (SITHS) som levereras av Inera AB.

Det är viktigt att lagar, föreskrifter, riktlinjer, policys med mera efterlevs i syfte att minimera risker och avvikelser, ur såväl patientsäkerhet som informationssäkerhet och övriga säkerhetsaspekter. Brister kan leda till förtroendeskada och ekonomisk skada. Ett annat viktigt område är administrationen av eTjänstekort (inklusive behörigheter) och att det är ”ordning och reda”. Till stor del utgår säkerheten från användaren av eTjänstekort. Det gör att det är viktigt att säkerhetsnivån är hög och att användare har utbildning och kännedom om ansvar, rutiner och riktlinjer.

Några risker som identifierats är hanteringen när certifikat tilldelas som garanterar att användaren är anställd eller har uppdrag i regionen, om behörighetsnivå är rätt och om medarbetare inte genomför obligatoriska utbildningar inom informationssäkerhet. Andra risker är hanteringen för användare som avslutar anställning, är långtidsfrånvarande eller byter arbetsplats.

Med detta som bakgrund har revisorerna beslutat att göra en granskning för att bedöma om hanteringen av eTjänstekort ger förutsättningar för ett tillräckligt fysiskt och digitalt skalskydd för att säkerställa krav på informationssäkerhet och om hanteringen sker med en tillräcklig intern styrning och kontroll.

Till viss del har området granskats tidigare då hanteringen av passagebehörigheter ingick i granskningen av museets säkerhetsarbete<sup>1</sup> år 2019. I granskningen har vi följt upp rekommendationerna som lämnades till nämnden för kultur, utbildning och friluftsverksamhet. Området hantering av eTjänstekort ingår i revisionsplan 2024.

---

<sup>1</sup> RE-REV19-0044 Säkerhetsarbetet för museets samlingar



*Revisionen*

## Syfte och revisionsfrågor

Syftet med granskningen är att bedöma om regionstyrelsen säkerställer att hanteringen av eTjänstekort sker med en tillräcklig intern styrning och kontroll.

Revisionsfrågor att besvara är:

- ✓ Är ansvar och roller tydliggjorda?
- ✓ Finns ändamålsenliga styrande dokument, riktlinjer och rutiner?
- ✓ Säkerställs kunskap, kännedom och följsamhet om styrande dokument, riktlinjer och rutiner?
- ✓ Sker kontroll av området på ett effektivt sätt?

## Omfattning och avgränsning

Granskningen omfattar regionstyrelsen. Granskningen omfattar inte hanteringen av fysiska nycklar som ger åtkomst till bland annat lokaler.

I granskningen har vi följt upp rekommendationer som lämnats tidigare till nämnden för kultur, utbildning och friluftsverksamhet<sup>1</sup>.

Granskningen avser 2024 och har genomförts under oktober-december. Internrevision och informationssäkerhetsberättelsen avser 2023 då det är de senaste som återrapporteras när granskningen genomfördes.

## Metod

Granskningen har genomförts med dokumentstudier och intervjuer. Intervjuer har genomförts med medarbetare som arbetar på området inom RSIT (informationssäkerhetschef, infrastrukturspecialist arbetsplatsteknik, processledare IAM<sup>2</sup> kompetensservice, supportcenter och gruppchef servicedesk), regionservice (ansvarig utgivare SITHS-kort, enhetschef och kundserviceagent kontaktcenter och spetstekniker teknik och energi, fastighetsservice) och enhetschef teknik- fastighet och säkerhet Sörmlands museum, Kultur & Utbildning i Sörmland och utvecklingschef, staben för demokrati och insyn.

De som intervjuats har getts möjlighet att faktaavstämma granskningsanteckningarna. Inkomna synpunkter har beaktats i rapporten.

---

<sup>2</sup> Identitets- och åtkomsthantering är den svenska benämningen på engelska Identity & Access Management som förkortas IAM.

*Revisionen*

Mejlfrågor har ställts till förvaltare, fastighetsförvaltning södra, regionservice och förvaltningsledare utveckling och förvaltning (HSA-ansvarig), RSIT

## Revisionskriterier

Granskningens bedömningar har gjorts bland annat mot gällande lagstiftning/regelverk, regionens styrande dokument, riktlinjer och rutiner på området.

## Granskningens resultat

Regionen använder benämningen eTjänstekort, (elektroniska tjänstekort) för SITHS-kort. SITHS står för **Säker IT Hälsa** och Sjukvård och är en identifieringstjänst som är en godkänd metod för inloggning i nationella vårdssystem.

Regionen tillhandhåller fyra olika typer av ”bärare” för behörigheter till IT-system och inpassering i lokaler. Dessa är eTjänstekort, reservkort, nyckelkort och taggs.

Hanteringen av nyckelkort och taggs, som endast ger åtkomst till passage, beskrivs avsnittet inpassering i lokaler.

Den gemensamma nämnaren för eTjänstekort och reservkort är att korten innehåller tjänstecertifikat (SITHS) och för SIS-godkända<sup>3</sup> kort även en personlig e-legitimation. Tjänstecertifikatet är personligt och innehåller medarbetarens/personens behörigheter.

Inera AB<sup>4</sup> tillhandahåller identifieringstjänsten SITHS. Region Sörmland är ansluten till SITHS e-id portalen och har därmed förbundit sig att följa beslutat *Tillitsramverk Identifieringstjänst SITHS*<sup>5</sup>. Tillitsramverket beskriver de krav som gäller för att utfärda och hantera SITHS e legitimation och SITHS funktionscertifikat.

För elektroniska identitetshandlingar för personer är kraven fördelade på olika så kallade Tillitsnivåer. Detta svarar mot olika grader av teknisk och operationell säkerhet hos ansluten organisation som ger olika säkerhet i kontrollen av att en person, som tilldelas en

---

<sup>3</sup> Ett SIS-märkt kort är det enda kort som samtidigt kan visa företagstillhörighet och fungera som giltig legitimation. SIS står för Svenska Institutet för Standarder. Standarder på SIS - Svenska institutet för standarder, SIS, hämtad 2024-12-03

<sup>4</sup> Inera AB är kommunernas och regionernas digitaliseringsbolag med uppdrag att utveckla välfärden. Om Inera - Inera, hämtad 2024-12-03 Ägs av SKR-Företag, 21 regioner, 289 kommuner. Inera ansvarar för ett 40-tal nationella digitala tjänster. För media - Inera, hämtad 2024-12-03

<sup>5</sup> Tillitsramverk Identifieringstjänst SITHS, fastställt datum 2024-01-11 Tillitsramverk för Identifieringstjänst SITHS.pdf hämtad 2024-12-03

*Revisionen*

elektronisk identitetshandling, verkligen är den hen utger sig för att vara. Ju högre tillitsnivå, desto säkrare e-legitimation.

I granskningen har vi tagit del av skriftlig information, rutiner på intranätet, i Självbetjäningsportalen och på Ineras hemsida. Vi har fått hantering och rutiner beskrivna för oss vid våra intervjuer.

**eTjänstekort**

Alla medarbetare och personer med uppdrag i regionen ska ha eTjänstekort. Kortet har foto på personen och är en tjänstelegitimation, en elektronisk ID-handling som ger åtkomst till IT-system och lokaler. Giltighetstiden är fem år.

eTjänstekort kräver att medarbetaren finnas registrerad i HSA-katalogen<sup>6</sup>. Det sker med automatik utifrån information i det personaladministrativa systemet Heroma. Informationen i Heroma överförs till den elektroniska katalogen i Sörmland (ekS<sup>7</sup>). Informationen i ekS överförs till HSA-katalogen.

