# SITHS Säkerhetsarbete

## Hitta i dokumentet



## Syfte

Syftet med denna rutin är att ge en samlad bild och beskrivning av det systematiska säkerhets- och riskhanteringsarbetet inom SITHS i Region Halland och anslutna organisationer.  För mer information om SITHS-organisationen och kontaktuppgifter till ansvariga se: Vårdgivare - Region Halland

## Bakgrund

SITHS strukturerade och systematiska säkerhetsarbete pågår kontinuerligt och styrs av Ineras Tillitsramverk för Identifieringstjänst SITHS. Syftet med arbetet är att ständigt förbättra säkerheten och kvalitén inom utgivningsområdet. Bland annat genomförs riskanalyser och internrevisioner. Avvikelser och inträffade säkerhetsincidenter ska alltid vara ingångsvärden till riskanalys och internrevision. Arbete med åtgärder efter revision och riskanalys pågår kontinuerligt.

Löpande arbete pågår kontinuerligt med att följa upp inträffade avvikelser och säkerhetsincidenter. Det kontinuerliga säkerhetsarbetet med SITHS inom Region Halland följer årshjulet, se nedan i dokumentet.

**Förkortningar som förekommer i dokumentet**
AU = Ansvarig utgivare, BU = Biträdande ansvarig utgivare, SA = SITHS säkerhetsansvarig.

**Områden**
De områden, inom SITHS, som regelbundet omfattas av riskhantering och granskning är:
**Områden inom ramverket (att revidera löpande)**

1. Organisation och styrning RH
2. Säkerhet och Revision
3. Direktansluten organisations förpliktelser
4. Avveckling av utgivningsområde
5. Fysisk och administrativ säkerhet
6. Elektroniska identitetshandlingar för personer
7. Elektroniska identitetshandlingar för funktioner
8. Regler för ombud

För mer information hur de olika områdena omfattas av revision och riskhantering, se fördjupning under respektive rubrik i detta dokument: Tillitsramverk för Identifieringstjänst SITHS

## Fysisk och administrativ säkerhet

### Administrativ säkerhet

Åtkomst till SITHS eID Portal för ID-administratörer kräver identifiering med tillitsnivå 3 och är det krav som Inera ställer på åtkomsten.

## Riskhantering - Förebyggande arbete

### Riskanalys – process/genomförande

Riskanalyser ska genomföras löpande vid större förändringar inom området.

En årlig riskanalys bör genomföras och ska då omfatta alla områden inom SITHS, enligt ovan. Vid dessa tillfällen ska även tredjepartsanslutna delta i arbetet.

Inom IT- och digitalisering genomförs årligen en övergripande riskanalys, här ska SITHS-området beaktas, se rutin: Riskhantering ITD

Ansvarig utgivare ansvarar för att riskanalyser genomförs samt upprättar åtgärdsplaner

Arbetet genomförs i workshopform i grupp. Deltagare varierar utifrån behov, ett ingångsvärde i riskanalysen är inträffade avvikelser och incidenter.

### Åtgärdsplaner efter riskanalys

Efter genomförd riskanalys ska åtgärdsplaner tas fram. Ansvarig utgivare ansvarar för att dessa tas fram samt att åtgärder genomförs. Flera olika roller kan behöva delta i arbete med att genomföra åtgärdsplanen. Åtgärdsförslag/planer dokumenteras i samma mall som riskanalysen genomförs i.

### Dokumentation

Riskanalys samt åtgärdsplaner ska bevaras i minst 10 år och ska kunna vara läsbara under hela denna tid. Dokument diarieförs och bevarande sker i Platina, i SITHS årsakt.
Rapporten distribueras till: Ansvarig utgivare, Säkerhetsledningen Region Halland samt till berörda avdelningschefer.

## Säkerhet och Revision - Granskning

### Extern revision

SITHS PA (SITHS Policy Authority) har rätt att revidera alla anslutna organisationer. Vid sådan revision ska den anslutna organisationen skyndsamt vara behjälplig med framtagande av uppgifter och säkerställa att relevant personal finns tillgänglig.

### Intern revision – Förbereda/genomföra

Internrevision genomförs årligen och sker genom *fastställd revisionsplan* som sträcker sig över tre år. Underlag till revision skall alltid vara resultat från genomförda riskanalyser, avvikelser och inträffade incidenter sedan föregående revision. Avvikelser och åtgärdsarbete från föregående revision följs upp. Internrevision initieras av säkerhetsansvarig. Den ska ledas av säkerhetsansvarig eller oberoende kontrollfunktion.

De organisationer som Region Halland har samarbetsavtal med (tredjepartsanslutna) ska erbjudas möjlighet att delta vid revision vid lämpliga tillfällen.

