Instruktion för att kunna använda Säkerhetstjänsternas administrationsgränssnitt

Innehållsförteckning

1. Inledning ... 3

2. SITHS-kort ... 4

3. Förutsättningar för åtkomst till Säkerhetstjänsterna ... 4

3.1. Brandväggsöppningar ... 4

3.2. Länk till Säkerhetstjänsternas gränssnitt ... 4

4. Behörighetsgrundande egenskaper i HSA ... 4

4.1. Medarbetaruppdrag med rättigheter för spärr- och loggadministration ... 4

4.2. Individuell egenskap för it-tjänster ... 5

Instruktion för att kunna utnyttja funktioner i Säkerhetstjänsterna

Denna instruktion beskriver vilka tekniska förutsättningar som gäller för att komma åt Säkerhetstjänsterna och hur man i HSA sätter upp behörigheten som behövs för att kunna utnyttja funktioner i Säkerhetstjänsterna. Instruktionen visar hur olika administratörer får tillgång till de användargränssnitt som Säkerhetstjänsterna tillhandahåller.

Denna instruktion täcker följande roller:

- Loggadminstratör
- Spärradministratör

I dokumentet refereras dessa roller som ”Administratören” när informationen gäller alla roller.

Revisionshistorik		
Version	Författare	Kommentar
1.0	Tomas Fransson	Slutversion
1.1	Tomas Fransson	Uppdaterat länkar till 2.1-versionen av SÄK i kap 3
1.2	Tomas Fransson	Referens till Portöppnningsdokumentet för att bättre förklara förutsättningarna för 2.1
1.3	Tomas Fransson	Döpt om dokumentet, ny huvudrubrik
1.4	Tomas Fransson	Korrigerat URL till Sjunet
1.5	Tomas Fransson	Uppdaterat referens till Portförändringsdokumentet
1.6	Tomas Fransson	Uppdaterat referens till Webadmin-GUI efter produktionssättning av 2.6.1
1.7	Henrika Littorin	Uppdaterat information om HSA
1.8	Tomas Fransson	Revidering efter Henrikas kommentarer

1. Inledning

Administratören behöver tillgång till Säkerhetstjänsternas användargränssnitt.

För att administratören ska kunna arbeta behöver organisationen vara ansluten till Säkerhetstjänsterna.

Som administratör behöver man ha

- giltigt SITHS-kort och tillhörande inloggningskoder
- åtkomst till Säkerhetstjänsternas administratörsverktyg

- registrerade behörighetsegenskaper i HSA

Denna instruktion ger information om hur organisationen skapar förutsättningar för att kunna agera som administratör i Säkerhetstjänsterna.

2. SITHS-kort

Saknar administratören giltigt SITHS-kort alternativt att man inte har sina koder kontaktar man den egna enheten för utgivningen av SITHS-kort.

Mer om SITHS-kort finns att läsa på Ineras webbplats: www.inera.se.

3. Förutsättningar för åtkomst till Säkerhetstjänsterna

3.1. Brandväggsöppningar

I dokumentet ”Port och IP-adresser för nationella Säkerhetstjänster” beskrivs brandväggsöppningarna som gäller för att få åtkomst till Säkerhetstjänsterna.

Alla dokument som beskriver Säkerhetstjänster finns på www.inera.se.

3.2. Länk till Säkerhetstjänsternas gränssnitt

Länkarna nedan ger tillgång till Säkerhetstjänsternas administrationsverktyg. OBS kräver SITHS-kort och tillhörande programvara.

Sjunet
https://sakerhetstjanst.sjunet.org/spadmin

Internet
https://sakerhetstjanst.inera.se/spadmin

4. Behörighetsgrundande egenskaper i HSA

Varje person som ska vara administratör måste finnas upplagd i HSA. Personen måste också ha verksamhetschefens uppdrag att få åtkomst till patientinformation i ändamålet Administration samt att vara spärr- och/eller loggadministratör.

Administration i HSA görs av lokala HSA-administratörer i den egna organisationen, antingen via det nationella administrationsgränssnittet HSA Admin eller via ett administrationsgränssnitt mot den lokala HSA-katalogen. Kontakta din lokala HSA-förvaltning för att få veta vad som gäller hos er.

4.1. Medarbetaruppdrag med rättigheter för spärr- och loggadministration

Medarbetaruppdrag är den tekniska beskrivningen av verksamhetschefens individuella behörighetstilldelning i enlighet med Patientdatalagen. Verksamhetschefen för en vårdenhet beslutar att en medarbetare för att kunna utföra sitt arbete behöver åtkomst till patientdata och i vilket ändamål. För att få åtkomst till Spärr- och loggfunktionen krävs att administratören har verksamhetschefens

tillåtelse/uppdrag att läsa patientdata i ändamålet Administration, d.v.s. **spärr- och loggadministratören är kopplad till ett medarbetaruppdrag med ändamålet Administration**.

För mer information om hur detta hanteras i HSA, se Handbok för HSA-administratörer på www.inera.se alternativt den egna organisationens handbok för det lokala administrationsgränssnittet.

Notera att medarbetaruppdraget ska registreras på vårdenhetsnivå. Verksamhetschefen för den vårdenheten inom vårdgivaren vidtalas och står för uppdragsgivandet till de spärr- och loggadministratörer som kommer att arbeta för hela vårdgivaren. Eftersom spärrar och loggdata betraktas som patientdata måste verksamhetschefen för de medarbetare som arbetar som administratörer följa upp deras arbete. Detta möjliggöras genom den loggning som sker i administrationsgränssnittet.

4.2. Individuell egenskap för it-tjänster

Utöver medarbetaruppdraget med ändamålet Administration krävs även att ett värde läggs in i attributet ”Individuell egenskap för it-tjänster”. Följande värden ska användas:

Roll	Värde
Loggadministratör	BIF;Loggadministratör
Spärradministratör	BIF;Spärradministratör

För mer information om hur detta hanteras i HSA, se Handbok för HSA-administratörer på www.inera.se alternativt den egna organisationens handbok för det lokala administrationsgränssnittet.