Inhyrd personal/personer som har uppdrag i regionen läggs upp manuellt i ekS av ansvarig chef.

Beställning och utgivning av eTjänstekort följer särskild rutin inom kontaktcenter/ID-handläggare (fotografering i fotostation, tilldelning av behörigheter utifrån beställning av behörig beställare), aktivering<sup>8</sup>, legitimering<sup>9</sup>, kvittering och utlämning). Medarbetaren får del av Ineras skriftliga dokument *Allmänna villkor för SITHS e-legitimation*.

**Reservkort**

Ett reservkort kan ersätta eTjänstekort och ska användas under en begränsad tid, normalt två månader men kan vid speciella behov utfärdas på maximalt sex månader. Foto saknas på personen. Reservkort har samma behörigheter som eTjänstekort. Reservkort ges till visstidsanställda och till personer som inte är anställda, till exempel

---

<sup>6</sup> HSA står för Hälso-och Sjukvårdens Adressregister. Det är en databas innehåller all information om alla personer och verksamheter inom sjukvården i Sverige. (källa: sv e-identitet). Uppgifterna i HSA används också för att ge rätt behörighet när användare loggar in i tjänster och IT-system.

<sup>7</sup> ekS är regionens grunddataregister över organisation och medarbetare, inhyrd personal med flera.

<sup>8</sup> Aktivering av eTjänste-kort har Tillitsnivå/giltighetsnivå 3 som krav som kräver giltig legitimationshandling. Saknar medarbetare giltig legitimationshandling kan medarbetaren endast få ett reservkort som har Tillitsnivå/giltighetsnivå 2 som krav.

<sup>9</sup> Utgivningsrutinen för eTjänstekort har Tillitsnivå 3 (särskilda krav ska uppfyllas på personnivå). Medarbetaren har med sig kortet, identifiering och verifieringen sker enligt godkänd rutin och två ID-handläggare godkänner samtidigt i (SITHS eID-portal) i två olika datorer med kortläsare.

*Revisionen*

praktikanter och studerade. Giltig legitimation krävs för att få ut ett reservkort

Beställning och utgivning av reservkort följer särskild rutin och utfärdas av ID-handläggare /ID-handläggare reservkort på kontaktcenter, akutmottagningar och i verksamheterna.

Giltigt certifikat laddas ned, identifierar<sup>10</sup> sker med svensk id-handling eller på annat sätt enligt särskild rutin. Kvittens undertecknas och reservkort/pinkod överlämnas. Reservkortet aktiveras på plats. Personen tar del av villkoren innan certifikaten laddas ned på kortet. När kontaktcenter utfärdar reservkort får personen del av Ineras skriftliga dokument *Allmänna villkor för SITHS e-legitimation*.

**Avslut**

Chef ansvarar för att eTjänstekort/reservkort avslutas så snart som möjligt när en medarbetare slutat sin anställning, ett kort försvunnit eller slutat användas. Det görs i Självbetjäningsportalen och kortet klipps itu och kastas. När en medarbetares anställning upphör och avslutas i ekS, avslutas eTjänstekort/reservkort automatisk. ekS uppdateras varje dygn. Reservkort är tidsbestämda och avslutas när tiden är uppnådd.

**Beställning av behörigheter och felanmälan**

Behöriga beställare<sup>11</sup> beställer nya, ändrar och avslutar behörigheter till regionen IT-system i Självbetjäningsportalen. Behörigheter beställs utifrån arbetsuppgifter som ska utföras beroende på tjänst/anställning. Beställning bekräftas av verksamhetschef eller delegerad och anger, att behovet och risken med åtkomst har beaktats. Servicedesk RSIT tilldelar behörighet till eTjänstekortet/reservkortet i SITHS e-ID-portalen. Om något inte stämmer avbryter de beställningen och kontaktar beställaren. Om reservkortet ersätter ett eTjänstekort, följer behörigheterna med över till reservkortet.

Servicedesk tar emot felanmälningar via telefon, under kontorstid eller självbetjäningsportalen. Ett vanligt fel är att kort inte fungerar då de är låsta. Om fel kod slås in för många gånger låses eTjänstekort och reservkort. Korten låses upp enligt särskild rutin.

---

<sup>10</sup> Kraven för Tillitsnivå 2 är att personen är 18 år eller äldre. Om personen inte har godkänd svensk id-handling sker identifiering på annat sätt enligt särskild rutin.

<sup>11</sup> Objektspecialister ITA, behörighetssamordnare, IT-koordinatorer, chefer. Utsedda personer i förvaltningsobjekt får endast beställa behörigheter inom egen förvaltning. Behörigheter får inte beställas till sig själv.

*Revisionen*

**lakttagelse**

Det finns många olika benämningar för samma sak på området när man tar del av information på intranätet, i styrande dokument och hos Inera med flera.

Hantering av eTjänstekort/reservkort sker i många delar av organisationen.

Det beskrivs att det förekommer att medarbetare glömmar eTjänstekortet hemma. Om medarbetaren inte hämtar kortet blir det svårt att utföra arbetsuppgifter. För läkare, som behöver behörighet till nationella system för att till exempel skriva ut mediciner, krävs ett eTjänstekort med tillitsnivå 3. Det i sin tur kräver att ett reservkort utfärdas med tillitsnivå 3 som kräver att två ID-handläggare i kombination måste finnas på plats. Det är inte möjligt utanför kontorstid och i verksamheter utanför sjukhusen där kontaktcenter inte finns.

## **Organisation, roller och ansvar**

**Revisionsfråga: Är ansvar och roller tydliggjorda?**

### **Regionservice**

SITHS-organisationen leds och samordnas av ansvarig utgivare i Region Sörmland (SITHS-kortansvarig), som organisatoriskt tillhör kontaktcenter, regionservice.

Ansvarig utgivare SITHS är både ansvarig utgivare SITHS och kundserviceagent. I rollen som ansvarig utgivare ansvarar hen för den övergripande administrationen på området, har kontakt med Inera, beställer hem de fysiska reservkort buntvis och tilldelar roller för ID-handläggare/ ID-handläggare reservkort med mera. Det beskrivs att det är svårt att kombinera båda uppdragen och att hen hade velat ha mera resurser/arbetstid för att till exempel kunna besöka verksamheter och informera och ta del av deras arbetssätt i hanteringen av eTjänstekort/reservkort.

### **RSIT**

Informationssäkerhetschefen är säkerhetsansvarig och tillhör organisatoriskt RSIT och ansvarar för att övervaka att Ineras regelverk följs och genomför årlig internrevision.

Enheterna servicedesk och behörighet och inköp arbetar också på området med hanteringen av eTjänstekort.

Enheten arbetsplatsteknik, IT-infrastruktur ansvarar för programvaran och hårdvaran som läser av eTjänstekort/reservkort i dator, tangentbord eller i extern kortläsare. Programvaran finns i alla

*Revisionen*

arbetsverktyg/system/datorer där inloggnings sker.