Då Region Halland delar kortkontor med de halländska kommunerna ska de erbjudas möjlighet att delta på de revisioner som genomförs gällande kortkontoren. De ska ha möjlighet att delta i hela revisionsarbetet med både förberedelser, genomförande och efterarbete.

**Åtgärdsplaner**
Efter genomförd internrevision ska åtgärdsplaner tas fram. Ansvarig Utgivare är ansvarig för att ta fram åtgärdsplaner samt att åtgärderna genomförs enligt plan. Flera olika roller kan behöva delta i arbete med att genomföra åtgärder efter revision. Åtgärdsplaner dokumenteras i revisionsrapporten

**Dokumentation**
Revisionsresultat dokumenteras i mallen: *SITHS - Intern revisionsrapport.*
Revisionsrapport samt åtgärdsplaner ska bevaras i minst 10 år och ska kunna vara läsbara under hel denna tid. Dokument diarieförs och bevarande sker i Platina, i SITHS årsakt
Rapporten distribueras till: Ansvarig utgivare, Säkerhetsledningen Region Halland Säkerhetsledningen Region Halland samt till berörda avdelningschefer.

## Avvikelser och säkerhetsincidenter SITHS

Alla avvikelser inom SITHS ska rapporteras i Platina enligt gällande rutiner.
(Avvikelser.docx (regionhalland.se)
Avvikelser ska kategoriseras: Informationssäkerhet/SITHS.

Om avvikelsen också är en SITHS säkerhetsincident (för exempel på vad som är en säkerhetsincident SITHS se nedan) ska detta även meddelas till Ansvarig utgivare på adressen: siths.eid@regionhalland.se. Vid behov av stöd kontakta servicecenter.
Det som ska framgå i meddelandet är:

1. Kontaktperson och kontaktuppgifter
2. Vad har hänt?
3. När hände det?
4. Genomförda åtgärder

**Exempel på SITHS Säkerhetsincidenter som ska rapporteras enligt ovan är:**

- **Falsk identitet**
  Om du misstänker eller vet att någon försöker använda falsk identitet eller felaktiga grunder för att komma över ett SITHS-kort eller reservkort.
- **Felaktig kort- och kodhantering**
  Här avses händelser som medför en säkerhetsrisk då man hanterar kort felaktigt. Det kan handla om att man utfärdar reservkort på felaktigt sätt, exempelvis till personer som ej är på plats, felaktigt användande av reservkort istället för ordinarie kort, utlånande av SITHS-kort eller om kort utfärdats på fel person.
  Det kan också vara om koder hamnar fel. Exempelvis om kodkuvert förvaras felaktigt eller om koder på annat sätt är tillgängliga för obehöriga.
- **Manipulering av certifikat, kort och system för SITHS**
- Om du upptäcker att någon har försökt eller lyckats manipulera certifikat, kort eller system för SITHS.
- **Hot och våld**
  Incidenter där personal är utsatta för hot och våld kopplat till SITHS. Exempelvis kunder eller patienter som försöker komma över SITHS-kort, hotfulla personer på

kortkontoren vid utfärdande av kort och dylikt. Hot och våld som inte är kopplat direkt mot utgivningsområdet behöver ej rapporteras

- **Inbrott/stöld**
  Inbrott och stöld som är riktat mot SITHS, dvs där man har som syfte med inbrottet eller stölden att komma över SITHS-kort, reservkort eller dylikt. Ett inbrott där syftet varit att stjäla datorer, men där ett SITHS-kort också ”följt med” ska inte rapporteras som incident. Om du blivit av med ditt personliga SITHS-kort via inbrott i hemmet eller rån, men där syftet ej var att stjäla kortet ska det inte heller rapporteras.
- **Fysisk säkerhet**
  Brister i den fysiska säkerheten runt hantering av kort. Exempelvis kort låses ej in enligt gällande rutiner på kortkontoren, felaktig behörighet till låsta utrymmen, försändelse som har manipulerats/öppnats felaktigt/skickats fel, bristande säkerhet vid mobila kortkontor.
- **Misstanke mot kollega**
  Om det föreligger misstanke om att korthandläggare utfärdar kort på fel grunder eller till fel personer utifrån ett kriminellt syfte.

**Polisanmälan**
Vid behov ska polisanmälan göras. Polisanmälan genomförs alltid direkt av drabbad person/verksamhet. Ansvarig utgivare stöttar vid behov. Se regional rutin för polisanmälan här

**Vidarerapportering till Inera**
Händelser som ska rapporteras vidare till Inera är händelser där konfidentialitet eller riktighet är bekräftat eller befarat påverkat. Ansvarig utgivare beslutar tillsammans med SITHS. Händelserapport skrivs av Ansvarig utgivare och skickas till Inera via e-post support@inera.se.