Enligt *regionstyrelsen verksamhetsplan 2024*<sup>12</sup> har RSIT det övergripande ansvaret för styrning och utveckling av regionens informationssäkerhet inklusive informations- och sekretessutbildningar och utveckling av dessa.

**Regionservice**

Förutom SITHS-kortansvarig arbetar kontaktcenter med hantering av eTjänstekort. Fastighetsservice ansvar för behörigheter kopplat till inpassering i lokaler (beskrivs i avsnittet inpassering i lokaler).

**ID-handläggare/ID-handläggare reservkort**

Kontaktcenters medarbetare är ID-handläggare för utgivningsprocessen av SITHS-kort och reservkort. Rollen ID-handläggare reservkort finns i verksamheterna. Handläggaren genomför en utbildning innan rollen tilldelas. På Ineras hemsida finns beskrivning av ID-handläggares/ID-handläggare reservkorts roll.

**Bedömning och rekommendationer**

Bedömningen är att ansvar och roller är tydliggjorda. Hanteringen är utspridd i organisationen vid tiden för granskningen. Förändringar planeras från 2025 (beskrivs i avsnittet framtida arbete).

**Styrande dokument, riktlinjer och rutiner**

**Revisionsfråga: Finns ändamålsenliga styrande dokument, riktlinjer och rutiner?**

I granskningen har vi tagit del av regionens styrande dokument för området informationssäkerhet. Hanteringen av eTjänstekort beskrivs inte specifikt i *Informationssäkerhetspolicy*<sup>13</sup> och inte heller i *Regionstyrelsens reglemente*<sup>14</sup>.

Det styrande dokumentet *Riktlinje för informationssäkerhet*<sup>15</sup> konkretiserar regionens informationssäkerhetspolicy. Riktlinjerna förtydligar externa krav på informationssäkerhet<sup>16</sup> och omsätter dessa i interna krav. Informationssäkerhet ska skydda information

<sup>12</sup> Regionstyrelsen § 203/23, Regionstyrelsens verksamhetsplan med budget 2024–2026

<sup>13</sup> Regionfullmäktige § 131/21, Informationssäkerhetspolicy

<sup>14</sup> Regionfullmäktige § 14/21, Reglemente för regionstyrelsen

<sup>15</sup> Regionstyrelsen § 242/21, Riktlinje informationssäkerhet

<sup>16</sup> Riktlinjen utgår från författningar på området där följande utgör huvuddelen av externa krav, EU:s Dataskyddsförordning, lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, patientdatalag (2008:355), lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, säkerhetsskyddslag (2018:585) och dess förordningar och föreskrifter.

*Revisionen*

oavsett hur den hanteras, lagras och kommuniceras. Skyddet utgörs av administrativa, organisatoriska, tekniska eller fysiska skyddsåtgärder.

Riktlinjen är omfattande och områden kopplat till granskningsområdet är bland annat organisation, roller och ansvar, personalsäkerhet, styrning av åtkomst och fysisk säkerhet.

Under rubriken personalsäkerhet framgår att:

- ✓ Chef ansvarar för att medarbetare genomgår introduktion/utbildning i informationssäkerhet och hur den ska hanteras i verksamheten
- ✓ Innan tilldelning av certifikat (SITHS) ska introduktion/utbildning vara genomförd
- ✓ Aktuell chef ska säkerställa att medarbetare endast har behörighet att komma åt uppgifter eller lokaler/utrymmen som behandlar information eller kan påverka informationshanteringen som är absolut nödvändig. Vid förändringar (avslut/ eller förändrat ansvar, arbetsuppgifter eller organisatorisk placering) ska aktuell chef omgående avsluta/revidera åtkomst till informationssystem och lokaler/utrymmen.

Under rubriken fysisk säkerhet beskrivs att tillträde till utrymmen där informationstillgångar förvaras eller lagras ska begränsas så att endast behöriga har tillträde.

Det styrande dokumentet *Styrning av åtkomst*<sup>17</sup> är en anvisning. Syftet är att och det framgår att regelverket syftar till att förtydliga kraven i *Informationssäkerhetspolicy* och *Riktlinje för informationssäkerhet* samt ge stöd för hur identitet och åtkomst till informationssystem tilldelas, begränsas, styrs och kontrolleras.

Chefen ansvarar för att regelbundet följa upp behörigheter till informationssystem och lokaler. Chefen ska också kontrollera åtkomst till information för att säkerställa god följsamhet av att behörigheter och åtkomst brukas på rätt sätt.

Kontaktcenter har en intern rutin, *e-Tjänstekort och Reservkort*<sup>18</sup>. Rutinen beskriver hur kontaktcenter och, hanterar beställningar av SITHS-kort, fotografering och utlämning av eTjänstekort/reservkort och kvittenser. Den avser också ID-handläggare i verksamheterna och rutinen är att följa rutiner som finns hos Svensk e-identitet och Inera. Länkar anges.

<sup>17</sup> Verkställighetsbeslut, informationssäkerhetschef, RS-LED21-3437-2, Styrning av åtkomst, datum saknas, giltig från 2022-01-01

<sup>18</sup> Beslutad av Ansvarig utgivare för SITHS i Region Sörmland, Rutinbeskrivning E-Tjänstekort och Reservkort, dokumentnummer 19-3078, dokumentdatum 2024-03-05



RSIT har en rutinbeskrivning som heter *Utgivning och hantering av eTjänstekort SITHS*<sup>19</sup>. Rutinen finns på intranätet och beskriver hur kort- och certifikatutgivning och arkivering med mera. Rutinen ska följas av alla ID-handläggare/ID-handläggare reservkort och utgår från Ineras Tillitsramverk identifieringstjänst SITHS.

Servicedesk arbetar enligt framtagna skriftliga rutiner i respektive kunskapsartikel per IT-system, för hur behörigheter ska tilldelas.

### **lakttagelser**

I policyn och i riktlinjen framgår att verksamhetsansvarig ansvarar för att utforma verksamhetsspecifika anvisningar och rutiner om behov finns och att det ska utformas från den regiongemensamma. De som intervjuats har inte kännedom om det finns verksamhetsspecifika anvisningar/rutiner. En översiktlig sökning i ärendehanteringssystemet har gjorts som inte heller visat på att det finns i verksamhetsspecifika anvisningar/rutiner.

Det framgår inte i något av de styrande dokumenten eller rutinerna vad som gäller för förtroendevaldas och medarbetares åtkomst till informationssystem och lokaler vid långtidsfrånvaro (till exempel föräldraledighet, sjukfrånvaro, tjänstledighet eller avstängning). I granskningen har det framkommit att rutin ska tas fram 2025 för långtidsfrånvaro.

Kontaktcenter<sup>18</sup> och RSIT:s<sup>19</sup> rutiner har delvis samma innehåll. Båda rutinerna anger att de använder sig av svensk E-identitets och Ineras rutiner för ID-administratörer när de ska lämna ut SITHS-kort och reservkort. Några exempel på skillnader är kring arkivering och vilken hantering som gäller när en medarbetare har glömt eTjänstekortet hemma och om/hur reservkort ska utfärdas. Kontaktcenter har en muntlig rutin där medarbetare som bor nära arbetsplatsen får hämta eTjänstekortet. I RSIT:s rutin står det att reservkort utfärdas för sju dagar. I intervjuerna har det inte varit tydligt vilken rutin som gäller och om rätt rutin används av kundcenter.

I kontaktcenters rutin finns några inaktuella uppgifter (till exempel avsnittet arbetsbeskrivning beställning av SITHS-kort Unilabs).

Området skyddade personuppgifter/finns inte med i *Policyn* och *Riktlinjen*. I *Styrning av åtkomst* beskrivs att åtkomsten till skyddade personuppgifter ska bedömas och särskilt dokumenteras i behovs-

---

<sup>19</sup> Beslutad av saknas, Rutinbeskrivning Utgivning och hantering av eTjänstekort SITHS, dokumentnummer RS-RSIT24-0020-1, dokumentdatum 2024-02-14



*Revisionen*

och riskanalysen av behörighetsprofiler/roller. Både kontaktcenter RSIT:s rutin beskrivs att särskild hantering krävs för kortbeställning för personer med skyddad identitet.

**Bedömning och rekommendationer**

Bedömningen är att det till stor del finns ändamålsenliga styrande dokument och riktlinjer som beskriver ansvar och som förtydligar externa krav på informationssäkerhet<sup>20</sup> och omsätter dessa i interna krav. I granskningen har de som intervjuats inte haft kännedom om det finns verksamhetsspecifika anvisningar/rutiner.

Chefers ansvar beskrivs i de styrande dokumenten *Riktlinjen* och *Styrning av åtkomst*. RSIT har skriftliga rutiner, per system, för tilldelning av behörighet. Kontaktcenter och RSIT har skriftliga rutiner för hantering av eTjänstekort, det är inte tydligt vilken av dem som gäller. Hantering av skyddade personuppgifter ingår i styrning av åtkomst och i rutinerna.

Det ska tas fram en rutin för hantering av åtkomst till information och lokaler vid långtidsfrånvaro, vilket är positivt. Bedömningen är att det kan utgöra en risk till exempel om en medarbetare stängs av från arbetet och kan vilja åstadkomma skada. De som intervjuats har inte kännedom om vilken hantering som gäller för förtroendevaldas eventuella eTjänstekort. Chefen för staben för demokrati och insyn beskriver att det är otydligt vem som ansvarar för förtroendevaldas eventuella eTjänstekort. I nuläget har staben för demokrati och insyn inte någon rutin som beskriver en hantering.

Vi lämnar rekommendationerna att:

- ✓ Tydliggör vilken rutin som gäller för hantering av eTjänstekort och gör den känd
- ✓ Förtydliga hantering för förtroendevalda och för utfärdande av reservkort då eTjänstekort glömts hemma
- ✓ Säkerställ att planerad rutin för långtidsfrånvaro tas fram och görs känd
- ✓ Säkerställ att verksamhetsspecifika anvisningar/rutiner tas fram.

---

<sup>20</sup> Riktlinjen utgår från författningar på området där följande utgör huvuddelen av externa krav, EU:s Dataskyddsförordning, lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, patientdatalag (2008:355), lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, säkerhetsskyddslag (2018:585) och dess förordningar och föreskrifter.

Revisionen

## Utbildning och information

### Revisionsfråga: Säkerställs kunskap, kännedom och följsamhet om styrande dokument, riktlinjer och rutiner?

På intranätet och i Själbetjäningsportalen finns information, lathundar, ”frågor och svar” och kunskapsartiklar för medarbetare, chefer och de som arbetar på området.

Regionen har tre e-utbildningar<sup>21</sup> på området informationssäkerhet. Det anges i styrande dokument<sup>14</sup> att de är obligatoriska att genomföra innan eTjänstekort tilldelas.

I e-utbildningen *Grundutbildningen informationssäkert* beskrivs att SITHS-kort används för åtkomst till känslig information. SITHS-kort, tjänstekort med flera är värdehandlingar och inloggningsuppgifter ska skyddas. Användaruppgifter, lösenord och enheter för inloggning är personliga, datorn ska aldrig lämnas obevakad när man är inloggad och inloggningsuppgifter får inte delas mellan medarbetare. Incidenter och avvikelser ska rapporteras. Utbildningen avslutas med länkar till intranätet till styrande dokument och handbok informationssäkerhet.

ID-handläggare/ID-handläggare reservkort genomgår utbildning<sup>22</sup> innan de får behörighet i SITHS eID portalen, och delar av utbildningen repeteras en gång per år.

Där finns också RSIT:s broschyr som heter *Säkerhet börjar med dig, Praktisk IT-och informationssäkerhet hemma och på jobbet*<sup>23</sup>. Det anges bland annat att ”Ha för vana att aldrig lämna din dator olåst med tjänstekortet i”.

Kontaktcenter delar ut Ineras dokument *Allmänna villkor för SITHS e-legitimation* till personen som mottar SITHS-kort och reservkort. Dokument beskriver när/hur kort ska spärras, innehavarens ansvar med mera. Ett informationsbrev bifogas också där det bland annat framgår att om en person som förlorar sitt kort ska det omgående spärras med hjälp av ID-administratören eller begära spärr genom att kontakta Ineras support.

### lakttagelser

I intervjuerna beskrivs att det är svårt att få medarbetare på olika

<sup>21</sup> Grundutbildning informationssäkerhet, informationssäkerhet i vården och informationssäkerhet i skolan. På intranätet framgår det att det finns en chefsutbildning för nyblivna chefer och en e-utbildning om informationssäkerhet för chefer.

<sup>22</sup> Secure State Cyber som regionen har avtal med. [SITHS-utbildningar — Secure State Cyber](#)

<sup>23</sup> [Informationssäkerhet - Insidan](#), hämtad 2024-12-03

*Revisionen*

nivåer att förstå att eTjänstekort är en värdehandling och regelverket som finns. Exempel som ges är att kort glöms hemma och medarbetare vill att reservkort utfärdas, koder slängs, borttappade kort anmäls inte och passagebehörigheter som inte är aktuella finns kvar.

I granskningen har vi inte tagit del av om/på vilket sätt ansvarig chef har som rutin att kontrollera att medarbetare genomfört obligatorisk e-utbildning innan eTjänstekort tilldelas.

Informationssäkerhetschefen har kontrollerat detta och det samlade utfallet var att 75 % av medarbetarna hade genomfört e-utbildning (avser de tre obligatoriska e-utbildningarna).

Vi har noterat att det finns information om att eTjänstekort kan spärras hos Ineras support. Informationen är felaktig.

**Bedömning och rekommendationer**

Bedömningen är att det till stor del finns information och utbildning för att säkerställa att medarbetare och chefer har kunskap, kännedom om styrande dokument. E-utbildningarna är obligatoriska och återkommande. Det är en identifierad risk om medarbetare inte genomför utbildning innan de tilldelas eTjänstekort. Det är riskfyllt att det finns inaktuell information om hur kort spärras.

Utifrån de förbättringsområden som beskrivs i avsnittet iakttagelser, är bedömningen att informationen och kompetensen hos medarbetare och chefer behöver stärkas och att ytterligare insatser kan göras för att säkerställa kännedom och följsamhet till styrande dokument, riktlinjer och rutiner. Förslag om att informera på arbetsplatsträffar för att öka kunskap och medvetenhet, har framförts i intervjuerna. Ett annat förslag är att medarbetare får betala när eTjänstekort tappas bort/glömts hemma som gör att reservkort måste utfärdas.