**Dokumentation - bevarande**
Mall för händelserapport: Händelserapport)

Händelserapporter från SITHS Säkerhetsincidenter ska bevaras i fem (5) år efter inträffad händelse. Dokument diarieförs och bevarande sker i Platina, i SITHS årsakt.

**Uppföljning**
Om det i händelseanalysen framkommer ett behov av uppföljning av incidenten med tillhörande åtgärder ansvarar Ansvarig utgivare för att detta hanteras i Åtgärdsplanen.

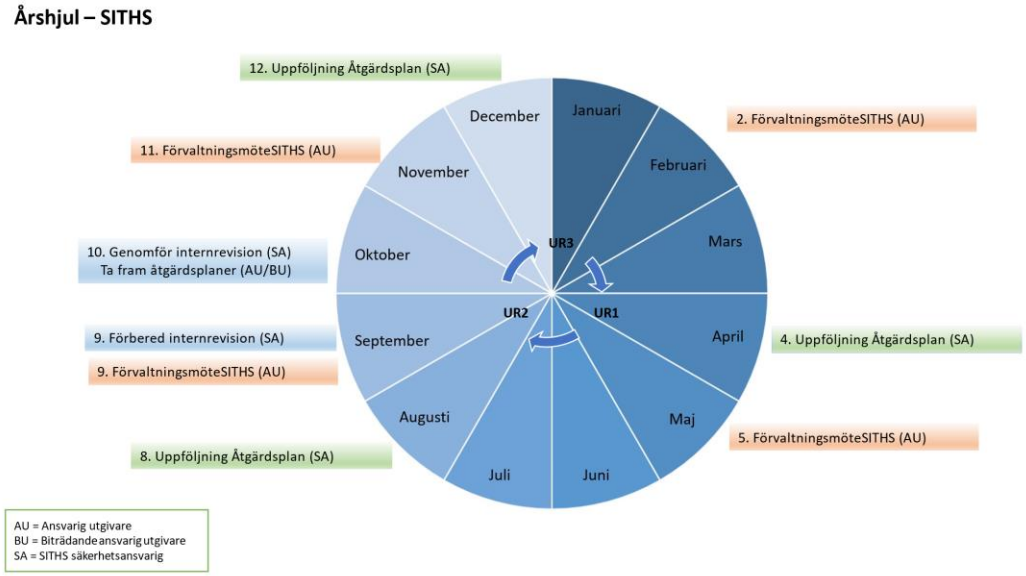
## Uppföljning/utvärdering

Säkerhetsansvarig har till uppgift att utvärdera utgivningsområdets efterlevnad av utgivningsprocesser för elektroniska identitetshandlingar. I detta ingår att initiera och följa upp resultat och åtgärdsplaner från internrevision och riskanalyser. Säkerhetsansvarig ska följa upp att organisationen uppfyller sitt åtagande och utöva tillsyn av Ansvarig utgivare

SITHS Säkerhetsansvarig initierar till uppföljning av åtgärdsarbetet enligt fastställt årshjul SITHS, 3 gånger per år. Underlag till uppföljning är SITHS Åtgärdsplan. Medverkande vid uppföljningsmöten, förutom SITS säkerhetsansvarig, är Ansvarig utgivare, Biträdande ansvarig utgivare samt avdelningschef/Applikationer för regional utveckling.

**Uppföljning av åtgärdersplaner**
SITHS Säkerhetsansvarig initierar uppföljning av åtgärdsplaner från bland annat riskanalyser och internrevisioner. Uppföljning sker i sammanställd Åtgärdsplan, minst tre gånger per år enligt fastställt ”Årshjul SITHS” enligt ovan.

**Dokumentation**
Rapport från riskanalys, internrevision ska bevaras i minst 10 år och ska kunna vara läsbara under hela denna tid. Dokument diarieförs och bevarande sker i Platina, i SITHS årsakt




## Bilagor/länkar:

Rutin: Riskhantering ITD
*SITHS – Intern revisionsplan*
*SITHS – Intern revisionsrapport*
Säkerhetsincident Händelserapport - rapportmall

## Uppdaterat från föregående version

Uppdaterat rutinen i sin helhet. Ändrat gällande: områden, internrevision, riskhantering, ansvarsfrågan, årshjul samt uppföljning. Ny huvudförfattare och fastställare

**Tidigare uppdateringar**
Uppdaterat rutinen i sin helhet. Tidigare namn: SITHS – Revisioner, loggkontroll, riskanalys och missbruk av certifikat.