Vi lämnar rekommendationen att:

- ✓ Säkerställ att informationen om hur eTjänstekort spärras är aktuell
- ✓ Säkerställ att obligatoriska utbildningar genomförs innan eTjänstekort tilldelas.

## Uppföljning

**Revisionsfråga: Sker kontroll av området på ett effektivt sätt?**

Informationssäkerhetschefen, i sin roll som säkerhetsansvarig, ansvarar för att initiera internrevision SITHS och det beskrivs i Ineras Tillitsramverk Identifieringstjänst SITHS<sup>5</sup> och syftar till att

*Revisionen*

kontrollera följsamheten till Ineras beslutade regelverk som står under kontroll av Myndigheten för digital förvaltning (DIGG).

*Internrevision – SITHS 2023*<sup>24</sup> fokuserade på att säkerställa att utgivningen av SITHS-kort uppfyller två viktiga komponenter i tillitsnätverket SITHS från Inera. Internrevisionen kontrollerade också hur väl organisationen var förberedd för de nya utgivningsprocesserna för SITHS som infördes januari 2024.

I internrevisionen konstaterades att arbetet med SITHS-kort sköts på ett bra sätt men att tre brister i regionens efterlevnad av Ineras regelverk identifierades:

- ✓ ”I enlighet med SITHS regelverk så framgår det tydligt att det ska finnas en ansvarig utgivare som har det övergripande ansvaret för kort och kortutgivning i organisationen. Vid granskningen kan vi konstatera att ansvaret och arbetsfördelningen är fragmenterad.
- ✓ Vid granskningen kan vi konstatera att det finns bristande resurser att hantera de uppgifter som åligger ansvarig utgivare.
- ✓ Det saknas en heltäckande kontinuitetsplan som omfattar alla SITHS-korts relaterade händelser.”

*Internrevisionen* beskriver förslag till åtgärder.

Enligt det styrande dokumentet *Informationssäkerhetspolicy* under rubriken informationssäkerhetsberättelse, framgår det att ledningen och styrelsen ska informeras av särskilt utsedda roller om informationssäkerhetsläget och dataskydd i regionen samt om vilka åtgärder som bör vidtas.

Regionstyrelsen har beslutat om *Informationssäkerhetsberättelsen 2023 och handlingsprogram 2024–2025*<sup>25</sup>. *Internrevisionen 2023*<sup>24</sup> ingår som en del och de områden som beskrivs i *Policy*<sup>13</sup>.

I avsnittet handlingsprogram för 2024, framgår att de brister som framkommit i *Internrevisionen* är nödvändiga att åtgärda, framför allt de organisatoriska bristerna.

Sedan en tid tillbaka kontrolleras regelbundet användare/medarbetare som har åtkomst, men som inte har loggat in på länge. Informationssäkerhetschefen har kontaktat ansvarig chef

---

<sup>24</sup> RS-LED24-0317-1, Internrevision SITHS 2023, Handläggare Thomas Sunesson, informationssäkerhetsexpert, datum 2024-01-26

<sup>25</sup> Regionstyrelsen § 46/24 Informationssäkerhetsberättelse 2023 och handlingsprogram 2024–2025

*Revisionen*

som informeras om att se över behörigheten och eventuellt avsluta den.

Enligt informationssäkerhetschefen är en förklaring att ansvarig chef inte avslutat behörigheten enligt rutinen eller att man begärt nya behörigheter utan att avsluta de gamla. Det förekommer också att ansvarig chef vill att medarbetare har kvar behörigheter i en övergångsperiod, vid byte av arbetsuppgifter/tjänst, och att sedan glöms det bort att avsluta de gamla behörigheterna.

Den senaste kontrollen som gjordes i kvartal tre 2024 visar att det antalet användare/medarbetare som inte har loggat in på länge har minskat.

Som tidigare beskrivits under rubriken styrande dokument, riktlinjer och rutiner ansvarar chef för att regelbundet följa upp behörigheter till informationssystem och lokaler. Chefen ska också kontrollera åtkomst till information för att säkerställa god följsamhet av att behörigheter och åtkomst brukas på rätt sätt.

#### **Övrig uppföljning**

Kontaktcenter och RSIT beskriver att de samarbetar och att de kontrollerar beställda behörigheter innan de läggs in på eTjänstekort/reservkort.

Enligt RSIT registreras alla typer av felanmälningar som görs i Självbetjäningssportalen. RSIT skulle kunna ta fram statistik över vilka olika typer av fel som uppkommer och som rör hanteringen av eTjänstekort. Ingen har efterfrågat statistik/uppföljning för felanmälningar.

Enligt ansvarig utgivare SITHS finns ingen rutin för uppföljning av behörigheter. Det har inte genomförts någon uppföljning eller tagits några stickprover, under tiden nuvarande ansvarig utgivare SITHS, varit ansvarig.

#### **lakttagelser**

Det finns inga mätbara mål för området och för informationssäkerhet enligt informationssäkerhetschefen. I granskningen har vi noterat att regionstyrelsens internkontrollplan<sup>12</sup> inte innehåller något kontrollområde som avser hantering av eTjänstekort.

Enligt informationssäkerhetschefen har åtgärderna som beslutades i *Internrevisionen 2023*<sup>24</sup> inte genomförts 2024. Planen är att de ska genomföras från 2025 och det beskrivs under avsnittet framtida arbete.

*Revisionen*

Vi har i intervjuerna efterfrågat uppföljning som ansvariga chefer i verksamheterna ska göra, i enlighet med de styrande dokumenten. Ingen av de intervjuade har haft kännedom om/hur uppföljning sker.

**Bedömning och rekommendationer**

Internrevision genomförs och informationssäkerhetsberättelse och handlingsplan beslutas av regionstyrelsen i enlighet med styrande dokument.

Bedömningen är att kontroll av området, som vi fått de beskrivet, inte sker på ett effektivt sätt kopplat till chefsansvaret som anges i de styrande dokumenten. Då det bland annat förekommer att behörigheter inte avslutas när medarbetare byter arbetsuppgifter/tjänst, är uppföljning viktig.

För att uppföljning av behörigheter ska ske systematiskt/årsvis och enhetligt kan underlag tas ut för behörigheter i IT-system per verksamhet och överlämnas till ansvarig chef för kontroll.

Det är positivt att kontroller görs av behörigheter innan de registreras och att informationssäkerhetschefen kontrollerar användare/medarbetare som har åtkomst, men som inte loggat in på länge. Uppföljningen skulle kunna genomföras som ett kontrollområde i internkontrollplanen.

Vi lämnar vi rekommendationer att:

- ✓ Säkerställ att beslutat handlingsprogram 2024–2025 genomförs
- ✓ Säkerställa att ansvarig chef ges förutsättningar att systematiskt genomföra uppföljningar av behörigheter och kontrollera åtkomst till information, till exempel utifrån underlag som distribueras från IT-systemen där behörigheter och åtkomst, är registrerade
- ✓ Överväg att ha med kontrollen av medarbetare/användare som inte loggat in på länge, i internkontrollplanen.

**Inpassering i lokaler/passagebehörighet**

eTjänstekort och reservkort är grunden, och har också behörigheter, för fysisk inpassering, via kortläsare, i lokaler och särskilda utrymmen.

Det finns också nyckelkort och taggs som har samma funktion för inpassering och det beskrivs nedan.

I granskningen har vi tagit del av skriftlig information, rutiner på intranätet och i Självbetjäningsportalen, samt fått hantering och rutiner beskrivna för oss vid våra intervjuer.

*Revisionen*

## Nyckelkort

Nyckelkort används som lånekort. Nyckelkortet är avsedda för personer med tillfälliga uppdrag åt regionen (till exempel praktikanter, entreprenörer/hantverkare, personer under 18 år och varuleverantörer) och verksamheter i regionen.

Det finns två typer av nyckelkort, för medarbetare och för övriga (framför allt för entreprenörer). Nyckelkortet är oftast personliga. Det förekommer att det finns opersonliga nyckelkort. De finns bland annat i verksamheter som lånar ut dem till studenter eller personer med tillfälliga uppdrag. Den som beställer kortet är ansvarig för nyckelkortet. Enligt intervjuerna är det oftast ansvarig chef.

Medarbetare får nyckelkortet med internposten tillsammans med ett kvittensdokument som innehåller information om behörigheten med mera. Dokumentet ska undertecknas och skickas i retur till ansvarig chef på fastighetsservice, som diarieför dokumentet.

Nyckelkort till entreprenörer med flera, kvitteras av mottagaren när kortet lämnas ut. Kvittensdokumentet diarieförs av fastighetsservice.

Det opersonliga nyckelkortet kvitteras inte på personnivå.

## Tagg

Taggs som används för passage till dörrar är en komplettering till eTjänstekort/nyckelkort för passage. Taggen är kopplad till eTjänstekort/nyckelkort med samma passagebehörighet, taggen är personlig. Beställning görs i Självbetjäningsportalen av behörig beställare.

## Avslut

Behörigheter som finns inlagda på eTjänstekort, reservkort och nyckelkort till medarbetare, avslutas automatiskt i passersystemet när personen avslutas i ekS. Opersonliga nyckelkort, nyckelkort och taggs till entreprenörer har inte någon koppling från ekS till passersystemet, då personerna inte finns i ekS, utan måste avslutas manuellt.

## lakttagelser

Inom regionservice södra finns enbart personliga nyckelkort (lånekort) för medarbetare. Enligt intervjuerna ska regionservice norra och västra införa samma hantering.

Vad vi erfar sker ingen kontroll av att medarbetare som mottar personlig nyckelkort skickar in kvittensdokumentet.



*Revisionen*

De som intervjuats har inte kännedom om vilken hantering som gäller när medarbetare är låntidsfrånvarade och för förtroendevaldas eventuella nyckelkort/taggs. Chefen för staben för demokrati och insyn beskriver att det finns förtroendevalda som har tagg för inpassering i lokaler men att det är otydligt hur de tilldelats tagg och vem som ansvarar för hanteringen. Staben för demokrati och insyn saknar rutin som beskriver hanteringen och förteckning över vilka förtroendevalda som har en tagg.

### **Administration av passersystemet**

Det finns många olika passagebehörigheter i passersystemet. En förenklad beskrivning är att de är organiserade i passageområden i en ”katalog/trädstruktur”. Högst upp finns till exempel ett sjukhusområde och längst ned en specifik kortläsare på en dörr.

IT-stödet för passersystemet heter ARX (nedan benämnt passersystemet) och används i de tre fastighetsdriftsområdena (norra, västra och södra).

### **lakttagelser**

I intervjuerna beskrivs det att administrationen av passersystemet sker på olika sätt i de olika fastighetsdriftsområdena. Exempel på olikheter är att hur behörigheter skapas och hur ”katalog/trädstruktur” läggs upp. Vi har fått synpunkten att detta bland annat försvårar arbetet för kundcenters medarbetare som hanterar behörighetsbeställningar i alla fastighetsdriftsområdena. En enhetlig administration bedöms vara säkrare och mindre sårbar.

Det saknas skriftliga rutiner för fastighetsdriftsområdenas administration.

### **Ansvar och roller**

#### **Revisionsfråga: Är ansvar och roller tydliggjorda?**

Fastighetsservice och enheten teknik och energi ansvarar för behörigheter till lokaler förutom till Sörmlands museum och Regionsjukhuset Karsudden. Fastighetsservice ansvarar för ”grundbehörigheter” och ansvarig chef för behörighet till verksamhetens lokaler.

En medarbetare på fastighetsservice är tekniskt sakkunnig och har spetskompetens på området larm och passagesystem i regionen. Personen är ensam i rollen men har kollegor som kan passagesystemet.

### **Skalskydd**

Fastighetsservice ansvarar för det yttre skalskyddet. Det finns en standard för det yttre skalskyddet med krav på kod i kombination



*Revisionen*

med Tjänstekort, nyckelkort och tagg. För det inre skalskyddet är det upp till varje verksamhet att besluta om vilka behörigheter och krav som ska finnas.

Fastighetsservice och kontaktcenter beskriver att de samarbetar och att de kontrollerar beställda behörigheter innan de läggs in i passersystemet. Fastighetsservice har också dialog med verksamheter i enskilda fall.

Om fel kod matas in i kortläsare spärras eTjänstekort, nyckelkort och tagg. De låses upp enligt särskilt förfarande.

**lakttagelser**

Det saknas styrande dokument som beskriver regelverk och standard för skalskydd och det särskilda förfarandet vid upplåsning av spärrade kort när fel kod matats in. Enligt fastighetsservice ser det inre skalskyddet olika ut i verksamheterna och beskriver att den nuvarande hanteringen inte alltid är tydligt och att den bygger mycket på ”gammal hävd” i verksamheterna.

**Styrande dokument, riktlinjer och rutiner**

**Revisionsfråga: Finns ändamålsenliga styrande dokument, riktlinjer och rutiner?**

I det styrande dokumentet *Riktlinje för informationssäkerhet*<sup>15</sup> under rubriken fysisk säkerhet, beskrivs vad som ska gälla för behörighet med mera till utrymmen där informationstillgångar förvaras.

I det styrande dokumentet *Styrning av åtkomst*<sup>17</sup> beskrivs det att ”Regionen ska säkerställa att medarbetare endast har behörighet att komma åt uppgifter eller lokaler/utrymmen som behandlar information eller kan påverka informationshanteringen som är absolut nödvändig”.

Under rubriken uppföljning av behörigheter anges det att ”Det är chefens ansvar att regelbundet följa upp medarbetarnas tilldelade behörigheter till informationssystem och lokaler. Uppföljningen ska dokumenteras för att i efterhand kunna redovisas”.

En muntlig rutin finns för behörigheter för inpassering för AT-läkare som tagits fram tillsammans med enheten AT-läkare, Gemensamt Division Medicin. Kontaktcenter har fått del av rutinen.

På intranätet och i Självbetjäningsportalen framgår information och rutiner för beställning/avslut med mera.

Revisionen

**lakttagelser**

Tekniskt sakkunnig på fastighetsservice känner till de styrande dokumenten som beskrivits ovan men har inte tagit del av dem i detalj.

I det styrande dokumentet *Styrning av åtkomst*<sup>17</sup>, under rubriken kontroll av åtkomst, beskrivs att kontroll av åtkomst är en viktig del i säkerheten kring skyddet av känslig information med mera och syftar till att upptäcka och avskräcka otillåten åtkomst. Chef ska kontrollera åtkomst till information systematiskt och regelbundet, men åtkomst till lokaler nämns inte specifikt.

Vi har inte kunnat finna att det finns något styrande dokument, riktlinje eller rutin som avser området. Synpunkter har framförts vid intervjuerna att det är ett förbättringsområde och att det vore bra att arbeta med och ta fram. Diskussioner har förts om att ta fram regelverk/styrande dokument.

Det saknas styrande dokument, riktlinje eller rutin för de förtroendevaldas behörigheter för inpassering i lokaler. Fastighetsservice har lyft frågan med verksamhetsområdeschefen. Chefen för staben för demokrati och insyn har beskrivit att det finns förtroendevalda som har tagg, för inpassering men att ansvaret och hanteringen inte är tydlig.

I kontaktcenters rutin<sup>18</sup> finns inte hantering för behörigheter till lokaler, nyckelkort eller tagg med.

**Utbildning och information**

**Revisionsfråga: Säkerställs kunskap, kännedom och följsamhet om styrande dokument, riktlinjer och rutiner?**

På intranätet och i Självbetjäningsportalen finns information för medarbetare och chefer som avser området. E-utbildningen informationssäkerhet tar inte specifikt upp inpassering i lokaler men beskriver allmänt att eTjänstekort är en värdehandling.

**Uppföljning av behörigheter för inpassering i lokaler**

**Revisionsfråga: Sker kontroll av området på ett effektivt sätt**

Enligt fastighetsservice genomför ansvarig chef i liten utsträckning systematisk uppföljning av behörigheter i enlighet med det styrande dokumentet *Styrning av åtkomst*<sup>17</sup>.

Uppföljning sker sporadiskt, till exempel då en ny byggnad tas i bruk.

Fastighetsservice kan ta fram listor ur passersystemet, över behörigheter som finns registrerade per verksamhet.

*Revisionen*

I nuläget finns ingen beslutad uppföljningsmodell.

**lakttagelser**

I granskningen beskrivs det att det är problematiskt att det finns nyckelkort/taggs som chefer och verksamheterna inte har kontroll på. Nyckelkorterna kan vara opersonliga och det är också möjligt att en person har flera nyckelkort. Det gör att det är komplext att ha kontroll på dem och säkerställa spårbarheten med mera.

Fastighetsservice bild är att vissa verksamheter har en bra kontroll på vilket nyckelkort som delats ut till vem och att de kvitteras. De bevakar att kort lämnas i retur och att behörigheter avslutas. I andra verksamheter saknas kontroll och det förekommer att nyckelkort inte kvitteras, att kort som kvitterats aldrig lämnas åter och inte efterfrågas.

I granskningen har det framförts att behörigheter till utrymmen där informationstillgångar förvaras, är ett förbättringsområde för att uppfylla innehållet för området fysisk säkerhet, i det styrande dokumentet *Riktlinje för informationssäkerhet*<sup>15</sup>.

**Bedömning och rekommendationer**

Bedömningen är att hanteringen av behörigheter för inpassering i lokaler med eTjänstekort, nyckelkort och tagg, inte sker med en tillräcklig intern styrning och kontroll.

Granskningen visar att det saknas styrande dokument som avser området.

Bedömningen är att det styrande dokumentet *Styrning av åtkomst*<sup>17</sup> inte är känt då uppföljning av behörigheter sker sporadiskt, inte samlat och systematiskt. Uppföljning skulle kunna genomföras som ett kontrollområde i internkontrollplanen.

Administrationn av passersystemet för de tre fastighetsdriftsområdena, sker på olika sätt. Det försvårar bland annat behörighetsbeställningar, ökar sårbarheten och minskar säkerheten.

Det är positivt att kontroller görs innan behörigheter läggs in passersystemet, att medarbetare inom regionservice södra inte har några opersonliga nyckelkort och att det finns en muntlig rutin för AT-läkares behörigheter för åtkomst av lokaler.

Det sker ingen kontroll av att kvittenser kommer in från medarbetare som mottar personliga nyckelkort.

*Revisionen*

Bedömningen är att hanteringen av opersonliga nyckelkort inte sker med tillräcklig styrning och kontroll. Hanteringen är riskfylld då det saknas koppling till ekS, manuell hanteringen krävs, kvittens saknas och uppföljningen sker inte systematiskt av ansvarig chef enligt fastighetsservice.

Vi lämnar rekommendationer att:

- ✓ Upprätta och besluta om styrande dokument för området inpassering i lokaler
- ✓ Säkerställ att ansvarig chef ges förutsättningar att systematiskt genomföra uppföljningar till exempel utifrån underlag som distribueras från IT-systemen där behörigheter är registrerade/som distribueras från Självbetjäningsportalen och passersystemet
- ✓ Ta fram och inför enhetlig administration av passersystemet i samtliga fastighetsdriftsområden
- ✓ Säkerställ att rutiner som upprättas är skriftligt dokumenterade
- ✓ Säkerställ att medarbetare som mottar nyckelkort undertecknar och returnerar kvittensen
- ✓ Överväg att ha med området med kontroll av behörigheter i internkontrollplanen.

### **Sörmlands museum**

Som tidigare beskrivits ansvarar inte fastighetsservice för eTjänstekort/reservkorts behörigheter för inpassering till museet. Museets hantering av eTjänstekort/reservkort följer samma hantering som för övriga verksamheter (koppling finns till ekS och behörighet till IT-system) men museet ansvarar för hanteringen av behörigheter för inpassering.

Enligt enhetschef fastighet och säkerhet, har museet höga krav på säkerheten och på vilka som ska ha behörighet till lokaler och när. Kraven finns bland annat för att kunna få inlån av föremål från andra intuitioner och för att uppfylla försäkringskraven enligt Kammarkollegiet.

Ansvarig enhetschef ansöker om medarbetares behörighet till lokalerna, utifrån behoven för att utföra arbetsuppgifter. Behörigheter tidsätts och det är enhetschef för samlingar och kulturhistoria som beslutar om behörighet.

Information finns på intranätet, chefer informeras om hanteringen och informerar i sin tur medarbetare. Enhetschef fastighet och säkerhet registrerar behörigheterna i passersystemet. Det finns ingen

*Revisionen*

skriftlig rutin som beskriver hanteringen av behörigheter. Genomgång görs av behörigheter och inpasseringsloggar sker två gånger per år i enlighet med museets dokumenterade årshjul. Genomgången görs av enhetschef fastighet och säkerhet, enhetschef samlingar och kulturhistoria och länsmuseumchef.

### **Bedömning och rekommendationer**

Bedömningen är att Sörmlands museum, utifrån hur vi fått det beskrivet, säkerställer att hanteringen av behörigheter för inpassering på eTjänstekorten/reservkorten, sker med en tillräcklig intern styrning och kontroll bortsett från att skriftlig rutin saknas för hanteringen av behörighet. Efter genomförd granskning lämnar vi rekommendationen att säkerställa att skriftlig rutin upprättas för hantering av behörigheter.

### **Sörmlands museum- uppföljning av granskning av säkerhetsarbetet på Sörmlands museum**

En fördjupad granskning av säkerhetsarbetet för museets samlingar<sup>1</sup> genomfördes 2019. Då granskningen har kopplingar till denna granskning följs två rekommendationer upp.

Syftet med granskningen var att bedöma om säkerhetsarbetet för föremålen i museets samlingar var ändamålsenlig och bedrevs med en god intern kontroll och om avgränsningen mot regionstyrelsen var tydlig avseende de förhyrda lokalerna där museet finns.

För att ytterligare stärka säkerhetsarbetet och ansvarsfördelningen lämnades rekommendationer till nämnden för kultur, utbildning och friluftsverksamhet om att bland annat:

- ✓ Säkerställa att utvärdering genomförs årligen enligt säkerhetsplanen och att samtliga enheter/professioner på säkerhetsrådet ingår.

Rekommendationer lämnades till regionstyrelsen om att bland annat:

- ✓ Göra ett tillägg i hyresavtalet så att det framgår att museet ansvarar för passagesystemet.

### **Uppföljning av rekommendationer från 2019**

Enhetschefen fastighet och säkerhet, beskriver att ledningsgruppen årligen utvärderar säkerhetsplanen. Utvärderingen sker muntligt på ledningsgruppens möte.

Vi har tagit del av gällande hyreskontrakt för museet från förvaltaren, fastighetsförvaltning södra inom regionservice. Hyreskontraktet har kompletterats med ett tilläggsavtal i december 2019. Det framgår att avsteg görs från Region Sörmlands

*Revisionen*

gränsdragningslista och att museet ansvarar för inbrottslarmet (som hör ihop med passagesystemet).

**lakttagelser**

I granskningen har vi noterat att nämndens<sup>26</sup> internkontrollplan inte innehåller något kontrollområde som avser eTjänstekort kopplat till inpassering i lokaler.

**Bedömning och rekommendationer**

Efter genomförd uppföljning av rekommendationen lämnas ingen rekommendation till regionstyrelsen.

Då den årliga utvärderingen av säkerhetsplanen sker muntligt och inte dokumenteras, är bedömningen att den inte är spårbar. Till nämnden för kultur, utbildning och friluftsverksamhet lämnar vi (fortsatt) rekommendationen/rekommendationerna att:

- ✓ Säkerställa att utvärderingen som utförs årligen enligt säkerhetsplanen, dokumenteras för att säkerställa spårbarhet.

**Framtida arbete**

I granskningen har vi tagit del av organisationsförändringar och utvecklingsarbeten som pågår på området, vilket är positivt. Då granskningen omfattar 2024 är avsnittet med som information om det planerade framtida arbetet.

**Organisationsförändringar**

**Omorganisering av hantering/förvaltning av tjänstekort**

Från januari 2025 kommer ansvaret för hantering/förvaltning av eTjänstekortet (rollen ansvarig utgivare SITHS-kort, SITHS eID portalen och fotostationerna) att flyttas från regionservice till RSIT. Det innebär att hantering och funktioner blir mer samlade i organisationen.

I granskningen har vi tagit del av arbetsgruppen SITHS dokument *Förslag för tjänsteverifiering SITHS kortutgivning*, och där beskrivs bakgrund, det nya upplägget och beslutet om omorganisationen.

I informationssäkerhetsenhetens *internrevision 2023*<sup>26</sup> konstaterades ett antal allvarliga brister i regionens efterlevnad av Ineras regelverk som i värsta fall bedöms kunna utgöra ett hinder mot fortsatt användning av SITHS-kort. Den nya placeringen och en tydlig ansvarig utgivare bör utses med placering på RSIT med mera, bedöms ge bättre förutsättningar för att efterleva Ineras regelverk.

---

<sup>26</sup> Nämnden för kultur, utbildning och friluftsverksamhet § 48/23, Verksamhetsplan med budget 2024–2026, Kultur & utbildning

*Revisionen*

Från januari 2025 kommer informationssäkerhetsenheten flyttas från RSIT och ingå i säkerhets- och krisberedskapsstaben som är en av regiondirektörens staber.

**Mobilt SITHS eID**

Inera har tagit fram en lösning som heter mobilt SITHS eID och som också kan användas för att legitimera sig vid inloggning i stället för med ett fysiskt SITHS-kort. SITHS eID är en applikation som laddas ned på mobiltelefon/surfplatta och inloggningen fungerar på liknande sätt som Mobilt Bank-ID. Lösningen kräver att användaren har ett fysiskt SITHS-kort i grunden.

Lösningen ingår i den senaste versionen från Inera av SITHS eID<sup>27</sup>, och ingår i regionens befintliga avtal. Lösningen kostar inget extra och kan användas redan nu (men inte för inloggning i det nuvarande journalsystemet NCS Cross). Enligt behörighetssamordnaren har regionen valt att fokusera på införandet till SITHS e-ID först och tanken är att lösningen ska lanseras längre fram. Instruktion finns på intranätet, i Självbetjäningssportalen, om hur man loggar in med mobilt SITHS e-ID.

En förhoppning som beskrivs i intervjuerna, är att antalet reservkort kan minska när breddinförande skett. Det skulle bland annat innebära lägre kostnader, mindre administration och minska sårbarheten i verksamheterna.

**Vårdinformationssystemet Cosmic**

När det nya vårdinformationssystemet Cosmic införs vecka 7 2025 kommer Mobilt SITHS eID att kunna användas för inloggning. Det är inte möjligt i det nuvarande journalsystemet NCS Cross.

**Behörighetsportalen**

Behörigheter till regionens IT-system beställs via Självbetjäningssportalen. För hälso-och sjukvården och för Cosmic kommer beställning att hanteras via den nya Behörighetsportalen och för den egna verksamheten. Breddinförandet har inletts i september 2024. Verksamheterna har utsett en behörighetsamordnare som har utbildats och fått behörighet att lägga behörighetsbeställningar i Behörighetsportalen. Chefer har också utbildats och har automatiskt behörighet i sin roll som chef. Inloggning med SITHS-kort krävs. Processledaren IAM<sup>2</sup> kompetensservice beskriver att Behörighetsportalen förenklar hanteringen av behörigheter genom att

---

<sup>27</sup> Enligt ansvarig utgivare SITHS-kort, är kravet i dagsläget att SITHS-kort/reservkort har Tillitsnivå 3. Reservkort med Tillitsnivå 2 fungerar inte för att kunna använda Mobilt SITHS eID.



*Revisionen*

använda grupperingar med grundbehörigheter och tilläggs paket utifrån arbetsuppgifterna som personen ska utföras.

**Kompetenscenter för identiteter och behörigheter (IAM<sup>2</sup> Kompetenscenter)**

Teamledaren för behörigheter & inköp berättar att de, förutom arbetet med Behörighetsportalen, håller på att etablera ett kompetenscenter för identiteter och behörigheter. Kompetenscentret ska inte arbeta direkt med SITHS-kort men systemen de ansluter för hantering av inloggning i olika system, kommer att nyttja SITHS e-id som autentiseringsmetod.

**Säkra utskrifter**

Det är förberett för att eTjänstekort ska kunna användas, som inloggning på regionens skrivare, för att ge säkra utskrifter. Enligt infrastrukturspecialisten arbetsplatsteknik kommer säkerheten att höjas, framför allt för känsliga uppgifter som bland annat finns i journalanteckningar. Förhoppningen är också att antalet utskrivna dokument ska minska. Planen att beslut ska tas i år och införandet ska ske från och med 2025.

Revisionen

Åsa Forsman

Certifierad kommunal revisor